



# Packet Flow Operating Software (PFOS) 6.x

## User Guide

---

Software Version 6.5.1

733-1944 / 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

<b>PFOS User Guide 6.5.1 Revision History</b>	16
<b>1 PFOS User Guide 6.5.1 Introduction</b>	18
Audience	18
Related Documentation	18
Applicable Hardware Systems	19
PFOS on NETSCOUT Hardware	19
PFOS on Certified Hardware	19
PFOS on Third-Party Qualified Hardware	19
PFOS Licensing	20
Licensing for Applicable Hardware Systems	22
License Status	22
License Notifications	22
Retrieving New or Renewal Full License Keys	23
PFS 5000/7000 and PFS 6000 Appliances purchased from NETSCOUT	23
Certified and Qualified Switches	23
License File Format	23
Installing a New License File	24
Deleting a License File	24
Related NETSCOUT Products	25
Hardware Feature Cross-reference	26
PFS 5121/7121-64X Limitations and Configuration Considerations	28
PFS 503x/703x-32X, 5031/7031-56X, and 5030/7030-54X Limitations and Configuration Considerations	28
PFS 5040/7040-32D and 5041/7041-32D Limitations and Configuration Considerations	30
Network Access to PFOS	32
<b>2 Managing with PFOS</b>	33
Configuration File Types	33
Management Interfaces	33



Command Line Interface (CLI) .....	34
Web UI .....	34
NETCONF API .....	34
RESTCONF API .....	34
Logging in to the Web UI .....	35
Change Default Password .....	35
License Agreement .....	36
Using Secure (HTTPS) Web Browser Connections .....	36
Failed Login Attempts .....	37
Password Policies .....	38
Using the Web UI .....	39
Toolbar Details .....	39
System Status .....	41
System Tab .....	42
Network Tab .....	42
Software Tab .....	42
Clocks Tab .....	43
Configuration Task Flow .....	43
Zero Touch Provisioning .....	44
ZTP Activation Process .....	45
PFS Configuration File .....	45
DHCP Server Configuration .....	45
IPv4 (dhcpd.conf) .....	46
IPv6 (dhcpd6.conf) .....	46
Zero Touch Provisioning Known Limitations .....	47
<b>3 Configuring the System and Ports .....</b>	<b>48</b>
Configuring System Settings .....	48
Configuring Global System Settings .....	49
Basic Information Settings .....	49
Network Settings .....	50
Source Port VLAN Tagging .....	55
Features .....	55
Syslog .....	69
Trace Log .....	74
nCM .....	74
NMS .....	75
Configuring Notifications .....	75
Events .....	75
SNMP .....	77
Configuring Time Settings .....	81
Manual Time Setting (Clock) .....	81



Port Timestamp .....	.82
NTP .....	.82
GPS .....	.84
PTP .....	.84
Linux PTP .....	.86
Configuring Access Control .....	.87
User Access (Roles and Users) .....	.87
Add a Role .....	.88
Add a New User .....	.92
List Currently Configured Users .....	.93
Delete One or More Users .....	.93
Change a Password .....	.93
Password Policies .....	.93
Password Expiration .....	.94
Minimum Password Length and Character Requirements .....	.94
Remote Authentication .....	.95
Configure Authentication Order .....	.96
Add a RADIUS Server .....	.97
Add a TACACS Server .....	.97
Add an LDAP Server .....	.98
CLI Remote Authentication with FIPS or Common Criteria Modes Enabled .....	.99
Remote Authorization .....	.100
Session Limit .....	.100
Limit Concurrent Sessions .....	.100
User and IP Lockout Settings .....	.101
Configure User and IP Lockout Settings .....	.102
Client IP Lockout .....	.102
Firewall Rules .....	.103
Configure Firewall Rules .....	.103
Firewall Rule Considerations and Limitations .....	.105
Configuring Ports .....	.105
Port Classes .....	.106
Span Ports .....	.106
Monitor Ports .....	.106
Span-Monitor Ports .....	.106
Service Ports .....	.106
pStack and pStack plus Ports .....	.106
Inline Network Ports .....	.107
Inline Monitor Ports .....	.107
Using the Port Settings Page .....	.107
Configure Port Settings .....	.108
Port Settings .....	.108
Port Groups .....	.118



Port Group Procedures .....	119
<b>4 Base Features and Tasks .....</b>	<b>126</b>
About 200G Port Groups .....	126
Traffic Maps .....	127
Traffic Map Processing .....	127
Example 1 – Traffic Maps with Filtering on Same Input Ports .....	127
Example 2 – Traffic Maps with Filtering on Different Input Ports .....	128
Merging Traffic Maps .....	128
About Traffic Maps and Service Ports .....	129
About Traffic Maps and Span-Monitor Ports .....	129
Traffic Map Procedures .....	129
Create a Traffic Map .....	129
Change the Processing Order of Traffic Maps .....	133
Merge Traffic Maps .....	135
Delete Traffic Maps .....	135
View Traffic Map Status .....	136
View Remote Monitor Group Status .....	136
View Output pStack Interface .....	136
Traffic Filtering .....	137
Forwarding Filters Library .....	138
Filtering Workflow .....	138
Constructing Filter Expressions .....	140
Octet Locations on a TCP/IP Frame for IPv4 and IPv6 Packets .....	143
Packet Fields .....	144
Special Filters: Unfiltered and Nonmatch .....	144
Filter Expression Examples .....	144
Filtering Bi-directional Traffic .....	146
Filter Precedence .....	146
Understanding PFS Filter Resources .....	148
Filter Elements .....	149
Calculating Filter Resource Usage .....	149
Filter Resources Usage by pStack and pStack+ .....	151
Filter Resource Limits .....	152
PFS 5010/7010 Filter Resource Limits .....	153
PFS 51xx/71xx Filter Resource Limits .....	155
PFS 503x/703x-32X, PFS 5031/7031-56X, and PFS 5030/7030-54X Filter Resource Limits .....	159
PFS 5040/7040-32D Filter Resource Limits .....	163
PFS 5041/7041-32D Filter Resource Limits .....	166
PFS 6000 Series Filter Resource Limits .....	168
Custom Offset Filters .....	169
Match Filter .....	170
Filter Masks .....	170



Custom Offset Filters for PFS 503x/703x-32X, PFS 5031/7031-56X, and 5030/7030-54X .....	171
PFS 503x/703x Custom Offset Tokens and Offsets .....	172
PFS 503x/703x Custom Offset Error Handling .....	173
Custom Offset Filters for PFS 504x/704x-32D .....	174
PFS 504x/704x Custom Offset Tokens and Offsets .....	174
Filtering on Packets with Multiple VLAN Tags .....	176
Local Destination .....	177
Remote Destination over pfsMesh .....	177
Inline Tool Chains .....	178
Traffic Load Balancing .....	179
Load Balance Criteria .....	180
Load Balance Groups and Failover Actions .....	181
About Load Balancing and Filtering .....	182
Load Balance Weighted Calculation .....	183
Load Balancing Workflow .....	183
Define Load Balance Criteria .....	183
Create Load Balance Groups with Ports .....	185
Create Load Balance Groups with Tunnels .....	188
Delete Load Balance Groups .....	190
Load Balancing Considerations .....	191
Load Balance Criteria .....	191
Load Balancing with Span-Monitor Ports .....	191
Load Balancing with Custom Hash .....	192
Trigger Policies .....	193
Trigger Type Settings .....	193
Link State Triggers .....	193
Health Check Triggers .....	194
Overflow Drop Triggers .....	195
Bandwidth Utilization Triggers .....	195
Combination ("Combo") Triggers .....	196
PPS Threshold Triggers .....	197
Trigger Timer Settings .....	198
Port Selection .....	198
Port Selection .....	198
Port Group Selection .....	199
Trigger Actions .....	199
pfsMesh Option .....	200
Trigger Status and Nodes with Conflict .....	201
Configuring Trigger Policies .....	201
Source Port VLAN Tagging .....	203
Ingress Port VLAN IDs .....	203
VLAN Tag Format .....	204



Override the System Default Ingress VLAN ID on an Ingress Port .....	204
Configure a Port to Add VLAN Tags to Egress Packets .....	205
Change the Default TPID or Starting VLAN ID .....	206
IP Tunnel Termination .....	206
Create Tunnel Termination Group .....	207
Assign a Tunnel Termination Group to a Port .....	208
Delete a Tunnel Termination Group .....	209
Tunnel Termination Considerations and Limitations .....	209
pfsMesh .....	210
pStack Technology .....	211
pfsMesh pStack Protocol Requirements .....	211
pfsMesh Topology .....	212
pStack Optimal Path Forwarding .....	213
pStack Load Spreading in a pfsMesh .....	214
Technical Considerations for Load Spreading .....	215
Configuring a pfsMesh Using pStack .....	215
Configure pStack Port Settings .....	215
Configure Monitor Output with a pfsMesh .....	216
Using the pfsMesh Page (pStack) .....	221
Topology .....	221
Remote Monitor Groups .....	221
Remote Trigger .....	222
pStack Map .....	222
VLAN .....	223
<b>5 Enhanced Port Features .....</b>	<b>225</b>
PFS 5000/7000 Enhanced Port Features .....	225
Standard Stripping .....	225
Standard Stripping Port Class Compatibility .....	227
Configure Standard VLAN Tag Stripping (Ingress) .....	228
Configure Standard Egress VLAN Tag Stripping .....	228
Configure Standard Vn Tag Stripping .....	229
Configure Standard VXLAN Stripping .....	230
Configure Standard MPLS Stripping .....	232
Configure Standard L2GRE Stripping .....	238
Inline Monitor Egress VLAN Stripping .....	240
Configure an Egress VLAN Action Group .....	240
PFS 7000 Timestamping .....	241
Time Stamp Details .....	241
Time Stamp Example .....	242
Enable Time Stamping .....	242
L2GRE Tunnel Origination/Termination Support .....	243



Configuring L2GRE Tunnel Origination/Termination .....	243
Use Case 1 - L2GRE Tunnel between Two PFS 7000 Devices .....	244
Use Case 2 - L2GRE Tunnel from PFS to vSTREAMs .....	251
L2GRE Tunnel Statistics and Status .....	255
L2GRE Origination/Termination Limitations .....	259
VXLAN Tunnel Origination/Termination Support .....	260
Configuring VXLAN Tunnel Origination/Termination .....	260
VXLAN Tunnel Origination/Termination Limitations .....	269
Neighbor Discovery Using LLDP .....	270
LLDP Ethernet Frame Structure .....	271
Enabling LLDP Packet Transmit/Receive .....	273
Viewing PFS LLDP Neighbors .....	273
pfsMesh Using pStack+ .....	274
pStack+ Technology .....	274
pStack+ Topology .....	275
pStack and pStack+ Compatibility .....	276
pStack+ Optimal Path Forwarding .....	277
pStack+ Limitations .....	277
Configuring a pfsMesh Using pStack+ .....	278
Using the pfsMesh Page (pStack+) .....	280
pfsMesh Configuration Example Using pStack+ .....	282
Port Mirroring and Packet Slicing .....	291
Port Mirroring .....	291
Packet Slicing .....	293
Port Mirroring and Packet Slicing Use Case .....	294
Port Mirroring and Packet Slicing Limitations and Considerations .....	296
PFS 6000 Enhanced Port Features .....	297
Packet Deduplication .....	297
Enable Packet De-duplication .....	299
Port and Time Stamping .....	300
Port Stamping .....	300
Time Stamping .....	301
About Time Stamp Synchronization Sources .....	302
About Time Stamp Accuracy .....	303
Using Port Stamping and Time Stamping Together .....	303
Protocol De-encapsulation and Stripping .....	304
ERSPAN, GRE, GTP, MPLS-L2, and NVGRE De-encapsulation .....	304
MPLS-L3, VLAN and VN Tag Stripping .....	304
Protocol Stripping .....	305
Stripping and De-encapsulation Details .....	305
Protocol Stripping Configuration .....	308
VLAN and VN Tag Stripping .....	313
Conditional Packet Slicing .....	315
About Conditional Slicing and Packet Sizes .....	316



Conditional Packet Masking .....	319
Configure Conditional Masking .....	320
Extended Load Balancing .....	324
Extended Load Balancing Workflow .....	324
Extended Load Balancing Considerations .....	327
<b>6 Inline Traffic .....</b>	<b>328</b>
Tool Chain - Simple Mode vs. Advanced Mode .....	329
Inline Traffic Workflow .....	329
Simple Tool Chaining .....	330
Simple Tool Chain Use Case .....	330
Prerequisites .....	331
Create a Simple Tool Chain .....	334
Simple Tool Chain with Source Port VLAN Forwarding .....	335
Simple Tool Chain with Source Port VLAN Forwarding Use Case .....	335
Advanced Tool Chaining .....	336
Advanced Tool Chain Use Case .....	337
Prerequisites .....	337
Create an Advanced Tool Chain .....	340
Inline Traffic Maps .....	343
Create an Inline Monitor Traffic Map .....	344
Tool Chain Resource Limits and Considerations .....	345
LinkSafe .....	346
About interconnected LinkSafe ports .....	348
Health Check Profiles .....	348
Health Check Configuration Parameters .....	349
Transmit Rate .....	349
Destination MAC Address .....	349
Payload .....	350
Filter Expression .....	350
Wait Time .....	350
Health Check Considerations .....	350
Create a Health Check .....	350
Delete Health Checks .....	351
PowerSafe .....	352
External PowerSafe TAP 3296 Components .....	352
Understanding PowerSafe .....	353
Normal Operation .....	353
Heartbeat Failure Using Poweroff Bypass Mode (Default) .....	354
Power Failure Using Poweroff Forward Mode .....	355
Heartbeat Failure Using Poweroff Block Mode .....	356



Heartbeat Failure Using Poweroff Inpairdown Mode .....	356
Enabling the PowerSafe Feature .....	357
Viewing PowerSafe Hardware Details .....	357
Configuring PowerSafe Settings .....	358
Poweroff Mode .....	359
PowerSafe Manual Mode .....	359
PowerSafe Inline Network Port Group Settings .....	360
PowerSafe Trigger Mode .....	360
PowerSafe Operation Status .....	361
Operational State .....	361
Fiber Pair State .....	362
Use Case: Using PowerSafe Trigger Mode with Inline Network Ports .....	362
<b>7 PFOS Maintenance .....</b>	<b>365</b>
Uploading Files .....	365
Downloading Files .....	366
Saving and Loading Configurations .....	368
Save a Configuration File .....	368
Load a Configuration File Stored on PFOS .....	369
Save the Running Configuration to Startup Configuration .....	369
Maintaining Core Files .....	369
Maintaining Log Files .....	370
Maintaining Certificate Files .....	371
Installing Certificates and Keys .....	373
Upload a Certificate, Key, or CRL File .....	373
View, Install, or Delete Certificate Files .....	374
Certificate Limitations and Configuration Considerations .....	375
Maintaining SSH Public Key Files .....	375
Maintaining NTP Key Files .....	376
NTP Key File Format .....	377
Upload an NTP Key File .....	377
Maintaining SSH Knownhost .....	377
Strict Host Key Checking .....	377
Upload an SSH Known Host File .....	378
Upgrading PFOS .....	379
Rebooting PFOS .....	379
Managing Redundancy .....	379
Configure Management IP Addresses .....	380
Switch Current Management Module .....	381
Uploading Files to Each Management Module .....	381



View Management Module Status .....	382
Front Panel LCD Screen .....	382
Management Module Status LED .....	383
In the Web UI .....	383
About Licensing and Redundancy .....	384
Redundancy Considerations and Limitations .....	384
<b>8 PFOS Diagnostics .....</b>	<b>385</b>
System Status .....	385
Statistics .....	386
Network Statistics .....	387
Deduplication Statistics .....	389
Flow Statistics .....	389
Control Packets Statistics .....	391
Tunnel Statistics .....	392
Port Group Statistics .....	393
Event Notifications .....	394
Syslog History .....	394
Alarms .....	395
Hardware Information .....	396
SNMP MIBs .....	398
SNMP Configuration Support .....	399
nGeniusONE PFS Monitoring .....	400
Consolidated Traffic Monitor .....	400
Grid .....	400
PFS Monitor .....	401
Syslog Messages .....	401
User .....	401
Configuration .....	402
Chassis .....	408
<b>A PFOS Packet Fields in Filter Expressions .....</b>	<b>412</b>
<b>B Configuring SNMP for PFOS .....</b>	<b>418</b>
Configuring SNMPv1 or SNMPv2c .....	418
Enable SNMP and Configure SNMP Versions .....	419
Create a New SNMP Community (Optional) .....	419
Add Security Name to View-Based Access Control Model (Optional) .....	419
Grant Access Rights to the VACM Group .....	420
Add New Security Models .....	421
Verify SNMP Configuration .....	422
Limit SNMP Access Rights .....	423



Verify SNMPSet by Using the New Access Configuration .....	424
Configuring SNMPv3 .....	424
Create a User-Based Security Model (USM) with Authentication and Privacy .....	425
Add the USM User to VACM Group .....	425
Verify Using New USM User “v3user” without Password .....	426
Request Authentication and Privacy Password for USM .....	426
Verify Using New USM User “v3user” without Password .....	427
Limit Access Rights for SNMPSet .....	428
Verify SNMPSet by Using the New Access Configuration .....	429
Configuring SNMP Notification (Traps) .....	429
SNMP Notify Tags .....	430
Add Trap Receiver IP Address to Target Table .....	430
SNMP v2c Receiver Example .....	431
SNMP v3 Receiver Example .....	431
Enable SNMP Traps .....	432
Notifications>SNMP>Traps .....	432
Notifications>Events .....	433
Verify SNMP v2c Trap is Received by Third-Party SNMP Trap Receiver .....	434
<b>C SNMP MIB and Trap Definitions .....</b>	<b>435</b>
Traps/Notifications .....	435
Interfaces MIB Traps .....	435
VSS Enterprise MIB Traps .....	436
SNMPv2-MIB Traps .....	442
Packet/Port Statistics .....	442
Interfaces MIB Stats .....	442
ifNumber .....	442
ifTable .....	443
ifXTable .....	444
RMON-MIB (RFC 2819) .....	445
etherStatsTable .....	445
HC-RMON-MIB (RFC 3273) .....	447
etherStatsHighCapacityTable .....	447
System Information .....	449
Community MIB .....	449
RFC 3584 .....	449
View-based Access Control Model (VACM) MIB .....	450
RFC 3415 .....	450
User-based Security Model (USM) MIB .....	452
RFC 3414 .....	452
Target MIB .....	454
RFC 3413 .....	454



Notification MIB .....	455
RFC 3413 .....	455
SNMPv2-MIB .....	455
RFC 3418 .....	455
NTCT-PFS-HEALTH-MIB .....	456
VSS-SYSTEM-MIB .....	467
<b>D PFS+PFX Inner Filtering and Inner Load Balancing .....</b>	<b>471</b>
PFS+PFX Inner Filtering .....	472
PFX+PFS Inner Filtering Configuration Workflow .....	473
PFX+PFS Inner Filtering Configuration Example .....	474
PFS+PFX Inner Load Balancing .....	479
PFX+PFS Inner Load Balancing Configuration Workflow .....	480
PFX+PFS Inner Load Balancing Configuration Example .....	481
PFOS/PFX Inner Filtering and Inner Load Balancing Known Limitations .....	485

## PFOS User Guide 6.5.1 Revision History

Date	Revision	Description
June 2024	PFOS 6.5.1 Rev A	<p><b>PFOS 6.5.1</b></p> <ul style="list-style-type: none"> <li>PFS 503x devices now support GRE-ERSPAN custom offset filters. Refer to <a href="#">Custom Offset Filters for PFS 503x/703x-32X, PFS 5031/7031-56X, and 5030/7030-54X</a>.</li> </ul> <p><b>Documentation Updates</b></p> <ul style="list-style-type: none"> <li>Updated <a href="#">Port Mirroring and Packet Slicing</a> with examples and use cases.</li> </ul>
April 2024	PFOS 6.5.0 Rev A	<p><b>PFOS 6.5.0</b></p> <ul style="list-style-type: none"> <li>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: <ul style="list-style-type: none"> <li><b>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 <a href="#">pfsMesh pStack Protocol Requirements</a> for additional pfsMesh compatibility details.</b></li> <li>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 user-configured VNIDs for <a href="#">VXLAN tunnels</a> and <a href="#">VXLAN stripping</a> is 8388607.</li> </ul> </li> <li>A new <a href="#">Tx Laser</a> setting on the Port Settings page enables users to disable the transceiver transmitter on PFS 5000/7000 ports.</li> <li>PFOS now supports <a href="#">Port Mirroring and Packet Slicing</a> on PFS 7000 devices.</li> <li>PFOS provides a new option <a href="#">Source Port VLAN Forwarding</a> for the Simple Tool Chain mode.</li> </ul>



April 2024	PFOS 6.5.0 Rev A	<p><b>PFOS 6.5.0 (Continued)</b></p> <ul style="list-style-type: none"><li>PFOS has enhanced several GUIs to provide more detailed PFS 5000/7000 power usage information:<ul style="list-style-type: none"><li>The <a href="#">Hardware&gt;Power Supplies GUI</a> has been updated to include more information.</li><li>The <a href="#">System Status&gt;System Information GUI</a> and the <a href="#">Hardware&gt;State GUI</a> have new Energy Consumption and Power Consumption fields.</li></ul></li></ul> <p><b>Documentation Updates</b></p> <ul style="list-style-type: none"><li>All references to the PFS 5130-128X device have been removed from PFOS documentation.</li></ul>
------------	---------------------	---

# 1 PFOS User Guide 6.5.1 Introduction

This document describes the system software and graphical user interface of the NETSCOUT Packet Flow Operating Software (PFOS).

Refer to the following sections for more information:

- [Audience](#)
- [Related Documentation](#)
- [Applicable Hardware Systems](#)
- [PFOS Licensing](#)
- [Related NETSCOUT Products](#)
- [Hardware Feature Cross-reference](#)
- [Network Access to 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 PFOS.

## Related Documentation

The following documents provide additional information about PFOS 6.x. All of the documents are downloadable at [my.netscout.com](http://my.netscout.com).

- **PFOS 6.x CLI Reference Guide:** Describes the command line interface (CLI) and includes reference pages for all of the commands.
- **PFOS 6.x NETCONF XML API Reference Guide:** Describes the NETCONF XML application programming 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](http://my.netscout.com).



## Applicable Hardware Systems

### PFOS on NETSCOUT Hardware

PFOS 6.x runs on the following NETSCOUT 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 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](http://my.netscout.com).

Refer to the [Hardware Feature Cross-reference](#) for a listing of hardware support per feature.

### PFOS on Certified Hardware

PFOS 6.x runs on Certified hardware available from NETSCOUT resellers. Refer to [PFOS Licensing](#) 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 and is 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 PFS 7000 feature functionality. Refer to [PFOS Licensing](#) licensing details.

Vendor Model	NETSCOUT Model Numbers	
	PFS 5000 Series	PFS 7000 Series
Edgecore Networks AS5812-54X	PFS 5010 PFS 5010-16X <sup>1</sup>	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 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



Vendor Model	NETSCOUT Model Numbers	
	PFS 5000 Series	PFS 7000 Series
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

<sup>1</sup> The PFS 5010-16X provides a 16-port capacity license option that enables only the first 16 ports to be configurable and used for application; the remaining ports will be disabled.

PFOS must be purchased from NETSCOUT to obtain a copy of the software and generate License Keys for Full PFOS Support; refer to [PFOS Licensing](#) for licensing details. For installation details for Qualified hardware, refer to the *PFOS Installation Guide for Qualified PFS Devices*. For more information about supported third-party qualified hardware, contact your NETSCOUT representative.

See also:

- [PFS 5121/7121-64X Limitations and Configuration Considerations](#)
- [PFS 503x/703x-32X, 5031/7031-56X, and 5030/7030-54X Limitations and Configuration Considerations](#)
- [PFS 5040/7040-32D and 5041/7041-32D Limitations and Configuration Considerations](#)

## PFOS Licensing

The following table describes available licensing.

License	License Options	Description
<b>Support License (PFS 5000)</b>	<b>Full</b>	Enables full PFOS 5000 <a href="#">base feature</a> functionality, subject to the normal constraints of the hardware on which it is running, until the license expiration date. When a Full License expires, further installation of PFOS software is disabled, but you still can perform all other functions and configuration. <b>Note:</b> The PFS 5010-16X provides a 16-port capacity license option that enables only the first 16 ports to be configurable and used for application; the remaining ports will be disabled.
	<b>Trial</b>	Enables PFOS base feature functionality for 90 days. Upon expiration, <b>PFOS automatically clears its configuration</b> and no further configuration or software upgrades can be performed until a Full Support License is installed. PFOS 5000 Trial Licenses may be used on NETSCOUT Evaluation hardware. Installation of PFOS software is only allowed if the build date of the image is before the license expiration date.



License	License Options	Description
<b>PFS 7000 License</b>	<b>Full</b>	<p>Enables full PFS 7000 functionality including:</p> <ul style="list-style-type: none"><li>• <a href="#">MPLS Stripping</a></li><li>• <a href="#">L2GRE Stripping</a></li><li>• <a href="#">Inline Tool Chain</a></li><li>• <a href="#">External PowerSafe TAP Configuration</a></li><li>• <a href="#">L2GRE Tunnel Origination/Termination Support</a></li><li>• <a href="#">VXLAN Tunnel Origination/Termination Support</a></li><li>• <a href="#">Timestamping (only supported on certain models)</a></li><li>• <a href="#">Tunnel Load Balancing</a></li><li>• <a href="#">Inner Header Load Balancing (PFS 7040-32D and 7041-32D)</a></li><li>• <a href="#">Neighbor Discovery Using LLDP</a></li><li>• <a href="#">pfsMesh Using pStack+</a></li><li>• <a href="#">Inline Monitor Egress VLAN Stripping</a></li><li>• <a href="#">Port Mirroring and Packet Slicing</a></li></ul> <p>PFOS 7000 functionality is subject to the normal constraints of the hardware on which it is running, until the license expiration date.</p>
	<b>Trial</b>	<p>Enables <i>advanced</i> PFOS functionality for 90 days. Upon expiration or deletion, <b>PFOS automatically clears any advanced feature configuration</b>; standard configuration is not cleared. No further configuration of advanced features can be performed until a Full Advanced license is installed.</p>

The following table lists the type and expiration of licenses that come with (or are automatically installed on) various NETSCOUT PFS.

Applicable Hardware Systems	License		
	PFOS pre-installed?	Type	Expiration
PFS 6000-series Appliances purchased from NETSCOUT	Yes	Full	Permanent
PFS 5000-series Appliances purchased from NETSCOUT	Yes	Full	Permanent
PFS 7000-series Appliances purchased from NETSCOUT	Yes	Full	Permanent
Certified switches	Yes	Trial <sup>(1)</sup>	90 days
Qualified switches	No	Trial <sup>(2)</sup>	90 days

#### Notes:

(1) Certified PFS 5000s and 7000s are pre-installed with Trial Support and PFS 7000 licenses. Customers must acquire and install Full 5000 and optional 7000 licenses in order to maintain PFOS functionality.

(2) Trial Support and PFS 7000 licenses are automatically installed upon PFOS installation on Qualified PFS. Customers must acquire and install Full 5000 and optional 7000 licenses in order to maintain PFOS functionality.



## Licensing for Applicable Hardware Systems

**PFS 5000 Appliances** shipped from NETSCOUT include Full Support licenses.

**PFS 7000 Appliances** shipped from NETSCOUT include Full Support and PFS 7000 licenses.

**NETSCOUT Certified PFS** come with PFOS pre-installed. Certified PFS include Trial Support and PFS 7000 licenses that are valid for 90 days.

**Eligible Qualified PFS** come without PFOS pre-installed. Upon installation PFOS will automatically install Trial Support and PFS 7000 licenses that are valid for 90 days.

## License Status

In the Web UI, the current license status displays in the header of the System Status page. The Platform field will display the appropriate PFS 5000 or PFS 7000 model number.

System Status					
System Information					
Name: SW-189	Location: Sunnyvale, CA USA	Mgmt-1: active	Data Disk Usage: 59%	System Status: OK	
Product ID: 2301	Contact: tsupport@vssmonitoring.com	Mgmt-2: standby	System Disk Usage: 11%	Temperature: 44 °C	
Serial Number: 14100444	Support License: <b>Current</b>	Platform: PFS6010	Redundancy Status: ready		

To view all of the licenses that are installed on a system, go to the License section of the File Management page (Full License examples shown below):

License							
Name	Description	Type	State	Expiration Date	Mac Address	Ports	
Support	Supports base features and upgrades	full	current	Permanent	8c:ea:1b:ff:bb:a4	all	
PFS 7000	Supports PFS 7000 features	full	current	-	8c:ea:1b:ff:bb:a4	all	
Showing 1 to 2 of 2							

The following graphic shows an example of 16-port limited capacity licensing for the PFS 5010-16X.

License							
Name	Description	Type	State	Expiration Date	Mac Address	Ports	
Support	Supports base features and upgrades	full	current	Nov 2020	8c:ea:1b:26:76:09	16-ports	
Showing 1 to 1 of 1							

## License Notifications

When the PFS 5000/7000 Full License is scheduled to expire within 30 days, or if a Trial License is in use, PFOS sends a Syslog notification every night at midnight (system clock time) warning about the license expiration date. For more information on Syslog notifications, refer to [Syslog Messages](#).



## Retrieving New or Renewal Full License Keys

If multiple License Keys are loaded on a system, the License Key with the latest expiration date will be in effect.

### PFS 5000/7000 and PFS 6000 Appliances purchased from NETSCOUT

To renew a Full Support license, contact NETSCOUT Technical Support by opening a case at [my.netscout.com](http://my.netscout.com) or call +1-888-357-7667 (US) or +800 4764 3337 (outside US) for assistance; you will need the MAC address of the hardware plus its NETSCOUT hardware serial number.

If you have purchased a PFS 7000 Add-On to add PFS 7000 functionality to an existing PFS 5000 device, log on to the MasterCare portal to retrieve the PFS 7000 license. You will need the MAC address of the hardware and the software Serial Number (provided on your software Order Fulfillment Acknowledgment).

### Certified and Qualified Switches

When PFOS is purchased it includes a Full Support license and, if PFOS for a 7000-series PFS is purchased, a Full PFS 7000 license. To retrieve the license(s), log on to the MasterCare portal; you will need the MAC address of the hardware plus the software Serial Number provided on the software Order Fulfillment.

To renew a Full Support license, contact NETSCOUT Technical Support by opening a case at [my.netscout.com](http://my.netscout.com) or call +1-888-357-7667 (US) or +800 4764 3337 (outside US) for assistance; you will need the MAC address of the hardware plus its NETSCOUT hardware serial number.

If you have purchased a PFS 7000 Add-On to add PFS 7000 functionality to an existing Certified or Qualified PFS 5000 device, log on to the MasterCare portal to retrieve the PFS 7000 license. You will need the MAC address of the hardware and the software Serial Number (provided on your software Order Fulfillment Acknowledgment).

## License File Format

A license file has one or more lines of this format:

```
mac-address license-key
```

where mac-address is the MAC address of the chassis on which the license will run, and license-key is the encoded hexadecimal license key for that system. For example:

```
c4:ee:ae:01:f1:a9
0229dd88b85f4af37b8a9bdbb865a40e6174f48dfc2661ea87e51e4fc74ccf53
cc:37:ab:bd:46:67
ed7d215ba04df4a38340d92daf9d5f4a626d07a1cfdf8320a56e88769320dee
```

You can use either spaces or tabs to separate the two fields.

License keys are generated by the MasterCare portal or Customer Support and are usually sent via email.



A license file can contain multiple lines. When reading a license file, PFOS uses the line with the MAC address of the hardware on which it is running. This means that, if you wish, you can combine all of your PFOS licenses into one file and copy that file to all of your PFOS systems.

If a license file contains more than one entry for the same MAC address, PFOS uses the entry that has the latest expiration date.

To view the MAC address of a PFOS system, go to the **System Administration > Hardware > State** page or use the `show mac-address` CLI command.

## Installing a New License File

To install a new license file, you must first upload the file to PFOS, and then you must install it. This section describes how to install a new license file using the Web UI. For information on using the CLI to manage license files, refer to the *PFOS 6.x CLI Reference Guide*.

**Important: If a PFS 5000/7000 Series or third-party hardware system loses power for more than a few seconds, its system clock resets to 2001-01-01. To avoid having to reset the system clock and ensure more accurate and reliable time, you can set up an [NTP server](#). Prior to upload, verify your system time is accurate, or your license upload will fail.**

### Upload License File

1. On the File Management page, if this system has more than one management module installed, click the tab to select the desired management module.
2. On the File Management page, scroll down to the **Upload File to Chassis** section.
3. In the drop-down list, select **License**.
4. Click **Select files**.

The screenshot shows a user interface for uploading files to a chassis. At the top, there is a heading 'Upload File to Chassis'. Below it, a dropdown menu is open, with the word 'License' circled in red. To the right of the dropdown is a blue button labeled 'Select files...', also circled in red. The overall background is white, and the text is in a standard sans-serif font.

5. Select the license file that you want to upload. If the license file contains at least one entry for the MAC address of this system, then the filename appears in the list in the License section.

The License file will be automatically installed after upload.

## Deleting a License File

PFOS users with Delete privileges for File Management can delete PFS 7000 trial licenses.

1. On the File Management page, if this system has more than one management module installed, click the tab to select the desired management module.
2. On the File Management page, scroll down to the **License** section.



License							
Name	Description	Type	State	Expiration Date	Mac Address	Ports	
Support	Supports base features and upgrades	trial	current	Trial license is valid for 74 days only	a8:2b:b5:9d:b7:c5	all	
PFS 7000	Supports PFS 7000 features	trial	current	Trial license is valid for 74 days only	a8:2b:b5:9d:b7:c5	all	
Showing 1 to 2 of 2							

3. In the Name column, select the PFS 7000 trial license you want to delete. A page appears with license details.

## PFS 7000

Description	Supports PFS 7000 features	Type	trial	State	current
Expiry Date	Trial license is valid for 74 days only	MAC Address	a8:2b:b5:9d:b7:c5		
<a href="#">Delete</a>					

4. Click **Delete** to delete the file.

## 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.



## Hardware Feature Cross-reference

The following table shows which PFOS 6.x features are available on each hardware platform.

**Table 1.1 - PFOS 6.x Hardware Feature Cross-Reference**

Feature		PFS 5000 Series	PFS 7000 Series	PFS 6000 Series
Management interfaces	Web UI	Yes	Yes	Yes
	CLI	Yes	Yes	Yes
	SNMP	Yes	Yes	Yes
	NETCONF API	Yes	Yes	Yes
	RESTCONF API	Yes	Yes	Yes
	Syslog	Yes	Yes	Yes
Load balancing	Flow-aware L2-L4 load balancing	Yes	Yes	Yes
	Encapsulated (inner L2-L4) load balancing	No	Yes <sup>3</sup>	Yes <sup>1</sup>
	Custom Hash	Yes <sup>2,3</sup>	Yes	No
	Round Robin	Yes <sup>4</sup>	Yes <sup>4</sup>	No
	Failover actions: Rebalance, redistribute, drop	Yes	Yes	Yes
	Failover actions: Weighted	Yes	Yes	No
	Tunnel	No	Yes <sup>3</sup>	Yes
Traffic filtering	Inner Load Balancing	Yes <sup>5</sup>	Yes <sup>5</sup>	No
	L2-L4 filters	Yes	Yes	Yes
	Custom offset/user-defined filters	Yes	Yes	Yes
	Filter service ports	Yes	Yes	Yes
	Inner Filtering	Yes <sup>5</sup>	Yes <sup>5</sup>	No
	Aggregation	Yes	Yes	Yes
	Extended microburst protection (HDBB)	No	No	Yes
	Deduplication	Yes <sup>5</sup>	Yes <sup>5</sup>	Yes <sup>1</sup>
	IP tunnel termination <sup>6</sup>	Yes	Yes	Yes
	NetFlow generation	Yes <sup>5</sup>	Yes <sup>5</sup>	Yes <sup>5</sup>

**Table 1.1 - PFOS 6.x Hardware Feature Cross-Reference (continued)**

Feature		PFS 5000 Series	PFS 7000 Series	PFS 6000 Series
Packet modification	Generic Protocol stripping / de-encapsulation	Yes <sup>5</sup>	Yes <sup>5</sup>	Yes <sup>1</sup>
	Payload modification: Conditional slicing, Conditional masking	Yes <sup>5</sup>	Yes <sup>5</sup>	Yes <sup>1</sup>
	Port stamping	No	No	Yes <sup>1</sup>
	Time stamping	No	Yes <sup>8</sup>	Yes <sup>1</sup>
	Ingress VLAN tag, VN-tag, and VXLAN stripping	Yes <sup>2,3</sup>	Yes <sup>2,3</sup>	Yes <sup>1</sup>
	Egress VLAN tag stripping	Yes <sup>2,3</sup>	Yes <sup>2,3</sup>	No
	Inline Monitor Egress VLAN Stripping	No	Yes <sup>3</sup>	No
	MPLS stripping	No	Yes <sup>3</sup>	Yes <sup>1</sup>
	L2GRE stripping	No	Yes <sup>3</sup>	Yes <sup>1</sup>
	VLAN Tagging	Yes	Yes	Yes <sup>1</sup>
	Inline traffic and tool chains	No	Yes	Yes
	External PowerSafe TAP (EPT)	No	Yes	No <sup>8</sup>
	Neighbor Discovery Using LLDP	No	Yes	No
	L2GRE Encapsulation/ Decapsulation (Tunnel origination/termination)	No	Yes <sup>3</sup>	No
	VXLAN Encapsulation/ Decapsulation (Tunnel origination/termination)	No	Yes	No
	Port Mirroring (all PFS 7000s) and Packet Slicing ( PFS 703x and PFS 704x devices only) <sup>2,3</sup>	No	Yes	No
	Clock Sources	Local clock	Yes	Yes
	NTP	Yes	Yes	Yes
	GPS	No	No	Yes
	PTP	No	No	Yes
	Linux PTP	Yes	Yes	No
	Locator LED	Yes	Yes	Yes
	LCD display	No	No	Yes
pfsMesh (pStack)	pfsMesh (pStack)	Yes	Yes	Yes
	pfsMesh (pStack+)	No	Yes <sup>3</sup>	No

**Notes:**

1. Available on systems with one or more 40SadvR line cards.
2. The PFS 5031/7031-56X, PFS 503x/703x-32X, and 5030/7030-54X devices provide limited support; refer to [PFS 503x/703x-32X, 5031/7031-56X, and 5030/7030-54X Limitations and Configuration Considerations](#).



3. The PFS 504x-32D/704x-32D devices provide limited support; refer to [PFS 5040/7040-32D and 5041/7041-32D Limitations and Configuration Considerations](#).
4. [Round Robin load balancing](#) is not supported for PFS 5010/7010 or PFS 504x-32D/704x-32D devices.
5. Available with the use of PFX; refer to PFX documentation. For Inner Filtering and Inner Load Balancing, see also [PFS+PFX Inner Filtering and Inner Load Balancing](#).
6. Generic IP Tunnel Termination does not include header stripping or de-encapsulation, though this feature can be combined with the stripping capabilities of the PFS or PFX when necessary.
7. [Timestamping](#) is only available on PFS 7120, PFS 7121-64X, PFS 7031-56X, PFS 703x-32X, PFS 704x-32D, and the PFS 7030-54X devices.
8. Not supported on PFS 6010 or original revision of PFS 6002. Is supported on new revision of PFS 6002 only.

## PFS 5121/7121-64X Limitations and Configuration Considerations

- The PFS 5121/7121-64X system requires approximately 30 seconds to initialize each transceiver. While transceivers are being initialized, detection of transceiver and FRU (power supply and fan) insertions and removals will be delayed until the batch being initialized is finished. The following table shows the amount of time a fully loaded chassis requires to initialize all transceivers:

PFS Model	Approx. Time for Initialization per Transceiver	Approx. Time for Initialization of Fully Loaded Chassis
PFS 5121/7121-64X (64 ports)	30 seconds	30-32 minutes

- For PFS 5121/7121-64X, the [Tunnel feature](#) is always enabled; therefore, this option is not shown to users.
- The PFS 5121/7121-64X has limited port breakout capability on certain ports; refer to [PFS 5121/7121-64X Port Breakout Limitations](#) for details.

## PFS 503x/703x-32X, 5031/7031-56X, and 5030/7030-54X Limitations and Configuration Considerations

- The PFS 5031/7031-32X system requires approximately 30 seconds to initialize each transceiver while the PFS 5031/7031-56X requires approximately 15 seconds to initialize each transceiver. While transceivers are being initialized, detection of transceiver and FRU (power supply and fan) insertions and removals will be delayed until the batch being initialized is finished. The following table shows the amount of time a fully loaded chassis requires to initialize all transceivers:



PFS Model	Approx. Time for Initialization per Transceiver	Approx. Time for Initialization of Fully Loaded Chassis
PFS 5031/7031-32X (32 ports)	30 seconds	14-16 minutes
PFS 5031/7031-56X (56 ports)	15 seconds	11-14 minutes

- Ports

- For PFS 5031/7031-56X, there is one physical port for ports 49-50 and one physical port for ports 51-52. These ports support both QSFP28-DD or QSFP28 transceivers. If QSFP28 is used, only one port in each port pair appears as link up in WebUI: port 49 for ports 49-50, and port 52 for ports 51-52 as shown in the following graphic.

<b>One physical port for 49-50</b>		100000 49 FINISAR CORP FTLC9551REPM 100GBase-SR4 -0.62 -0.25	100000 53 FINISAR CORP FTLC9551REPM 100GBase-SR4 -0.63 -0.25
<b>One physical port for 51-52</b>		100000 57 FINISAR CORP FTLC9551REPM 100GBase-SR4 -0.76 -0.35	100000 61 FINISAR CORP FTLC9551REPM 100GBase-SR4 -0.76 -0.34

- PFS 5031/7031-56Xs do not support 100G-DR1, 100G-FR1, and 100G-LR1 transceivers in the QSPF28-DD ports (ports 49-50 and 51-52).
- PFS 5031/7031-56Xs support SFP28, SFP+, and SFP transceivers in ports 1-1 to 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 1-1 (for example, ports 1-1 to 1-4 must all have the same speed). On the Port Settings page, 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).
- PFS 5030-32X/7030-32X and 5031-32X/7031-32X devices support [4x1G port breakout](#).
- 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.
- The PFS 5030/7030-54X has limited port breakout capability on certain ports; refer to [PFS 5030-54X/7030-54X Port Breakout Limitations](#) for details.
- The PFS 503x/703x-32X, PFS 5031/7031-56X, and PFS 5030/7030-54X devices do not support [Vn Tag stripping](#) or [Egress VLAN Tag Stripping](#).
- The PFS 503x/703x-32X, PFS 5031/7031-56X, and PFS 5030/7030-54X devices do not support [Custom Hash for Load Balancing](#).
- PFS 503x/703x-32X, PFS 5031/7031-56X, and 5030/7030-54X devices require specific [Custom Offset Filter](#) configurations that are only compatible with PFS 503x/703x devices.
- For PFS 503x/703x-32X, 5031/7031-56X, and 5030/7030-54X devices, the [Tunnel feature](#) is always enabled; therefore, this option is not shown to users.
- The PFS 703x-32X, PFS 7031-56X, and PFS 7030-54X devices support the [Packet Slicing](#) feature, which requires the [Port Mirroring](#) feature and is part of the mirroring session configuration.



## PFS 5040/7040-32D and 5041/7041-32D Limitations and Configuration Considerations

- The PFS 5041/7041-32D system requires approximately 30 seconds to initialize each transceiver. While transceivers are being initialized, detection of transceiver and FRU (power supply and fan) insertions and removals will be delayed until the batch being initialized is finished. A fully loaded PFS 5041/7041-32D chassis requires approximately 14-16 minutes to initialize all transceivers.

PFS Model	Approx. Time for Initialization per Transceiver	Approx. Time for Initialization of Fully Loaded Chassis
PFS 5041/7041-32D (32 ports)	30 seconds	14-16 minutes

- VLAN Tagging: If enabled, packets egressing the PFS 5040/7040-32D and 5041/7041-32D devices will be tagged with the Default or "User-Defined" VLAN ID configured at [Source Port VLAN](#). However, if packets are from a remote device over pfsMesh and they egress at the PFS 5040/7040-32D and 5041/7041-32D, they will be tagged with the Default VLAN ID of the remote source port; the user-defined VLAN ID of remote source port will not be applied.
- [FEC](#) is always enabled for 400G for 5040/7040-32D and 5041/7041-32D devices.
- Traffic Filtering
  - [Map profile](#) is not configurable; only the Legacy mode can be supported (No SIP or DIP mode).
  - PFS 5040/7040-32D and 5041/7041-32D devices have similar Custom Offset Filters as the 503x/703x devices, although some differences exist. Refer to [Custom Offset Filters for PFS 504x/704x-32D](#) for a summary of these differences.
  - PFS 5040/7040-32D and 5041/7041-32D devices do not support masking of MAC addresses using the custom offset Header MAC option. PFS 5040/7040-32D and 5041/7041-32D devices only support masking to source/destination MAC addresses in the Filter Expression Builder. See [Traffic Filtering](#).
- For 5040/7040-32D and 5041/7041-32D devices, the [Tunnel feature](#) is always enabled; therefore, this option is not shown to users.



- Load Balancing
  - When configuring Load balancing with MPLS label, Source IP and Dest IP must be enabled together with MPLS LB Criteria to hash MPLS labels. PFS 5040/7040-32D and 5041/7041-32D devices will load balance using up to 7 MPLS labels (compared to 3 MPLS Labels in other devices). See [Load Balance Criteria](#).
  - The PFS 5040/7040-32D and 5041/7041-32D devices do not support [Custom Hash for Load Balancing](#).
  - The PFS 5040/7040-32D and 5041/7041-32D devices do not support [Tunnel Load Balancing](#).
  - The PFS 7040-32D and 7041-32D devices support additional inner header [Load Balance Criteria](#) for L2GRE, L3GRE, L3 MPLS, and VxLAN packets. Inner header criteria configuration is only supported for L2GRE, L3GRE, L3 MPLS, and VxLAN packets; existing load balance criteria is not affected.
  - The PFS 5040/7040-32D and 5041/7041-32D devices do not support [Round Robin load balancing](#).
- The PFS 5040/7040-32D and 5041/7041-32D devices do not support [Vn Tag Stripping](#) or [Egress VLAN Tag Stripping](#).
- The PFS 7040-32D and 7041-32D devices support the [Packet Slicing](#) feature, which is only supported as part of the [Port Mirroring](#) feature and is part of the mirroring session configuration. PFS 704x systems support an additional option to configure the slicing offset value; refer to [Hardware Feature Cross-reference](#) for details.
- The PFS 704x-32D devices do not support the following PFS 7000 functionality features:
  - [MPLS stripping](#)
  - [L2GRE Stripping](#)
  - [Inline Monitor Egress VLAN Stripping](#)
  - [L2GRE Tunnel Origination/Termination](#)
  - [VxLAN Tunnel UDP Source Port setting](#)
  - [VXLAN Tunnel Vlan Tagging setting](#)



## Network Access to PFOS

The following TCP and UDP ports are used by PFOS and should be accessible if the described interface is used. Several of these ports can be changed or disabled.

Protocol and Port	Description	Refer To:
TCP/22	PFOS CLI	<a href="#">Management Interfaces</a>
TCP/80	PFOS Web UI (HTTP – disabled by default)	
TCP/443	PFOS Web UI (HTTPS)	
TCP/832	NETCONF (SSH) interface (required by PFS Fabric Manager)	
TCP/443	RESTCONF (HTTPS) interface	
UDP/161	SNMP	
TCP/8443	PFS Monitor and PFS Fabric Manager access	<a href="#">PFOS Diagnostics</a> and the <i>PFS Fabric Manager Admin Guide</i> .
UDP/395	PFS Monitor and PFS Fabric Manager traps	

## 2 Managing with PFOS

This section provides information about managing PFOS.

- [Configuration File Types](#)
- [Management Interfaces](#)
- [Logging in to the Web UI](#)
- [Using the Web UI](#)
- [Configuration Task Flow](#)
- [Zero Touch Provisioning](#)

### Configuration File Types

Configuration changes are stored in the following configuration files:

- **Running configuration:** The set of configurations in running memory (RAM).
- **Startup configuration:** The file that contains the configurations that are loaded on boot up.
- **Saved configuration:** Configuration files saved on the hard drive and available to apply to the running configuration.

All changes to software parameters made using the Web UI or CLI are made to the running configuration. Any time the system is rebooted, the startup configuration – not the running configuration – is applied.

NETSCOUT strongly recommends that you copy the running configuration to the startup configuration prior to reboot if any changes have been made since the last reboot. For details on how to load PFOS configurations, see [Saving and Loading Configurations](#).

### Management Interfaces

The following management interfaces allow access to the PFS devices for configuration, monitoring and troubleshooting purposes. You can control access to these interfaces on the System>Features>[Access Management](#) page. See [Network Access to PFOS](#) for network port details.



## Command Line Interface (CLI)

A command-based user interface for configuring and managing PFS devices. You access the PFOS CLI through the serial console, over Ethernet using SSH, or by clicking the CLI button in the Web UI. See the *PFOS 6.x CLI Reference Guide* for details.

## Web UI

The web browser-based user interface described in this guide. See [Logging in to the Web UI](#) for access details.

## NETCONF API

An IETF-standard XML-based API to PFOS. See 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.



Online documentation appears in a Swagger UI. The Swagger UI provides an interactive API console for you to quickly learn about the RESTCONF API and experiment with requests.

A screenshot of the Swagger UI interface for the RESTCONF API. The top header says 'Swagger UI' and 'Select a definition' with 'access control' selected. Below the header, there's a detailed description of the 'access\_control\_m' module, including its version (PFOS swagger version 2021-11-06) and a note about the URL [ Base: 'http://127.0.0.1:8080/restconf '] and file '/pfos/access\_control\_m.json'. It also mentions that this module defines VSS access control data. The main area shows the API structure with sections for 'root', 'operations', and 'data'. Under 'root', there's a single 'GET' operation. Under 'operations', there's a single 'GET' operation. Under 'data', there are two operations: a 'GET' operation and a 'POST' operation, with the 'POST' operation being highlighted with a green background.



## Logging in to the Web UI

The PFOS Web UI is supported on recent versions of many popular web browsers. For an up-to-date list of supported browsers and versions, refer to the PFOS Release Notes that are distributed with each release of PFOS .

### Connect to the Web UI

1. Connect a CAT 3 (or higher) Ethernet cable between one of the management ports and a PC or server. We recommend that the cable length not exceed 10 feet (3 meters). If longer cable lengths are needed, use CAT 5 (or higher) shielded cable.
2. Power on the system. After power-on completes, the Link Status LED illuminates on the connected management Ethernet port.
3. Connect to PFOS by entering **https://** followed by the IP address of the device in the web browser's URL address box. The login page appears.



**Note:** At login, the Web UI displays either a default or custom text banner. See [Basic Information Settings](#) for details.

4. Enter **admin** for the username and **admin** for the password (or another username/password that you previously created).

**Note:** To specify a user account from a different domain, use the format **<domain>\<user>**. Note that two backslashes are used to ensure successful authentication.

5. Click **Sign in**.

**Note:** On systems with a front panel LCD, the IP address of the system is displayed on the LCD. If necessary, you can connect to the serial port first and then set the IP address.

## 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. In the Web UI, after changing the password, you will need to enter the admin login and new password again before proceeding.



## 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 Web UI, you can use the scrollbars in the browser window to scroll horizontally or vertically as desired to read the agreement, or you can print the agreement. After reading the agreement, click **Accept** or press Enter to accept, or click **Decline** 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 through RADIUS, TACACS, or LDAP, as long as that user is first granted the Admin role in PFOS.

## Using Secure (HTTPS) Web Browser Connections

By default, PFOS accepts web browser connections using FIPS-compliant secure and encrypted HTTPS.

**Note:** For fastest performance and responsiveness, use HTTP connections. For maximum security, use only HTTPS connections.

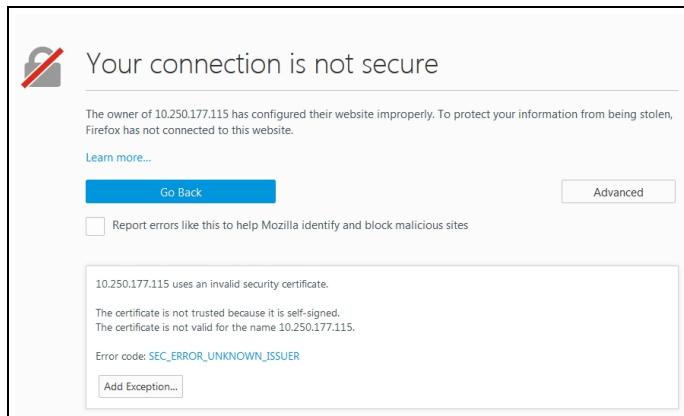
HTTPS uses the secure session layer (SSL) protocol to establish secure connections. The SSL implementation is based on transport layer security (TLS) version 1.2.

When an HTTPS connection is made, the web browser receives a digitally-signed certificate from the web server (in this case, the one running on PFOS), and the browser uses the certificate to verify that the web server you have connected to is the site and domain that it claims to be.

This mechanism causes some anomalies with applications that do not involve an actual website. Web browsers, as part of the authentication of the “website” to which the user has connected, insist that the domain name within the digitally-signed certificate must exactly match the domain name to which the user has connected – whatever was entered into the browser’s address bar.

But a managed device is not an actual website. In almost all cases, it does not have an actual domain name assigned to it. Therefore, the digital certificate returned by the system (which identifies itself with the domain www.netscout.com) does not match the URL that you entered into the browser’s address bar (the IP address of the system). As a result, the web browser displays a message that the certificate is incorrect. You must respond to such a message in a way that instructs the web browser to accept the certificate and proceed. (The exact message and how to respond varies by browser, but all browsers have an option that you can choose to proceed and accept the certificate.)

For example, in Firefox, the page is similar to the following:



To permanently accept the certificate for this session and future sessions, click **Advanced**, then click **Add Exception**, verify **Permanently store this exception** is selected, and click **Confirm Security Exception**.

In some other browsers, you might need to manually install the certificate. For more information, refer to the documentation for your web browser.

For information on how to configure PFOS to allow web browser connections via only HTTP, only HTTPS, or both HTTP and HTTPS, refer to [Management Interfaces](#).

To upload and manage the security certificates that PFOS uses, refer to [Maintaining Certificate Files](#).

## Failed Login Attempts

PFOS detects multiple failures to log in, and blocks access to the system when certain thresholds are met. You can [configure 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.

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

PFOS manages failed login attempts as described below:

- **User tries to log in with a local username that exists but with an incorrect password.** PFOS allows each user from each IP address to enter a valid password for the [configured number of failed attempts](#). After reaching the configured threshold of password failures, that username is locked out from all access and cannot log in for 60 minutes, even with the correct password. The counter resets after a valid password is entered. The failure counter is reset an hour after the first failed attempt occurs. PFOS generates a Syslog message when a login is blocked.

**Note:** When remote authentication is used, PFOS does not track invalid logins for each (remote) account; invalid login attempts by valid remote usernames are tracked only by IP address (see next bullet).



- **User tries to log in with a username that does not exist or a username from a remote AAA server.** PFOS allows a user to enter a valid username from a specific IP address for the [configured number of failed attempts](#). After reaching the configured threshold of invalid username attempts, that IP address is locked out from all access and cannot log in for 60 minutes, even with a valid username and password. The counter resets after a valid username and password are entered. The failure counter is reset an hour after the first failed attempt occurs. PFOS generates a Syslog message when a login is blocked.

You can view failed login attempts count and times and account lockout times on the [Users](#) and [Client IP Lockout](#) tabs in [Access Control](#).

## Password Policies

PFOS enforces system-wide [password policies](#) which include [password expiration](#) and [minimum password length and character requirements](#). If a user 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/RESTCONF API interfaces. 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.

Current password is not password policy compliant. Password update required. Password policy: \* Password length should be minimum 5 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.

Password

Enter new password

Confirm-Password

Re-enter new password

Cancel Submit

Passwords are encrypted and cannot be recovered if lost. If you forget your password, then an administrator must assign you a new password.



## Using the Web UI

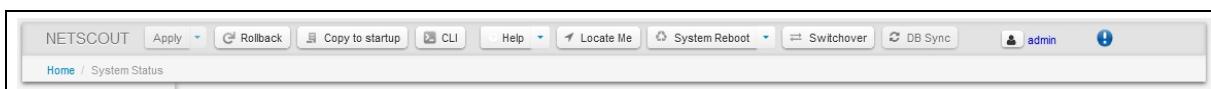
The Web UI contains the following areas:

- **Toolbar:** Perform system level actions, including saving configuration changes to the running configuration, copying the configuration to the startup configuration, rolling back a configuration, getting help, locating the system, rebooting, getting notification, and logging out. See [Toolbar Details](#).
- **Side Menu:** Access the status, configuration, and administration pages.
- **Main Panel:** View and configure content.

The screenshot shows the NETSCOUT System Status page. The Main Panel displays System Information for HW-LAB-DC-4, including Name, Location, Mgmt-1, Data Disk Usage, System Status, Product ID, Contact, Mgmt-2, System Disk Usage, Temperature, Serial Number, Support Licensee, Platform, Redundancy Status, and Energy Consumption. Below this is a table of modules with columns: ID, State, Time Left, Product ID, Configured Card, SKU/PN, Module Part Number, Module Revision Number, Module Serial Number, and PCBA Part Number. The Side Menu on the left lists categories like Status, Configuration, System Administration, and Monitoring.

## Toolbar Details

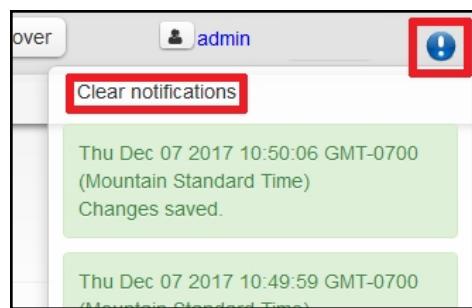
The toolbar is always visible. It provides access to the following configuration and system commands. The breadcrumb navigation just below the toolbar shows the current page.



- **Apply:** This button is activated when one or more configuration changes have been made using the Web UI. These changes are automatically stored only in the browser cache. Click this button to save the changes to the running configuration. The button is grayed out if there are no changes to save. If you log out before saving the changes to the running configuration, the changes are cleared from the browser cache and lost. These options are available if you have changes that are not yet applied:
  - **View changes:** Display a list of the changes to be applied.
  - **Validate changes:** Identify possible errors in changes to be committed.
  - **Cancel changes:** Remove the pending changes.



- **Rollback:** Each time configuration changes have been saved by clicking **Apply**, a rollback file is created containing the changes made since the last time they were saved. Clicking the Rollback button displays the list of rollback files from which you can choose one to view and load. 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 [Configuring Access Control](#)).
- **Copy to startup:** Copies all running configuration values to the stored startup configuration file.  
**Note:** NETSCOUT strongly recommends that you copy the running configuration to the startup configuration on a regular basis and before initiating a reboot.
- **CLI:** Launches the Command Line Interface (CLI) in a separate terminal window.
- **Help:** Opens a browser to My.NETSCOUT.com to provides access to user documentation for hardware and software.
- **Locate Me:** Varies depending on PFS model:
  - **PFS 5000/7000:** Turns on LOC indicator; LED color/behavior varies per model. Refer to *PFS 5000/7000 Series Packet Flow Switches Quick Connection Guide* for details.
  - **PFS 6000:** Flashes "Critical" Status indicator (RED).
- **System Reboot:** Initiates a software reboot sequence. Three options for the reboot are available:
  - **Reboot:** Reboot the system.
  - **Clear configuration:** Clears all settings except basic system and networking settings (such as IP addresses).
  - **Reset to factory default:** Clears all settings including system and networking settings.
- **Switchover:** On systems with more than one management module installed, switch current operation to the other management module.
- **DB Sync:** Appears only on PFS 6010 systems. This button 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.
- **User (👤):** Shows the currently logged in user. Click the icon for more options:
  - **Change password:** The current user can change their password by entering their current password, a new password (that is compliant with [password policies](#)), and then confirming the new password.
  - **Logout:** Logs user out of the Web UI.
- **Notifications:** Lists all alerts and notifications since the last time the notifications were cleared. The list carries across multiple sessions until it is cleared. Click the icon to view the messages. Click **Clear notifications** to clear the display.



## System Status

Open the System Status page to view the overall status of the system. For systems that support multiple line cards, this page displays the status of each chassis line card slot.

ID	State	Time Left	Product ID	Configured Card	SKU P/N	Module Part Number	Module Revision Number	Module Serial Number	PCBA Part Number
1	OK		5248	pre-configured	0GM4RM	N/A	N/A	FQ3RY03	N/A

The top part of the page has four displays of information that can be individually selected (System, Network, Software, Clocks). On systems with multiple management modules installed, information is displayed for all modules.

The table shows the status, where applicable, of each slot and line card. On systems without removable line cards, all ports are shown as being on line card 1. When a capability does not apply to the specific hardware on this system, it displays as either blank or "N/A."

To view and modify the settings for a specific port, click the slot number and select the port from the list of ports that displays.

Slot	State	Product
1	OK	1310
2	OK	1310
2-1	2-2	2-3
2-5	2-6	2-7
2-9	2-10	2-11
2-13	2-14	2-15
2-17	2-18	2-19
2-21	2-22	2-23
		2-24



## System Tab

When you open the page, the system settings display in the top area: Name, product ID, serial number, location contact, license status (refer to [PFOS Licensing](#)), management module status, data and system disk usage, temperature, system status, redundancy status, platform, and PFS 5000/7000 total energy consumption (total estimated daily power usage in kWh based on sampling over the past 1 hour).

System Information					
Name: PFS5031-56X-ZTP	Location: San Jose Lab, CA USA	Mgmt-1: <span style="color: green;">OK</span>	Data Disk Usage: <span style="color: green;">29%</span>	System Status: <span style="color: green;">OK</span>	
Product ID: 5248	Contact: support@netscout.com	Mgmt-2: <span style="color: orange;">N/A</span>	System Disk Usage: <span style="color: green;">8%</span>	Temperature: <span style="color: green;">27 °C</span>	
Serial Number: FQ3RY03	Support License: <span style="color: green;">Current</span>	Platform: PFS7031-56X	Redundancy Status: <span style="color: orange;">N/A</span>	Energy Consumption: <span style="color: green;">0.13 kWh</span>	

Disk Usage is displayed as Data and System – two major disk spaces in the device.

- **Data Disk Usage:** 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.
- **System Disk Usage:** Percentage of total disk space for system files (unreachable by users). It is the location for system execution files, including PFOS installation images.

Percentages display **green** for 70% or less usage; **amber** for usage between 70-90% usage, and **red** for 90% or more usage.

System Disk is controlled by the system while Data Disk usually does not require users to manage except when uploading a new image file. When data disk usage is more than 90%, the system will automatically remove unused files. However, since PFOS or PFS Fabric Manager image may need more than 10% of data disk space, users need to delete larger unused files (such as a standby image file) to gain enough disk space for a new image.

## Network Tab

The Network tab displays IPv4 address, IPv6 address, IPv4 gateway, IPv6 gateway, MAC address, DNS.

Network Configuration			
IPv4 Address:	<span style="color: green;">10.250.177.122/23</span>	IPv4 Gateway:	<span style="color: green;">10.250.176.1</span>
IPv6 Address:	<span style="color: green;">0049:1064</span>	IPv6 Gateway:	<span style="color: green;">0049:10</span>
MAC address:	A8:2B:B5:9D:C5:EF		

## Software Tab

The Software tab displays image name, version, core version, PFS FM version, and pStack version.



Software Image Information			
Mgmt-1:	vxos_core_PFS5k_8.1.2.22-6ceae740	Version:	6.1.2.22-6ceae740
Mgmt-2:	NA	Version:	NA
pStack:		Version:	30.1

## Clocks Tab

The Clocks tab displays current date/time, boot time, system uptime.

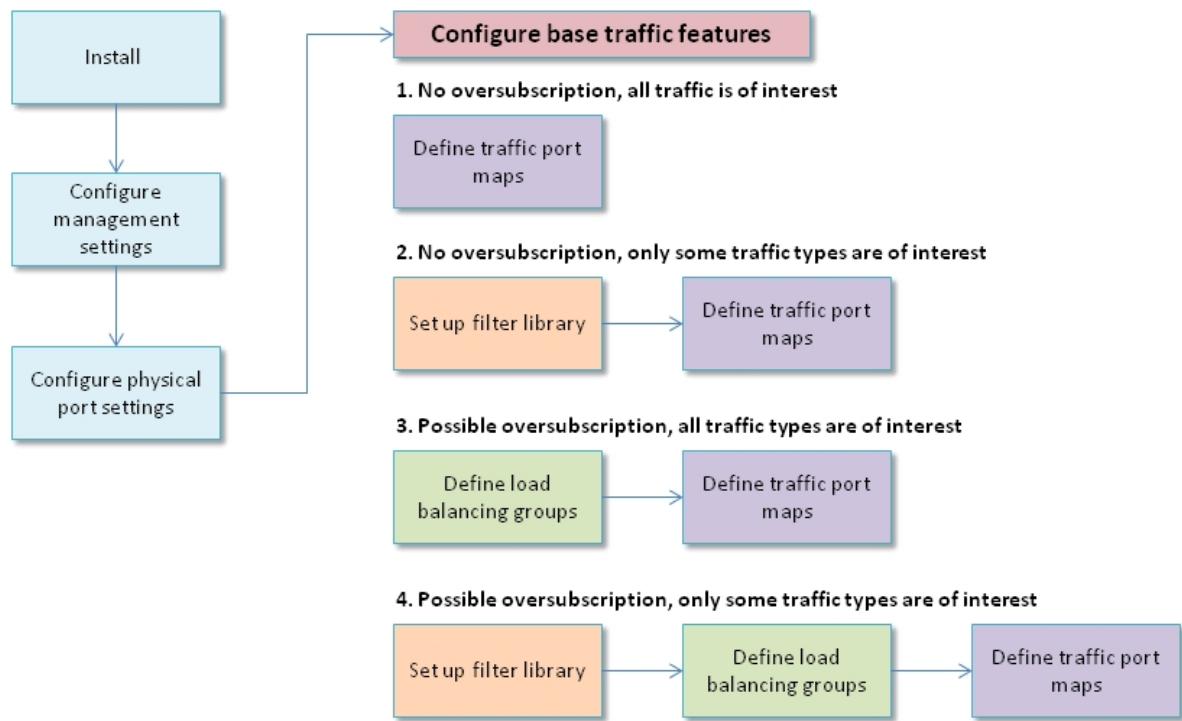
Clocks			
System datetime:	Fri, 08 Feb 2019 16:54:50 GMT	SYSTEM Boot time:	Fri, 01 Feb 2019 20:59:46 GMT
			Uptime: 6 days, 19 hours, 55 mins and 4 seconds
		MGMT-1 Boot time:	Fri, 01 Feb 2019 20:59:46 GMT
			Uptime: 6 days, 19 hours, 55 mins and 4 seconds
		MGMT-2 Boot time:	NA
			Uptime: NA

## Configuration Task Flow

The following steps describe PFOS configuration tasks. PFOS also supports [Zero Touch Provisioning](#).

1. Confirm that the system is installed and accessible on the network. See the [Quick Connection Guide](#) for your system.
2. Configure system settings, including system, network, and time settings. See [Configuring the System and Ports](#).
3. Configure physical port settings. See [Configuring Ports](#).
4. Configure filtering, as needed. See [Traffic Filtering](#).
5. Configure load balancing, as needed. See [Traffic Load Balancing](#).
6. Set up traffic maps. See [Traffic Maps](#).

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



## Zero Touch Provisioning

**Note:** Zero Touch Provisioning (ZTP) is only supported on PFS 5000/7000 devices.

Zero Touch Provisioning (ZTP) allows you to provision new PFS devices in your network automatically, with minimal manual intervention. When you physically connect a PFS device to the network and boot it with a default factory configuration, PFOS communicates with the Dynamic Host Configuration Protocol (DHCP) server to load its initial configuration.

**Note:** For PFOS 6.0.4 and later, on a newly installed PFS device or after a factory reset on an existing PFS device, DHCP is enabled by default to support ZTP. If ZTP is not desired, a static IP can be configured after disabling DHCP at the device.



## ZTP Activation Process

Once the PFS 5000/7000 device is connected to the network and booting in its factory-default configuration, the following series of events will occur.

1. The PFS 5000/7000 devices contact the DHCP server to obtain an IP address. The PFS tells the DHCP server that it is a PFS in the:
  - DHCP Vendor Class Identifier (option 60)
  - DHCPv6 Vendor Class (option 16)

**Note:** The DHCP Vendor Class Identifier contains a variable-length string of the form "NETSCOUT nGenius PFS5100 PFOS v6" or "NETSCOUT nGenius PFS5010 PFOS v6". The model identifier (such as, "5010") will reflect the base hardware model (it will not reflect 7000 series). The DHCPv6 Vendor Class field contains the 32-bit Enterprise Number 21671 followed by a 16-bit string length field followed by the same vendor class string as in DHCPv4.
2. The DHCP server assigns an IP address to the PFS device and also (optionally) provides the location of the [PFS configuration file](#) (via HTTP/HTTPS URL) to the device via:
  - [IPv4](#): DHCP option 114 (DHCP Captive Portal, often called default-url)
  - [IPv6](#): DHCPv6 Option 59 (dhcp6.bootfile-url)
3. The PFS device accesses the URL to download the PFS configuration file and renames it to "ztp\_pfs5000\_config."
4. The PFS device applies the "ztp\_pfs5000\_config" configuration file.
5. PFS copies the running-config to startup-config.

## PFS Configuration File

The configuration file given to the PFS uses the same format as configuration backups (see [Saving and Loading Configurations](#)). You define the location of your customized PFS configuration files (via HTTP/HTTPS URL) in the [DHCP server configuration](#) files.

**Note:** The comments at the top of the configuration file must be present or the configuration will not be loaded. The Platform in the comments must match the platform of the PFS onto which the file is loaded.

## DHCP Server Configuration

You need to configure the Dynamic Host Configuration Protocol (DHCP) server dhcpd.conf files to provide the necessary information the PFS devices require for initial configuration. If you do not configure the DHCP server to provide this information, the device boots with the default factory configuration.

Refer to the following sections for configuration details to add to dhcpd.conf files for PFS to support Zero Touch provisioning.

- [IPv4 \(dhcpd.conf\)](#)
- [IPv6 \(dhcpd6.conf\)](#)



## IPv4 (dhcpd.conf)

The following text is required in the dhcdp.conf file to support PFS ZTP (DHCP Option 114). The following text declares the option and matches the model number to send the default URL (PFOS config file). The defined URL should match your network location where the configuration files are located and the name of the files.

```
option default-url code 114 = text;
class "NETSCOUT nGenius PFS" {
    match substring( option vendor-class-identifier, 0, 40) ;
} subclass "NETSCOUT nGenius PFS" "NETSCOUT nGenius PFS5100 PFOS v6" {
    option default-url "http://<IPv4address>/users/ztp_pfs5100_config";
}
subklass "NETSCOUT nGenius PFS" "NETSCOUT nGenius PFS5120 PFOS v6" {
    option default-url "http://<IPv4address>/users/ztp_pfs5120_config";
}
subklass "NETSCOUT nGenius PFS" "NETSCOUT nGenius PFS5010 PFOS v6" {
    option default-url "http://<IPv4address>/users/ztp_pfs5010_config";
}
subklass "NETSCOUT nGenius PFS" "NETSCOUT nGenius PFS5031-32X PFOS v6" {
    option default-url "http://<IPv4address>/users/ztp_pfs5031-32X_config";
}
subklass "NETSCOUT nGenius PFS" "NETSCOUT nGenius PFS5031-56X PFOS v6" {
    option default-url "http://<IPv4address>/users/ztp_pfs5031-56X_config";
}
subklass "NETSCOUT nGenius PFS" "NETSCOUT nGenius PFS5121-64X PFOS v6" {
    option default-url "http://<IPv4address>/users/ztp_pfs5121-64X_config";
}
```

## IPv6 (dhcpd6.conf)

The following text is required in the dhcdp6.conf file to support PFS ZTP (DHCP Option 16). The DHCP server needs to match DHCPv6 Vendor Class (Option 16) data field. The following text declares the option and matches the model number to send the dhcp6.bootfile-url (PFOS config file). The defined URL should match your network location where the configuration files are located and the name of the files.

```
option dhcp6.vendor-class code 16 = {integer 32, integer 16, string};
class "NETSCOUT nGenius PFS" {
match substring( option dhcp6.vendor-class, 6, 40) ;
} subclass "NETSCOUT nGenius PFS" "NETSCOUT nGenius PFS5100 PFOS v6" {
    option dhcp6.bootfile-url "http://<IPv6address>/users/ztp_pfs5100_config";
}
subklass "NETSCOUT nGenius PFS" "NETSCOUT nGenius PFS5120 PFOS v6" {
    option dhcp6.bootfile-url "http://<IPv6address>/users/ztp_pfs5120_config";
}
subklass "NETSCOUT nGenius PFS" "NETSCOUT nGenius PFS5010 PFOS v6" {
    option dhcp6.bootfile-url "http://<IPv6address>/users/ztp_pfs5010_config";
}
```



```
subclass "NETSCOUT nGenius PFS" "NETSCOUT nGenius PFS5031-32X PFOS v6" {
    option default-url "http://<IPv6address>/users/ztp_pfs5031-32X_config";
}
subclass "NETSCOUT nGenius PFS" "NETSCOUT nGenius PFS5031-56X PFOS" {
    option default-url "http://<IPv6address>/users/ztp_pfs5031-56X_config";
}
subclass "NETSCOUT nGenius PFS" "NETSCOUT nGenius PFS5121-64X PFOS" {
    option default-url "http://<IPv6address>/users/ztp_pfs5121-64X_config";
}
```

## Zero Touch Provisioning Known Limitations

- PFS 6000s are not supported.
- Configuration files applied via ZTP must not enable DHCP together with a static IP address; such configuration files will not be applied.
- Only HTTP and HTTPS are supported for downloading the config file; if HTTPS is used, TLS v1.3 is not supported. Any TLS certificate warnings are ignored.
- PFOS sends requests over both DHCPv4 and DHCPv6, and processes the responses in the order received.
- PFOS is able to use the first three name servers received. If the DHCP server returns three each of IPv4 and IPv6 name servers, the first response will be used. If the DHCP server returns two of each, the second name server from the second response will not be used.
- PFOS does not support ZTP when IPv6 addresses are assigned via SLAAC; IPv6 addresses must be assigned by DHCP when using ZTP.

# 3 Configuring the System and Ports

This section describes how to configure PFOS and the physical ports on your system. Before you continue, review [Configuration Task Flow](#).

- [Configuring System Settings](#)
- [Configuring Access Control](#)
- [Configuring Ports](#)

**Note:** You must click **Apply** at the top of the Web UI to save configuration settings to the running configuration. To have changes persist through a reboot, you must also save them to the startup configuration by clicking **Copy to Startup**. See [Configuration File Types](#) for information on the running, startup, and saved configuration files.

## Unsupported Special Characters

The following special characters cannot be used in port names, filter names, system names, load balancing group names, system location, system contact, and filter expressions:

- Single quote (')
- Double quote (")
- Backslash (\) (Use a double-backslash, \\, to insert a backslash)
- Greater than (>)
- Less than (<)
- All control characters
- Accent (`)
- Tilde (~)
- Semicolon (;)
- Comma (,)

This limitation applies to all management interfaces: the Web UI, the CLI, and the API.

## Configuring System Settings

Refer to the following sections for system configuration:

- [Configuring Global System Settings](#)
- [Configuring Notifications](#)



- Configuring Time Settings

## Configuring Global System Settings

Use the pages listed under System on the side menu to configure global system settings.

Set global system properties on the **Global Settings > System** page.

- Basic Information Settings
- Network Settings
- Features
- Syslog
- Trace Log
- nCM
- NMS

### Basic Information Settings

The **Basic Information** tab displays similar information as the System Status page: Product ID, serial number, and System and Data disk usage. You can configure the following information on this page:

- Name - assign a name to the chassis.
- Contact - define an address.
- Location - define the chassis location (such as city, state)
- Notes - add additional device, location, or contact details up to 4000 characters



- Banner - define a text message that appears to users prior to logging into the PFOS Web UI and CLI. You can notify users of your corporate IT policies or communicate other important messages to all users system-wide. The message can contain up to 4000 characters. You can also configure the message using the CLI command `system banner`. When no banner is configured, the Web UI displays the default banner.

After assigning settings, click **Apply** in the toolbar to save the settings to the running configuration.

## Network Settings

Open the **Network** tab to view or configure network settings for the system, including system IPv4 or IPv6 address and netmask, gateway, and DNS server.

Note the following:

- The IPv4 and IPv6 addresses must be in address/prefix length format (for example, 10.250.176.81/23 or fc00:0:3:1ad3::23:a/64).
- If you change the IP address or netmask (IPv4 or IPv6), your current web browser connection will no longer be valid, because the IP address or netmask of the system will no longer match your browser settings. The Web UI will try to reconnect using the new address. If this does not succeed, close your browser window and restart with the new IP address.

After assigning settings, click **Apply** in the toolbar to save the settings to the running configuration.

Refer to the following sections for details:

- [PFS 5000/7000 System Network Settings](#)
- [PFS 6010 with Two Management Modules System Network Settings](#)



## PFS 5000/7000 System Network Settings

The following graphic shows network settings page for PFS 5000/7000 series.

**System**

Basic Information Network Source Port VLAN Tagging Features Syslog Trace Log nCM

DHCP  Enable/Disable DHCP

**Active Network Connection Details**

IP 4 Address	10.250.176.150/23	IP 4 Gateway	10.250.176.1
Default: 0.0.0.0		Default: 0.0.0.0	
IP 6 Address	::/0	IP 6 Gateway	::
Default: ::/0		Default: 0::0	

**DNS**

ID	IP
0	

**IPv6 DNS**

ID	IPv6 address
0	

**Static Network Connection Details**

ID	IP - IP 4 Address	IP - IP 4 Gateway	IP - IP 4 DNS	IPv6 - IP 6 Address	IPv6 - IP 6 Gateway	IPv6 - IP 6 DNS
0	10.250.176.150/23	10.250.176.1	0.0.0.0	::/0		

Showing 1 to 1 of 1

To update management IP information, click the ID number in the Static Network Connection Details area at the bottom of the page. A page appears allowing you to edit settings.

0 ×

**IP**

IP4 Address	10.250.176.150/23	IP4 Gateway	10.250.176.1
		Default: 0.0.0.0	
IP4 DNS	0.0.0.0	Default: 0.0.0.0	

**IPv6**

IP6 Address	::/0	IP 6 Gateway	ipv6-address
Default: ::/0		IP6 DNS ipv6-address	

### DHCP on PFS 5000/7000 Series

On a PFS 5000/7000 Series system, you can use this page to enable/disable Dynamic Host Configuration Protocol (DHCP). When DHCP is enabled and the system is rebooted, PFOS will try to get network information from a DHCP server on the connected network and, if found, will



automatically configure addresses.

If no DHCP server is found, or if DHCP is disabled, the network settings on the Network tab are used instead.

To view information about the currently active management connection to the network, click **Active Network Connection**.

**Note:** On a factory reset after upgrade to 6.0.4 or later, DHCP is enabled by default. If user wants to use static IP address, DHCP must be disabled first (see [Disable/Enable DHCP on PFS 5000/7000 Series](#)).

ID	IP - IP 4 Address	IP - IP 4 Gateway	IP - IP 4 DNS	IPv6 - IP 6 Address	IPv6 - IP 6 Gateway	IPv6 - IP 6 DNS
0	10.250.177.122/23	10.250.176.1	8.8.8.8	8049::1/64	8049::10	8049::20

## 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](#)
- [Enable DHCP](#)

### Disable DHCP and Configure a Static IP

**Note:** You can also disable DHCP and configure a static IP using CLI commands. See the `dhcp` command in the *PFOS CLI Reference Guide* for an example.

**Warning:** *Do not Apply changes between Steps 1 and 3; doing so may result in loss of network access to the device. All changes should be applied together in Step 4.*

1. Disable DHCP.
2. Configure static IPv4 or IPv6 address with gateway.
3. Configure DNS if needed.



4. Apply all changes together.
5. A validation warning message will pop up for confirmation.

Validation error source	Message
System / Network Settings	Changing the DHCP settings may lead to the change of the system IP address. Active sessions may be lost.

6. Reconnect the device with the static IP address.

ID	IP - IP 4 Address	IP - IP 4 Gateway	IP - IP 4 DNS	IPv6 - IP 6 Address	IPv6 - IP 6 Gateway	IPv6 - IP 6 DNS	Mac Address
0	10.250.177.115/23	10.250.176.1	0.0.0.0	::0	::0	::0	8C:EA:1B:FF:BB:A4

## 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.

Validation error source	Message
System / Network Settings / 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.

## 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.

To enable DHCP at WebUI, enable the DHCP option on the **System>Network>DHCP** page. You can also enable DHCP using CLI; see the `dhcp` command in the *PFOS CLI Reference Guide*.



## PFS 6010 with Two Management Modules System Network Settings

The following graphic shows network settings for a PFS 6010 with two installed management modules.

To change the settings, click the number of the management module that you want to configure. A page appears allowing you to edit settings for the selected management module.



## Source Port VLAN Tagging

Use this section to view or configure the VLAN tags that are used when VLAN tagging is enabled on one or more output ports.

- **TPID Ether Type:** 0x88A8 (default), 0x8100, or 0x9100
- **Starting VLAN 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, PFOS starts counting at the far left and uppermost hardware port and proceeds consecutively, top to bottom and left to right.

After assigning settings, click **Apply** in the toolbar to save the settings to the running configuration. Refer to [Source Port VLAN Tagging](#) for more information about VLAN tagging settings.

TPID Ether Type	88A8 – Provider Bridging (IEt)	Starting VLAN ID	1
Default: 88A8 – Provider Bridging (IEE... Valid values: 1—3464		Default: 1	

## Features

Open the **Features** tab to view or configure the settings for system-wide features. System-wide features include:

- [FIPS Mode](#)
- [Powersafe](#)
- [Hash Algorithm](#)
- [Tunnel](#)
- [Map Profile](#)
- [Slicing](#)
- [MPLS](#)
- [MPLS Max Labels](#)
- [MPLS Cleanup Mode](#)
- [Common Criteria Mode](#)
- [Custom Hash](#)
- [Custom Bytes](#)
- [Access Management](#)

To use the Features tab, your username must have the “Features” role assigned to it by the administrator. See [Configuring Access Control](#).



**System**

Basic Information Network Source Port VLAN Tagging Features Syslog Trace Log nCM NMS

FIPS Mode  Enable FIPS mode to use only FIPS-validated cr...

Powersafe  Enable/Disable powersafe feature

Hash Algorithm  Default: xor16 Hash algorithm to use for load balancing xor1...

Tunnel  Default: enable Enable Tunnel to use tunnel features Warning!...

Map Profile  Default: auto profile to be applied towards traffic maps

Slicing  Enable/Disable Slicing feature

MPLS  Enable MPLS Stripping to use MPLS Stripping fe...

MPLS Max Labels  Default: 1024 Valid values: 1—24576 Number of MPLS labels supported Max dynamic la...

MPLS Cleanup Mode  Default: manual Cleanup method used to flush dynamic MPLS labe...

Common Criteria Mode  Enable common criteria compliant mode Warning!...

Custom Hash  Default: disable Custom hash support for traffic distribution. ...

Custom Bytes  Default: 2 Number of custom hash bytes to support for tra...

## FIPS Mode

This feature is available on PFS 5000/7000. To enable or disable FIPS mode, either select or deselect the **FIPS Mode** checkbox. 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.
- 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](#).
- 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 [Common Criteria Mode](#) and FIPS mode are enabled, PFOS will only use ECDSA key type for [Maintaining SSH Knownhost](#).
- Refer to [Certificate Limitations and Configuration Considerations](#).

Users enabling or disabling the FIPS setting at the WebUI will be forced to relogin (no action required if changing FIPS mode via CLI).

## Powersafe

This feature requires the PFS 7000 functionality license. To enable or disable the Powersafe feature, either select or deselect the **Powersafe** checkbox. This feature requires an [PowerSafe](#) device.



## Hash Algorithm

This feature is only available on PFS 5000/7000 Series. Select the hash algorithm to use for [load balancing](#) traffic to/from PFS 5000/7000 series devices. If a hash algorithm resolves to the same output port for a flow regardless of the flow direction (that is, when source is transmitting and when destination is transmitting) then the algorithm is considered **Normalized**. Not all supported hash algorithms are inherently normalized. The following table lists the supported hash algorithms and indicates which algorithms support normalization.

**Note:** The BCM\_HASH\_FIELD\_CONFIG\_XOR16 algorithm will be used as the default algorithm if no algorithm is specified.

Name	Description	Normalization	
		PFS 5010/7010	PFS 51xx/ 71xx
BCM_HASH_FIELD_CONFIG_CRC16XOR8	Upper 8 bits of BISYNC CRC16 and 8 bit XOR8	Yes	Yes
BCM_HASH_FIELD_CONFIG_CRC16XOR4	Upper 8 bits of BISYNC CRC16 and 8 bit XOR4	Yes	Yes
BCM_HASH_FIELD_CONFIG_CRC16XOR2	Upper 8 bits of BISYNC CRC16 and 8 bit XOR2	Yes	Yes
BCM_HASH_FIELD_CONFIG_CRC16XOR1	Upper 8 bits of BISYNC CRC16 and 8 bit XOR1	Yes	Yes
BCM_HASH_FIELD_CONFIG_CRC16	16 bit CRC16	No	No
BCM_HASH_FIELD_CONFIG_XOR16	16 bit XOR (Default)	Yes	Yes
BCM_HASH_FIELD_CONFIG_CRC16CCITT	16 bit CRC16 calculated using CCITT polynomial	No	No
BCM_HASH_FIELD_CONFIG_CRC32LO	Lower 16 bit of computed CRC32	No	No
BCM_HASH_FIELD_CONFIG_CRC32HI	Higher 16 bit of computed CRC32	No	No
BCM_HASH_FIELD_CONFIG_CRC32_ETH_LO	Lower 16 bit of Ethernet CRC32	Yes	No
BCM_HASH_FIELD_CONFIG_CRC32_ETH_HI	Higher 16 bit of Ethernet CRC32	Yes	No
BCM_HASH_FIELD_CONFIG_CRC32_KOOPMAN_LO	Lower 16 bit of Koopman CRC32	Yes	No
BCM_HASH_FIELD_CONFIG_CRC32_KOOPMAN_HI	Higher 16 bit of Koopman CRC32	Yes	No

## Tunnel

**Note:** For PFS 5121/7121-64X, PFS 503x/703x-32X, 5031/7031-56X, 5040/7040-32D, 5041/7041-32D and 5030/7030-54X devices, the Tunnel feature is always enabled; therefore, this option is not shown to users.



This Tunnel option enables/disables tunnel features and functionality (including [IP Tunnel Termination](#), [L2GRE Tunnel Origination/Termination Support](#), [VXLAN Tunnel Origination/Termination Support](#), and [pfsMesh Using pStack+](#)):

- When the Tunnel option is disabled, users will receive an error when trying to configure and apply tunnel functionality.
- If existing tunnel functionality configuration exists and users try to disable this Tunnel option, they will receive an error.

Modifying this setting requires a reboot; you are prompted with a system message asking you to confirm the reboot.

## Map Profile

The Map Profile can be configured on the PFS 5000/7000 series. This setting controls how PFOS uses the TCAM (Ternary Content-Addressable Memory) for use in Forwarding Filters.

**Note:** Map profile is not configurable at 5040/7040-32D and 5041/7041-32D devices as only the Legacy mode can be supported.

<b>Auto Mode</b>	Auto Mode is the default mode. When the map profile is set to <i>Auto</i> , the system first selects <i>SIP mode</i> until source IP addresses configured in filter expressions exceed the limits described under SIP Mode below. Once exceeding SIP mode capability, the system selects <i>DIP mode</i> until destination IP addresses configured in filter expressions exceed the limits described under DIP Mode below. Once exceeding DIP mode capability, the system will select and stay with Legacy mode.
<b>SIP Mode</b>	SIP mode uses an extended user group for Source IPv4 and IPv6 address filters. It can be used when the number of source IPv4-only or IPv6-only address filters is 1024 or less, or the number of mixed source IPv4 and IPv6 address filters is 512 or less.
<b>DIP Mode</b>	DIP mode uses an extended user group for Destination IPv4 and IPv6 address filters. It can be used when the number of destination IPv4-only or IPv6-only address filters is 1024 or less, or the number of mixed destination IPv4 and IPv6 address filters is 512 or less.
<b>SIP-IPv6 Mode</b>	When configuration includes both source IPv4 and IPv6 addresses, SIP-mode capability reduces from 1024 to 512 entries. As SIP mode is most useful for source IPv6 addresses, <i>SIP-IPv6 mode</i> can limit the extended user group to be used for IPv6 only. <b>Note:</b> Map Profile with <i>Auto</i> mode does not automatically select <i>SIP-IPv6 mode</i> ; users need to manually configure it.
<b>DIP-IPv6 Mode</b>	When configuration includes both destination IPv4 and IPv6 addresses; DIP-mode capability reduces from 1024 to 512 entries. As DIP mode is most useful for destination IPv6 addresses, <i>DIP-IPv6 mode</i> can limit the extended user group to be used for IPv6 only. <b>Note:</b> Map Profile with <i>Auto</i> mode does not automatically select <i>DIP-IPv6 mode</i> ; users need to manually configure it.



<b>Legacy Mode</b>	Without using an extended user group for source or destination IP addresses, all IP addresses will be configured in the same user filter groups. Users should configure map profile as <i>Legacy mode</i> for the following two situations: <ul style="list-style-type: none"><li>The number of source and destination IP address filters exceeds SIP mode and DIP mode limitations as described above.</li><li>The filter expression contains IP dependency. For example, if one filter expression is 10.10.0.0/16 and the other filter expression is 10.10.0.0/24, both filters are configured for the same source ports but to different destination ports.</li></ul>
--------------------	---

**Caution:** Ensure the following:

- Be sure to choose the best mode to support your forwarding filter requirements *before* starting your configuration. Due to the different capabilities of each mode, modifying the Map Profile may prevent your existing filter settings from being reprogrammed in TCAM. Refer to [Filter Resource Limits](#) to understand more about hardware limitations on each platform.
- When the map profile is manually reconfigured or automatically changed by Auto mode; the system does not need a reboot. However, for the best practice, if any existing working map fails after a map profile change, save the config and reboot. The system can refresh to reprogram TCAM based on the original filters.

### Map Profile Configuration Considerations

Although the default setting is Auto mode, selecting a proper map profile can more efficiently use filter resources and avoid unnecessary map mode changes. Review your filter requirements and consider the following factors to select the best mode for your configuration needs. Refer to [Filter Resource Limits](#) to understand filter capability at each PFS platform.

- Leave the map profile as the default *Auto* mode if your filters will not have more than 1024 of IPv4-only, or 1024 of IPv6-only, or 512 of mixed IPv4 and IPv6 addresses.
- Select *SIP-IPv6* or *DIP-IPv6* mode if your filters include both IPv4 and IPv6 addresses, and the total number of source or destination IP addresses is more than 512 entries, but less than 1024 entries. SIP-IPv6 and DIP-IPv6 mode will limit only IPv6 addresses to be programmed at the extended user group to ensure all 1024 entries or less are used, versus 512 entries when mixing with IPv4 and IPv6 addresses.
- Select *Legacy* mode if your filters include IP addresses with overlay. In Legacy mode, IP address filtering is performed in the same stage as the rest of the filter. However, the total number of filter resources may be significantly reduced.

### Use Case 1 – Filters with IPv4 or IPv6 or Both Addresses

Filter capability at each profile mode depends on how many QSet bits are in use. SIP, DIP, SIP-IPv6, or DIP-IPv6 mode moves IP addresses to an extended group, significantly reducing QSet bits at user filter groups, thereby extending entire filter capability.



Either SIP or DIP mode can use the extended group for 1024 IPv4 or IPv6 addresses. However, when the configuration includes a mix of both IPv4 and IPv6 addresses, the extended group capability drops to 512. To reduce total QSet bits used at user filter groups, arranging IPv6 addresses only (128 bits) to the extended group can offer the most efficient filter usage at user filter groups.

- Use *SIP* or *DIP* mode if filter has the following situations:
  - Contains no IPv6 addresses, and total IPv4 addresses is not more than 1024.
  - Contains no IPv4 addresses; and total IPv6 addresses is not more than 1024.
  - Contains both IPv4 and IPv6 addresses, but total is not more than 512.
- Use *SIP-IPv6* or *DIP-IPv6* mode if filter has the following situation:
  - Contains both IPv4 and IPv6 addresses, and total is more than 512 but not more than 1024.

### PFS 5010 Filter Resources Example

Consider the following traffic map configuration for the PFS 5010.

Map	Ingress Port	Filter	Egress Port
1	1-1	IP Source 10.1.1.1 or IP Source 2001::1 or IP Dest 10.1.1.1 or IP Dest 2001::1	1-11
2	1-2	IP Source 20.1.1.1 or IP Dest 20.1.1.1	1-12
3	1-3	IP Source 2002::1 or IP Dest 2002::1	1-13
4	1-4	IP Source 21.0.0.1 or IP Dest 21.0.0.1	1-14

Map-1 has both IPv4 and IPv6 addresses. Map-2 to Map-4 also include both IPv4 and IPv6 addresses. In this scenario, SIP or DIP mode can be selected because the total IPv4 and IPv6 addresses is not more than 512.

The Filter Resource below shows the group information under SIP or DIP mode at PFS 5010.

```
+-----+
+ TCAM Information:
+ Group| Priority| TCAM Total| TCAM Used| TCAM Free| Bits Used|      Group Mode +
+-----+
+   0|    7ffff|      512|       5|     507|     160| IntraSliceDouble +
+   10|   7fff5|     6144|       4|     6140|     294|      Double +
+   20|   7ffeb|     6144|      10|     6134|     226|      Double +
+-----+
#####
MODE: sip-mode
Status: ALL FLOWS ARE IN WORKING STATE
```



The Filter Resource below shows the group information under SIP-IPv6 or DIP-IPv6 mode at PFS 5010.

TCAM Information:						
Group	Priority	TCAM Total	TCAM Used	TCAM Free	Bits Used	Group Mode
0	7ffff	1024	2	1022	128	Single
10	7fff5	6144	4	6140	294	Double
20	7ffeb	6144	10	6134	258	Double

\*\*\*\*\*  
MODE: sip-ip6-mode  
Status: ALL FLOWS ARE IN WORKING STATE

In this simple example, all SIP or DIP or SIP-IPv6 or DIP-IPv6 can offer 6144 filter entries at PFS 5010.

The Filter Resource below shows the group information under Legacy mode at PFS 5010. Without using SIP, DIP, SIP-IPv6, or DIP-IPv6 modes, the system needs to request more groups for the same configuration under Legacy mode.

TCAM Information:						
Group	Priority	TCAM Total	TCAM Used	TCAM Free	Bits Used	Group Mode
10	7fff5	3072	4	3068	294	Double
20	7ffeb	3072	3	3069	226	Double
21	7fea	2048	3	2045	226	Double
22	7ffe9	2048	2	2046	290	Double
23	7ffe8	4096	2	4094	98	Single

\*\*\*\*\*  
MODE: legacy  
Status: ALL FLOWS ARE IN WORKING STATE

For some scenarios, using Legacy mode at PFS 5010 for filters with a mix of both IPv4 and IPv6 will be very challenging. However, in some situations the map profile must be configured as Legacy mode, such as with filters having more than 1024 of IPv4 and IPv6 addresses or IP dependency.

When using Legacy mode for filter expressions including both IPv4 and IPv6 addresses, separating and then rearranging IPv4 and IPv6 maps can enhance filter usage.

- **Step 1:** Divide IPv4 and IPv6 addresses into separate filters as shown below.

Map	Ingress Port	Filter	Egress Port
1A	1-1	IP Source 10.1.1.1 or IP Dest 10.1.1.1	1-11
1B	1-1	IP Source 2001::1 or IP Dest 2001::1	1-11
2	1-2	IP Source 20.1.1.1 or IP Dest 20.1.1.1	1-12
3	1-3	IP Source 2002::1 or IP Dest 2002::1	1-13
4	1-4	IP Source 21.0.0.1 or IP Dest 21.0.0.1	1-14

- **Step 2:** Move all IPv4 maps before IPv6 maps as shown below.



Map	Ingress Port	Filter	Egress Port
1A	1-1	IP Source 10.1.1.1 or IP Dest 10.1.1.1	1-11
2	1-2	IP Source 20.1.1.1 or IP Dest 20.1.1.1	1-12
4	1-4	IP Source 21.0.0.1 or IP Dest 21.0.0.1	1-14
1B	1-1	IP Source 2001::1 or IP Dest 2001::1	1-11
3	1-3	IP Source 2002::1 or IP Dest 2002::1	1-13

After rearranging the maps, the filter usage is reduced to two groups only.

**Note:** If some maps are in error state due to filter resource limitation, a system reboot may be necessary. After separating and rearranging IPv4 and IPv6 maps, save to startup config, and then reboot the system.

```
+-----+
+ TCAM Information:
+ Group| Priority| TCAM Total| TCAM Used| TCAM Free| Bits Used|      Group Mode +
+-----+
+ 10|    7fff5|     5120|       4|     5116|      294|      Double +
+-----+
+ 20|    7ffeb|     5120|       7|     5113|      226|      Double +
+-----+
+ 21|    7ffea|     4096|       3|     4093|      290|      Double +
+-----+
+-----+
MODE: legacy
Status: ALL FLOWS ARE IN WORKING STATE
```

### PFS 5100 Filter Resources Example

PFS 5100 has different filter capability compared to the PFS 5010. The following graphics show the PFS 5100 filter usage for the same configuration as the 5010 in the previous example, using different map profile modes. Unlike the PFS 5010, the PFS 5100 does not need to create multiple filter groups for IPv4 and IPv6 addresses. When QSet bit requirement is more than 160 bits, the filter capability at the pipe will be reduced to 768 entries.

**Note:** If filters include more than 768 IPv4 or IPv6 addresses, the configuration needs to adjust ingress ports at different pipes to spread out TCAM requirements.

```
+-----+
+ PIPE: 2 (#1-1 to #1-4 and #1-9 to #1-12)
+-----+
+ 1|    7ffffe|     512|       5|     507|      160| IntraSliceDouble +
+-----+
+ 11|   7fff4|     768|       4|     764|      278|      Double +
+-----+
+ 30|   7ffe1|     768|      10|     758|      226|      Double +
+-----+
MODE: sip-mode
Status: ALL FLOWS ARE IN WORKING STATE
```

```
+-----+
+ PIPE: 2 (#1-1 to #1-4 and #1-9 to #1-12)
+-----+
+ 1|    7ffffe|    1024|       2|    1022|      128|      Single +
+-----+
+ 11|   7fff4|     768|       4|     764|      278|      Double +
+-----+
+ 30|   7ffe1|     768|      10|     758|      258|      Double +
+-----+
MODE: sip-ip6-mode
Status: ALL FLOWS ARE IN WORKING STATE
```



# PIPE: 2 (#1-1 to #1-4 and #1-9 to #1-12)						
11	7fff4	768	4	764	278	Double
30	7ffe1	768	10	758	354	Triple
=====						
MODE: legacy						
Status: ALL FLOWS ARE IN WORKING STATE						

### QSet Bits in Filter Expressions

The number of filter entries available at each PFS platform depends on how many QSet bits are in use. The PFS 5010 has an additional restriction that IPv6 source and destination addresses cannot be programmed in the same group as IPv4 source and destination addresses. All other PFS platforms behave like PFS 5100. Refer to [Filter Resource Limits](#) to understand filter capability and group information at each platform.

To summarize the Filter Resources for all above examples (PFS 5010 and 5100) with *SIP mode*:

**Note:** The same explanation applies to *DIP mode*.

- Group-0 (or Group-1) is an extended user group for both IPv4 source (32 bits) and IPv6 source (128 bits) addresses; QSet bits in use is 160 bits, so filter capability drops to 512 entries.
- Group-20 (or Group-30) is a user filter group for IPv4 destination (32 bits) and IPv6 destination (128 bits) addresses, plus 66 bits used for system.
- Group-20 (or Group-30) has 226 total QSet bits in use, so filter capability can serve up to 6144 entries at PFS 5010 or 768 entries at PFS 5100.

To summarize the Filter Resources for all above examples (PFS 5010 and 5100) with *SIP-IPv6 mode*:

**Note:** The same explanation applies to *DIP-IPv6 mode*.

- Group-0 (or Group-1) is an extended user group for only IPv6 source (128 bits) addresses; QSet bits in use is 128 bits, so filter capability can maintain at 1024 entries.
- Group-20 (or Group-30) is a user filter group for IPv4 source (32 bits) and IPv4 destination (32 bits) and IPv6 destination (128 bits) addresses; plus 66 bits used for system.
- Group-20 (or Group-30) has 258 total QSet bits in use, so filter capability can serve up to 6144 entries at PFS 5010 or 768 entries at PFS 5100.

To summarize the Filter Resources for PFS 5100 with *Legacy mode*:

- Group-1 is not in use.
- Group-30 user filter group is programmed for IPv4 source (32 bits), IPv4 destination (32 bits), IPv6 source (128 bits) and IPv6 destination (128 bits) addresses, plus 34 bits used (32 bits less than SIP/DIP mode needs) for system.
- Group-30 has 354 total QSet bits in use, so filter capability can serve up to 768 entries.

To summarize the Filter Resources for PFS 5010 with *Legacy mode* after separating and rearranging IPv4 and IPv6 maps:

- Group-0 is not in use.



- Group-20 user filters group is programmed for IPv4 source (32 bits), IPv4 destination (32 bits), and IPv6 source (128 bits) addresses, plus 34 bits used (32 bits less than SIP/DIP mode needs) for system. It has 226 total QSet bits in use with filter capability of up to 5120 entries.
- Group-21 user filters group is programmed for IPv6 source (12 bits) and IPv6 destination (128 bits) addresses, plus 34 bits used (32 bits less than SIP/DIP mode needs) for system. It has 290 total QSet bits in use with filter capability of up to 4096 entries.

**Note:** For PFS 5010, multiple user filters groups (Group 20 or greater) are needed due to the PFS 5010 restriction preventing IPv6 destination addresses from being programmed at the same group with IPv6 source addresses (if both IPv4 source and destination addresses have existed in the group), so filter capability will be significantly reduced. Separating and rearranging IPv4 and IPv6 maps can enhance filter usage when using Legacy mode; see [PFS 5010 Filter Resources Example](#).

### *Use Case 2 – Filters with IPv4 or IPv6 Addresses with Overlap*

SIP and DIP modes use an extended user group to enhance filter resources; however, when two or more source or destination IP address filters, respectively, have overlapping ranges, incorrect matching can occur.

Consider the following traffic map configuration:

Map	Filter	Egress Port
1	10.1.0.0/16 and TCP port 80	1-10
2	10.1.1.0/24 and TCP port 443	1-11

With these traffic maps in SIP or DIP mode, a packet with 10.1.1.2 IP source or destination address (respectively) and TCP port 443 will mistakenly be dropped, even if the traffic maps use different ingress ports. This occurs because in SIP or DIP mode, the IP address portion of the filter is evaluated first, matching traffic map 1, and because TCP port 443 does not match the second clause of map 1's filter, the packet is dropped. To prevent this scenario, the filters can be changed to avoid overlap, or the Map Profile mode can be changed to Legacy.

In Legacy mode IP address filtering is done in the same stage as the rest of the filter. However, the total number of filter resources may be significantly reduced.

### Slicing

This feature requires the PFS 7000 functionality license. Packet slicing is only supported as part of the [port mirroring feature](#) on PFS 703x and PFS 704x devices. PFS 704x systems support an additional option to configure the slicing offset value. 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. Refer to [Packet Slicing](#) for details.

### MPLS

This feature requires the PFS 7000 functionality license. The MPLS option enables/disables [MPLS stripping features and functionality](#).



Modifying this setting requires a reboot; you are prompted with a system message asking you to confirm the reboot.

## MPLS Max Labels

This feature requires the PFS 7000 functionality license. This feature enables you to control the number of MPLS labels that PFOS automatically defines for [MPLS Standard Stripping](#):

- Valid values: 1 - 24576
- Default value: 1024
- PFS 7120 and PFS 7010: Maximum of 24576 (24K) labels supported
- Other PFS 7000 platforms: Maximum of 12288 (12K) labels supported

**Note:** The current number of MPLS label entries can be viewed with the CLI command `show stripping mpls | include -mpls | count`. If the number of programmed MPLS labels reaches the maximum allocated MPLS entries, they can be cleared automatically or manually (default); see the `stripping mpls-cleanup-mode` command in the [PFOS CLI Reference Guide](#) for cleanup mode details. To manually clear programmed MPLS labels, refer to [Clear Programmed MPLS Labels Manually](#) in this guide or the `stripping clear mpls` command in the [PFOS CLI Reference Guide](#).

**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.

## MPLS Cleanup Mode

This feature requires the PFS 7000 functionality license. Configure the clean-up method used to clear auto-defined MPLS labels when the maximum limit is reached. See also the `stripping mpls-cleanup-mode` command in the [PFOS CLI Reference Guide](#).

- **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 the Status > Stripping option; refer to [Clear Programmed MPLS Labels Manually](#) for details.

This configuration will take effect on next reboot.

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

## Common Criteria Mode

This feature is only supported on PFS 5000/7000 devices.

Common Criteria Mode	<input type="checkbox"/>
Enable common criteria compliant mode. Warning!...	



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.
- [Maintaining SSH Knownhost](#) 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.
- 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](#).
- 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](#) 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.**

### *Online Certificate Status Protocol*

Online Certificate Status Protocol (OCSP) monitoring of certificates is supported in Common Criteria mode. OCSP is used by Certificate Authorities to check the revocation status of an X.509 digital certificate; in the case of PFOS the browser TLS certificate and the Certificate Authority certificates that signed it are checked.

OCSP monitoring is performed every hour. If a certificate or its issuer has any issue, the following syslog message is reported.

Sys. The PFOS web server certificate has been revoked. Please install a valid web server certificate.

If the OCSP server is unreachable, the following syslog message is reported.

Sys. Unable to verify the PFOS web server and its trust certificate(s). The verification server <http://10.250.178.4/ocsp> can't be reached. Check that the verification server configuration is valid

If a trust certificate is missing, one of the following syslog messages is reported.

Sys. One or more of PFOS web server trust certificates are missing. Please make sure all trusted certificates are installed.

Sys. None of the PFOS web server trust certificates are present and/or the web server certificate is self-signed. Please make sure to install a valid server and trust certificates.



## Custom Hash

Enable/disable a custom hash to be used 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 [Load Balance Criteria](#)) to be used in a custom hashing mechanism for traffic distribution. This configuration will take effect on next reboot.

## Custom Bytes

This field is only visible when Custom Hash is enabled.

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.

## Access Management

Access Management enables you to control the following settings:

- [Management Interfaces](#)
- [Front Panel \(PFS 6000 Series\)](#)
- [Idle Timeouts](#)

### *Management Interfaces*

Access to the following management interfaces can be individually controlled, and (where appropriate) you can specify the TCP port on which access is to be allowed. Select a checkbox to allow that type of access, or deselect a checkbox to disallow that type of access.

- **CLI via SSH:** Default TCP port is 22.
- **Web UI via HTTP and HTTPS:** Default TCP port is 80 for HTTP and 443 for HTTPS.
- **NETCONF XML API via HTTP and HTTPS:** Default TCP port is 832 for NETCONF over SSH.
- **RESTCONF API via HTTPS:** Default TCP port is 443 for HTTPS.



Access Management

SSH

CLI  Default: enable Select to enable SSH in CLI

Port  Default: 22 Valid values: 1-65535 Enter port number for SSH in CLI

HTTP

WEBUI  Default: disable Select to enable HTTP in WebUI

NETCONF  Default: disable Select to enable HTTP in NETCONF

HTTPS

WEBUI  Default: enable Select to enable HTTPS in WebUI

Port  Default: 443 Valid values: 1-65535 Enter port number for HTTPS in WebUI

NETCONF  Default: enable Select to enable HTTPS in NETCONF

Port  Default: 832 Valid values: 1-65535 Enter port number for HTTPS in NETCONF

RESTCONF  Default: enable Select to enable HTTPS in RESTCONF

Port  Default: 443 Valid values: 1-65535 Enter port number for HTTPS in RESTCONF

### Front Panel (PFS 6000 Series)

This option is only available on the PFS 6000 Series. It enables or disables the LCD panel on the front of the PFS 6000 series system.

Front Panel

enable  Default: enable Select to enable Front Panel

### Idle Timeouts

You can configure the maximum number of minutes the Web UI or CLI can remain idle before PFOS terminates the session. Valid values are 1 to 30 (default is 30); a value of 10 mins is used when PFOS is upgraded from pre-6.0.x versions.



**Note:** An idle timeout will not occur for a WebUI session if the browser displays the System Status or Statistics page. These pages do not experience idle timeout because the PFOS WebUI polls data every 10 seconds to refresh data on these pages (the minimum session idle timeout is 1 minute).

The screenshot shows the 'Idle Timeouts' configuration screen. It has two sections: 'WEBUI' and 'CLI'. Both sections have a text input field with the value '30' and a note below stating 'Default: 30'. The note for WEBUI also includes the text 'Maximum idle time in minutes before terminating a Web UI session.' and the note for CLI includes the text 'Maximum idle time in minutes before terminating a CLI session.'

## Syslog

Syslog settings enable you to:

- [Configure Severity Level for Local Syslog Buffer](#)
- [Define Syslog Servers](#)
- [Send System Logs to Remote Server over SSH Tunnel](#)

### Configure Severity Level for Local Syslog Buffer

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

The screenshot shows the 'Syslog History' configuration interface. On the left, there is a dropdown menu labeled 'Severity Level' with 'Debug' selected. Below it is a list of severity levels: Emergency, Alert, Critical, Error, Warning, Notification, and Info. The 'Critical' option is highlighted with a red box. On the right, there is explanatory text: 'Select the MINIMUM severity level you want to store in the Syslog buffer. PFOS stores messages with the severity you select and the severity levels ABOVE your selected severity.' and 'For example, selecting Critical severity level saves Critical messages as well as Alert and Emergency severity messages to the local buffer.'

The local Syslog buffer can be viewed in the [Syslog History](#), accessed from **Status>Event Notifications**.

**Note:** This severity Level setting must be reconfigured in the case of clear config or factory default reset. In the case of upgrade:

- If the previous version has no severity level support, the default level 'debug' will be used
- If the previous version has severity level configured, the existing security level will be retained



## Define Syslog Servers

Define up to three Syslog servers for PFOS to send information about events such as port up/down status changes.

### Add a Syslog Server

1. From the **System>Syslog** page, click the **Add** button.
2. In the **Hostname** field, enter the server IPv4 or IPv6 address or hostname of the server and click the **Add** button. Note that you must have a valid DNS server configuration to be able to configure hostnames.

The screenshot shows a modal dialog box titled "Add new Host" with the subtitle "Syslog server hostname". Inside the dialog, there is a single input field labeled "Hostname \*" containing the value "1.1.1.1". At the bottom of the dialog are two buttons: a blue "Add" button and a white "Cancel" button.

3. Select a transport protocol: UDP, TCP, or TLS. 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](#) for details.
  - If [TLS Peer Verify](#) 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](#) 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.
4. Define a 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)

**Note:** PFOS allows users to enter a port value of "0" without error; however, it is not a valid value, and users should not configure it.



The screenshot shows a configuration dialog for a Syslog server. On the left, there is a dropdown menu labeled 'Protocol' with 'UDP' selected. Below it, the text 'Default: udp' and 'Transport protocol to use' is displayed. On the right, there is a text input field labeled 'Port' with a placeholder 'Valid values: 0—65535'. Below the port input, the text 'Port number' is shown.

- If TLS is the selected protocol, configure whether the Syslog server's certificate is verified (Yes) or not verified (No).

The screenshot shows a 'TLS Config' dialog. It contains a dropdown menu labeled 'Peer Verify' with 'Yes' selected. Below it, the text 'Default: yes' and 'Verification method of the peer' is displayed.

- Select the minimum severity level to filter Syslog messages forwarded to this Syslog server. The Syslog severity levels are shown below:

The screenshot shows a dropdown menu labeled 'Severity Level' with several options: Emergency, Alert, Critical, Error, Warning, Notification, Info, and Debug. The 'Critical' option is highlighted with a red box. To the right of the dropdown, there is explanatory text: 'Select the MINIMUM severity level you want to forward to this Syslog server. PFOS forwards messages with the severity you select and the severity levels ABOVE your selected severity.' Below this, another text block says: 'For example, selecting Critical severity level forwards Critical messages as well as Alert and Emergency severity messages to the this Syslog server.'

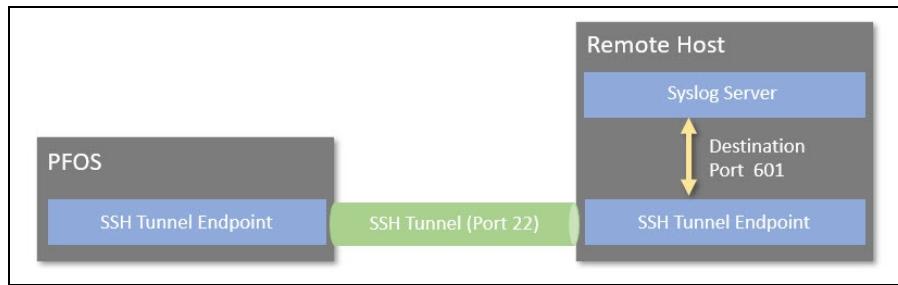
**Note:** This severity Level setting must be reconfigured in the case of clear config or factory default reset. In the case of upgrade:

- If the previous version has no severity level support, the default level 'debug' will be used
  - If the previous version has severity level configured, the existing security level will be retained
- Click **Apply** in the Toolbar to save the changes to the running configuration.
  - To add an additional Syslog server, click the **New Host...** button.

## Send System Logs to Remote Server over SSH Tunnel

PFOS supports sending system logs to a remote server over an encrypted SSH tunnel. The following bullets and graphic summarize this process:

- PFOS creates a tunnel using SSH and public key authentication to a remote server host. The SSH tunnel is created on standard SSH port 22 unless user configures different port.
- The SSH tunnel forwards all data received on the local port to the remote destination port (default 601) over the SSH tunnel.



### Configure PFOS to Send Syslog Messages to Remote Server over SSH Tunnel

**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. PFOS displays the public key in the SSH Public Key area; you must add this key to the list of authorized keys of *username* on the syslog SSH server.

1. From the **System>Syslog** page, click the **Add** button.
2. In the **Hostname** field, enter the server IPv4 or IPv6 address or hostname of the remote server and click the **Add** button. Note that you must have a valid DNS server configuration to be able to configure hostnames.

The screenshot shows a configuration window titled 'Add new Host'. The sub-section is 'Add new Host'. There is a 'Hostname \*' field containing '1.1.1.1'. At the bottom are 'Add' and 'Cancel' buttons.

3. The configuration window for the new Syslog server appears.



1.1.1.1 ×

Protocol	SSH
Default: udp Transport protocol to use	
Port	601
Valid values: 0—65535 Port number	
Severity Level	Emergency
Syslog server severity level filter at which m...	
SSH Port	22
Default: 22 Valid values: 0—65535 Remote SSH port number	
Username *	string
Remote user name	
SSH Public Key	SSH public key
SSH Tunnel Status	down
Default: down SSH tunnel status	

4. Select **SSH** as the transport protocol.
5. In the **Port** field, enter the destination port number on the remote server; the default for SSH is 601.

**Note:** PFOS allows users to enter a port value of "0" without error; however, it is not a valid value, and users should not configure it.

6. Select the minimum severity level to filter Syslog messages forwarded to the remote Syslog server. The Syslog severity levels are shown below:

Severity Level	<input type="button" value="▼"/>
Emergency	
Alert	
Critical	
Error	
Warning	
Notification	
Info	
Debug	

Select the MINIMUM severity level you want to forward to this Syslog server. PFOS forwards messages with the severity you select and the severity levels ABOVE your selected severity.

For example, selecting Critical severity level forwards Critical messages as well as Alert and Emergency severity messages to the this Syslog server.



7. In the **SSH Port** field, enter the port number on which you want PFOS to create the SSH tunnel. This is the port number of the SSH server on the syslog server. Valid values range from 1 to 65535; the default is port 22.
8. In the **Username** field, enter the username for the remote (SSH) server user account.
9. Click **Apply** in the Toolbar to save the changes to the running configuration. PFOS creates the SSH public key and displays it in the **SSH Public Key** field. PFOS generates the key once, so if you set up another SSH endpoint, the same key will be re-used.
10. Add the SSH public key to the list of authorized keys of *username* on the syslog SSH server.

## Trace Log

This section shows the current severity level of the trace logs for specific pre-defined functional areas (facilities). You can change the severity level of a facility, but you cannot delete a facility. To change the severity level of a facility, click the facility name, and select the new level (Emergency, Alert, Critical, Error, Warning, Notification, Info, or Debug).

Trace Log Level	
Facility	Severity
flowmapper	warning
load-balance	warning
access-control	info
system-mgmt	warning
stats-collector	warning
snmp	warning
hal	warning
chassis	info
switch-mgmt	info
port-mgmt	warning
notif-mgmt	warning
app-libs	warning
lcd	warning

## nCM

This setting supports [nGeniusONE PFS Monitoring](#). Configure the nGeniusONE Configuration Manager (nCM) server IP address to which the PFS device will send data.



The screenshot shows the 'System' configuration page with the 'nCM' tab selected. At the top, there are tabs for Basic Information, Network, Source Port VLAN Tagging, Features, Syslog, Trace Log, and nCM. Below the tabs, there is a 'Server' section containing an input field labeled 'ip-address'. The input field has placeholder text 'nCM server address'.

## NMS

The NMS field enables you to configure the IP address or hostname of a PFS Fabric Manager Central Server.

**Note:** This field is only applicable to PFS Fabric Manager 6.0 or later.

The screenshot shows the 'System' configuration page with the 'NMS' tab selected. At the top, there are tabs for Basic Information, Network, Source Port VLAN Tagging, Features, Syslog, Trace Log, nCM, and NMS. Below the tabs, there is a 'Server' section containing an input field labeled 'PFM server address or hostname'. The input field has placeholder text 'PFM server address or hostname'.

## Configuring Notifications

Use the pages listed under **Notifications** on the side menu to configure event and SNMP notification settings.

### Events

Use the Events page to manage notification settings.

The Global Notification Type boxes help you configure all of the tables the same way only on the currently selected tab. Any selected global notification boxes are not stored for subsequent configurations and must be explicitly selected each time you want to use them.



Select the **Config Notifications** tab to configure notifications related to configuration changes:

The screenshot shows the 'Event' page under 'Notification event Settings'. The 'User Notification' tab is selected. There are three main sections:

- Global Notification Type:** Options for All, None, Syslog, SNMP, and NETCONF.
- Port Port configuration events:** A table showing notification types for basic, advanced, and powersafe events. For each, 'Syslog' is checked, while 'None', 'SNMP', and 'NETCONF' are unchecked.
- Traffic Traffic configuration events:** A table showing notification types for map, lbg, lb-criteria, filter, port-group, tool-chain, and tunnel events. For each, 'Syslog' is checked, while 'All', 'None', 'SNMP', and 'NETCONF' are unchecked.

Below these are sections for **System System configuration events** and **Applications Application configuration events**, each with similar tables and notification type checkboxes.

**Note:** For Port Configuration events, configuring advanced notification types has no effect.

Select the **User Notification** tab to configure notifications related to user access:

The screenshot shows the 'Event' page under 'Notification event Settings'. The 'User Notification' tab is selected. There are two main sections:

- Global Notification Type:** Options for All, None, Syslog, SNMP, and NETCONF.
- Authentication User authentication events:** A table showing notification types for access and access-snmp events. For 'access', 'Syslog' is checked, while 'All', 'None', 'SNMP', and 'NETCONF' are unchecked. For 'access-snmp', 'None' is checked, while 'All', 'Syslog', 'SNMP', and 'NETCONF' are unchecked.

**Note:** As of PFOS 5.6.1, the default value for the access-snmp notification setting is "None." Therefore, you need to manually enable it to receive SNMP access notifications (Syslog, SNMP trap, or NETCONF).



Select the **Chassis Notification** tab to configure notifications related to chassis events:

The screenshot shows the 'Event' configuration page with the 'Chassis Notification' tab selected. It includes sections for Global Notification Type, FRU Field Replaceable Units events, Port Line card events, and various chassis management and environment events. Each section has a table where you can enable Syslog, SNMP, or NETCONF notification types for different event categories.

**Note:** The Port **link-state** traps ([link Down and link Up Objects](#) in standard **IF-MIB**) and the **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.

## SNMP

Use the SNMP page to set SNMP agent, community, target, and user-related configuration. See [Configuring SNMP for PFOS](#) for SNMP configuration workflows. Refer to the following sections for details about the SNMP page tabs:

- [Agent](#)
- [VACM](#)
- [USM](#)
- [Target](#)
- [Community](#)
- [Notify](#)
- [Traps](#)



## Agent

Select the **Agent** tab to enable or disable the SNMP agent, and to specify which version(s) of SNMP will be used. PFOS supports SNMP versions 1, 2c, and 3. You can also 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.

**SNMP** SNMP agent, community, target and user related configuration

Agent VACM USM Target Community Notify Traps

Enabled    
Default: Checked  
Enables/Disables the SNMP agent.

Versions:

V 1  V 2c   
V 3

Max Message Size    
Default: 50000  
Valid values: 484—214748364  
The maximum length of SNMP message agent can s...

## VACM

Select the View-Based Access Control Model (**VACM**) tab to:

- Manage VACM groups and MIB views.
- Manage each member of the VACM group and define access rights for groups.
- Manage the subtree for each view.

Agent VACM USM Target Community Notify Traps

**Group** VACM Groups

Add ... Delete

Name
all-rights

Showing 1 to 1 of 1

**View** Definition of MIB views

Add ... Delete

Name
internet

Showing 1 to 1 of 1



From the Group section of the VACM tab, you can add and edit members of the VACM group and define access rights. The following page shows the settings for the **all-rights** group. See [Configuring SNMP for PFOS](#) for SNMP configuration workflows.

The screenshot shows the 'all-rights' group configuration. It includes sections for 'Member' (listing public and remote users with security models v1, v2c, and usm) and 'Access' (listing 'any' with no-auth-no-priv security level and internet read/write/notify views).

## USM

Select the User-based Security Model (**USM**) tab to add users and set authentication and privacy settings in the User-based Security Model.

The screenshot shows the 'myuser' USM user configuration. It includes fields for Authentication (md5 selected), Password, Privacy (des selected), and another Password field.

## Target

Select the **Target** tab to specify SNMP target addresses and security model(s) to use.

The screenshot shows the '127.0.0.1 v2' target configuration. It includes fields for IP (127.0.0.1), UDP Port (6000), Tag (std\_v2\_trap), and Security Models (v1, v2c selected, usm). A note indicates that v2c is the default security model.



## Community

Select the **Community** tab to configure the list of SNMP communities.

The screenshot shows a software interface for managing SNMP communities. At the top, there is a navigation bar with tabs: Agent, VACM, USM, Target, Community, Notify, and Traps. The 'Community' tab is selected. Below the navigation bar, the title 'List of communities' is displayed. Underneath this, there is a table with two rows. The first row contains the name 'mycomm'. The second row contains the name 'public'. At the bottom right of the table, it says 'Showing 1 to 2 of 2'.

Name
mycomm
public

## Notify

Select the **Notify** tab to specify which targets will receive notifications.

The screenshot shows a software interface for managing notification targets. At the top, there is a navigation bar with tabs: Agent, VACM, USM, Target, Community, Notify, and Traps. The 'Notify' tab is selected. Below the navigation bar, the title 'Targets that will receive notifications' is displayed. Underneath this, there is a table with three rows. The first row contains 'std\_v1\_trap' in the Name column, 'std\_v1\_trap' in the Tag column, and 'trap' in the Type column. The second row contains 'std\_v2\_trap' in the Name column, 'std\_v2\_trap' in the Tag column, and 'trap' in the Type column. The third row contains 'std\_v3\_trap' in the Name column, 'std\_v3\_trap' in the Tag column, and 'trap' in the Type column. At the bottom right of the table, it says 'Showing 1 to 3 of 3'.

Name	Tag	Type
std_v1_trap	std_v1_trap	trap
std_v2_trap	std_v2_trap	trap
std_v3_trap	std_v3_trap	trap



## Traps

Select the **Traps** tab to specify which SNMP traps will be enabled. Refer to [Traps/Notifications](#) for details about the traps.

The screenshot shows the 'SNMP' configuration page with the 'Traps' tab selected. At the top, there are three global enablement options: 'Link up Down' (checkbox), 'All' (radio button), and 'None' (radio button). Below this, the 'System' section contains several trap types, each with its own enablement checkbox. The trap types include Temperature, File Mgmt, Health Stats, Tunnel State, Enhanced Link up Down, and others like pfsMesh, Health Check State, Restart, Stripping, Access, Fru, High Availability, Trigger Policy, and Access SNMP. The 'SNMP' section at the bottom contains a single trap type, 'Coldstart', with its enablement checkbox checked.

**Note:** The **Link up Down** traps ([link Down and link Up Objects in standard IF-MIB](#)) and the **Enhanced Link up Down** traps ([vsLinkUpNotif and vsLinkDownNotif in proprietary VSS-SYSTEM-MIB](#)) are similar traps, but the Enhanced Link up Down 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.

## Configuring Time Settings

Use the **Timing Sources** page to set the system time manually or by specifying one to three NTP servers. For PFS 6000s, you can also configure settings for GPS and PTP and view the current time source.

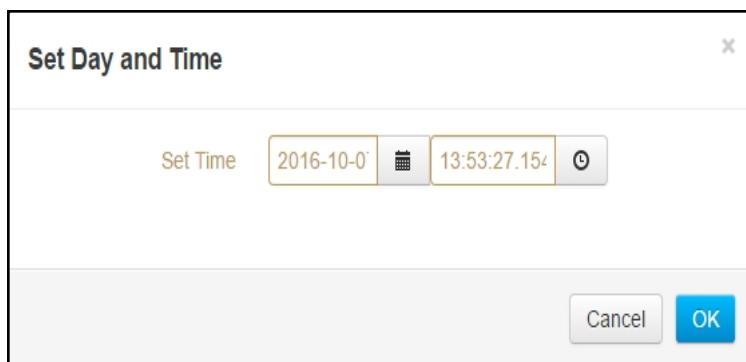
**Note:** If a PFS 5000/7000 Series or third-party hardware system loses power for more than a few seconds, its system clock resets to 2001-01-01. For a more accurate and reliable time, ensure that an NTP server is defined correctly.

### Manual Time Setting (Clock)

Select the **Clock** tab to set time manually. Click **Set** and use the calendar and clock icons to specify the time. Click **OK** to implement the settings. Click **Apply** in the Toolbar to save the changes to the running configuration. The Manual timing setting is disabled if an NTP server is

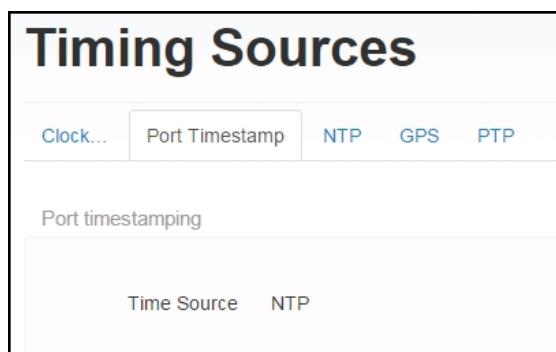


configured.



## Port Timestamp

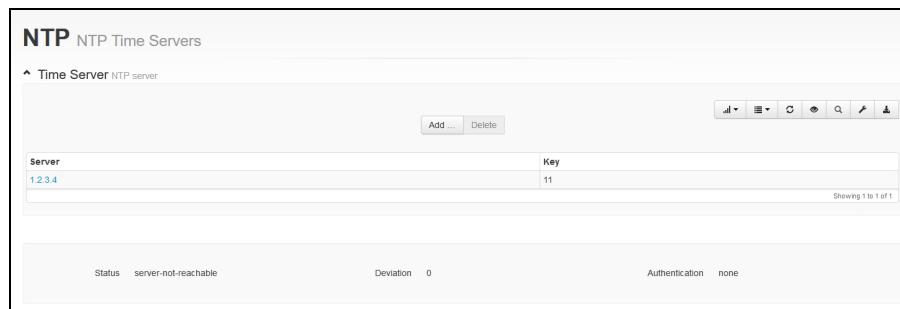
This tab is read-only. It displays the current time source.



## NTP

Select the **NTP** tab to specify up to three Network Time Protocol (NTP) servers to provide updated time to the system clock. The NTP protocol will automatically select the best of the three available time sources to synchronize to.

Additionally, Secure Network Time Protocol allows authentication of time server so only approved time sources provide time values. Users [upload an NTP authentication key file](#) and select the corresponding key while setting the NTP server.





You can view the following status fields for NTP.

**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 for time synchronization.

Status	<ul style="list-style-type: none"><li>• <b>server-not-reachable:</b> No NTP server is reachable.</li><li>• <b>syncing:</b> The system time is synchronized to one of the NTP servers.</li><li>• <b>running:</b> NTP is running but has not started to synchronize to any NTP server.</li><li>• <b>not-running:</b> No NTP server is configured.</li></ul>
Authentication	<ul style="list-style-type: none"><li>• <b>ok:</b> Authentication is successful. The "ok" status only displays while the status is "syncing."</li><li>• <b>bad:</b> Authentication failed.</li><li>• <b>None:</b> No authentication is configured for this NTP server.</li></ul>
Deviation	Displays the amount of time the system clock deviates from the NTP source at the last update.

## Add an NTP Server

**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. 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](#) for details.

1. Access **Timing Sources > NTP**.
2. In the Time Server area, click **Add**. The Add New Time Server dialog appears



3. Enter the **IP Address, Domain Name, or URL** (such as, us.pool.ntp.org) and click **Add**. A dialog appears prompting you to enter the authentication key for this server.
4. 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.



### 1.2.3.4 ×

Key  x

Default: 0

Authentication key, 0 for no authentication

- Click **Apply** in the Toolbar to save the changes to the running configuration. After NTP synchronization is configured, up to five minutes can elapse before the first synchronization with the external server occurs. After that, the system clock is resynchronized once every five seconds.

## GPS

**Note:** GPS timing source is only applicable for the PFS 6000 Series.

Select the **GPS** tab to view GPS status and specify the maximum cable length between the system chassis and a GPS receiver. Enter a cable length between 1 and 300 meters (1 is the default).

Click **Apply** in the Toolbar to save the changes to the running configuration.

### Timing Sources

Clock... Port Timestamp NTP GPS PTP

Status GPS not connected

Satellite Count 0

Default: 0

Cable Length  x

Default: 1

Valid values: 1—300

## PTP

**Note:** This tab is only applicable for the PFS 6000 Series. For PTP timing support for PFS 5000/7000 devices, see [Linux PTP](#).



Select the **PTP** tab to configure settings for Precision Time Protocol.

The screenshot shows the PTP configuration page with the following fields:

- Enable PTP: Set to **Enable** (Default: disable)
- Status: PTP cable disconnected
- IP Address: 224.0.1.129/24 (Default: 224.0.1.129/24)
- Domain: 0 (Default: 0, Valid values: 0—255)
- Announce Msg Interval: 1 (Default: 1, Valid values: -4—5)
- Announce Recv Timeout: 3 (Default: 3, Valid values: 2—10)
- Sync Interval: 0 (Default: 0, Valid values: -8—2)
- DHCP: Disable (Default: disable)
- Transport: UDP (Default: udp)
- Port: PTP (Default: ptp)
- Delay Mechanism: End End (Default: end\_end)
- PPS Source: PTP Port (Default: ptp\_port)
- Telecom Profile: Disable (Default: disable)

The following table shows the settings. After specifying the configuration, click **Apply** in the Toolbar to save the changes to the running configuration.

Enable PTP	Enables PTP for time setting (default is disable). When you select Enable, the additional fields are shown.
IP Address	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.
Domain	Specifies the PTP domain (1-255, default 0).
Announce Msg Interval	Configures the interval between PTP announcement messages (-4 to 5, default 1).
Announce Recv Timeout	Configures the number of attempts before timeout of receive messages (2 to 10, default 3).
Sync Interval	Configures the synchronization interval (-8 to 2, default 0).
DHCP	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.
Transport	Specifies the transport type for PTP messages (Ethernet or UDP, default UDP).
Port	Specifies the port as Ethernet or PTP (default PTP).
Delay Mechanism	Configures either end-to-end or peer-to-peer for PTP delay messages (default is end-end).
PPS Source	Specifies the source for pulse per second (PPS) (default is ptp_port). If you specified ptp_connector, you can also specify a maximum cable length for the distance between the system chassis and the PTP receiver (1-300m, default 10m).
Telecom Profile	Enable or disable the telecom profile.



## Linux PTP

### Notes:

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

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.

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.

Select the **Linux PTP** tab to configure settings for Linux-assisted PTP timing.

Status	NA	Clock Info	NA
Linux-PTP Status		Linux-PTP clock data	
Linux PTP	Enable	Domain Number	0
Default: disable Enable/disable Linux-PTP service (Disable)		Default: 0 Valid values: 0—255 Domain number assigned to a group of Linux-PTP...	
PTP Delay Mechanism	Auto	Hybrid Mode	<input type="checkbox"/> Linux PTP Hybrid mode
Default: Auto Linux PTP delay mechanism			

Status	Displays the Linux PTP status. <ul style="list-style-type: none"><li>• NA - Linux-ptp is not enabled.</li><li>• Syncing - Linux-ptp is enabled and is syncing time with network PTP clocks.</li><li>• Not Syncing - Linux-ptp is enabled but is not receiving valid PTP timing data.</li></ul>
Clock Info	Displays the Linux PTP clock info. <ul style="list-style-type: none"><li>• NA - Linux-ptp is not enabled.</li><li>• Clock data varies depending on current state</li></ul>
Linux PTP	Enables Linux-assisted PTP for time setting (default is disable). When you select Enable, the additional fields are shown.



Domain Number	Number assigned to a group of PTP clocks that synchronize to each other in the network. Valid values are 0 to 255.
PTP Delay Mechanism	Choose the mechanism for measuring the communication path delay between the PTP server and client: <b>Auto:</b> PFOS selects appropriate delay measurement <b>E2E:</b> End-to-end delay measurement <b>P2P:</b> Peer-to-peer delay measurement <b>None:</b> No delay measurement
Hybrid Mode	<b>Note:</b> 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. <ul style="list-style-type: none"><li>• <b>Enable:</b> 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.</li><li>• <b>Disable:</b> 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.</li></ul>

## Configuring Access Control

The Access Control Page provides the following settings for controlling access to PFOS:

- [User Access \(Roles and Users\)](#)
- [Password Policies](#)
- [Remote Authentication](#)
- [Remote Authorization](#)
- [Session Limit](#)
- [User and IP Lockout Settings](#)
- [Client IP Lockout](#)
- [Firewall Rules](#)

### User Access (Roles and Users)

To ensure security in the management of PFOS, access to PFOS is password-protected. The initial factory default setting is username **admin** and password **admin**; the admin password must be changed upon initial login. PFOS enables you to configure role-based local access control. First you [add roles](#) on the **Role tab**, then [add users](#) on the **Users tab** and assign roles to them.

**Note:** Because PFOS has multiple management interfaces and is multi-user, there is the possibility of multiple users attempting to control the unit at the same time. If multiple users try to change the same setting at the same time, only the most recent saved changes are used going forward.



Users and their roles can also be defined remotely; refer to [Remote Authentication](#) and [Remote Authorization](#).

## Add a Role

**Note:** PFOS supports a maximum of 100 roles.

1. Open the **Role** tab on the Access Control page.
2. Click **Add**, enter a name for the role, and click **Add**.

**Note:** 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).

3. A page for the new role (Operator in the following figure) opens.

4. (Optional) Add a description.
5. Click **Add** in the Rule area to define rules for the role.
6. Enter a name for the rule, and click **Add**. Click the icon to the right of the Feature field to display the available feature areas.

7. Select the checkbox for the desired feature (component). You can select only one feature per rule. Use the page controls near the bottom of the page to display additional options.



Refer to [Rule Component Feature Descriptions](#) for feature access details.

Component	
Name	Access Operation
Access Control	create read update delete
All	create read update delete exec
Features	create read update delete exec
File Management	create read update delete exec
Filter	create read update delete
LCD	create read update delete exec
Load Balance	create read update delete
Load Balance Criteria	create read update delete
Logging	create read update delete
Network Data	create read update delete

**1 2**

**OK Cancel**

8. Click **OK**.
9. Select the type of access to provide (create, read, update, delete and/or execute) and the context (CLI, Web UI, NETCONF, or all). Only one context can be selected per rule. To allow the same type of access in multiple contexts (such as through both the CLI and the Web UI), create multiple rules for the same component.

Feature \*  ...

(

Access  Create  Read  Update  Delete  Exec

Access operations associated with this feature

Context  Context associated with this rule.

10. Click **Apply** to save the settings and **OK** to confirm.
11. Click the **Role** breadcrumb near the top of the page to return to the role definition page.





## Rule Component Feature Descriptions

The following table provides descriptions for the features to which you can control access by creating rules.

Component Name	Description	For More Information, Refer To:
Access Control	Allows users to configure access control settings including user creation, password policies, remote authorization/authentication, session limits, lockout settings and firewall rules.  Global Settings>Access Control	<a href="#">Configuring Access Control</a>
Advanced Applications	Allows users to configure advanced applications. Accessible tabs vary depending on PFS model.  <b>All PFS Models:</b> Libraries>Applications>Tunnel Termination Libraries>Applications>Healthcheck	<b>All PFS Models</b> <ul style="list-style-type: none"><li>• <a href="#">IP Tunnel Termination</a></li><li>• <a href="#">Health Check Profiles</a></li></ul>
	<b>PFS 5000/7000 Series-Specific</b> Libraries>Applications>Standard Stripping	<b>PFS 5000/7000 Series-Specific</b> <a href="#">Standard Stripping</a>
	<b>PFS 6000 Series-Specific</b> Libraries>Applications>Deduplication Libraries>Applications>VLAN Tag Stripping Libraries>Applications>Slicing Libraries>Applications>Protocol Stripping Libraries>Applications>Extended LB	<b>PFS 6000 Series-Specific</b> <ul style="list-style-type: none"><li>• <a href="#">Packet Deduplication</a></li><li>• <a href="#">VLAN and VN Tag Stripping</a></li><li>• <a href="#">Conditional Packet Slicing</a></li><li>• <a href="#">Protocol De-encapsulation and Stripping</a></li><li>• <a href="#">Extended Load Balancing</a></li></ul>
All	Allows users to configure all features and functionality.	
Features	Allows users to configure system-wide feature settings.  Global Settings>System>Features	<a href="#">Features</a>
File Management	Allows users to upload/download different file types. File types that can be managed include configuration, software, firmware, log, certificates and keys.  System Administration>File Management	<ul style="list-style-type: none"><li>• <a href="#">PFOS Licensing</a></li><li>• <a href="#">PFOS Maintenance</a></li></ul>
Filter	Allows users to configure traffic filter settings.  Libraries>Forwarding Filters	<ul style="list-style-type: none"><li>• <a href="#">Traffic Filtering</a></li><li>• <a href="#">PFOS Packet Fields in Filter Expressions</a></li></ul>
LCD	Allows users access to a global setting that enables/disables the LCD display and keyboard on the front panel of the PFS 6000 Series.  Global Settings>System>Features>Front Panel	<a href="#">Front Panel (PFS 6000 Series)</a> <a href="#">Front Panel LCD Screen</a> <a href="#">PFS 6000 Series Hardware Installation Guide</a>
Load Balance	Allows users to configure Load Balance Groups.  Configuration>Load Balance Groups	<a href="#">Traffic Load Balancing</a>



Component Name	Description	For More Information, Refer To:
Load Balance Criteria	Allows users to configure Load Balance Criteria. Libraries>Load Balance Criteria	<a href="#">Traffic Load Balancing</a>
Logging	Allows users to configure Syslog settings including severity level for Syslog history and defining Syslog servers for PFOS to send Syslog messages. Global Settings>System>Syslog	<a href="#">Syslog</a>
nCM	Allows users to configure the IP address of an nGeniusONE Configuration Manager (nCM) server to which the PFS device will send data. Global Settings>System>nCM	<ul style="list-style-type: none"><li><a href="#">nCM</a></li><li><a href="#">nGeniusONE PFS Monitoring</a></li></ul>
NMS	Allows users to configure the IP address or hostname of a PFS Fabric Manager Central Server. Global Settings>System>NMS	<a href="#">NMS</a>
Network Data	Allows users to configure network settings including enabling/disabling DHCP and configuring static network connection details. Global Settings>System>Network	<a href="#">Network Settings</a>
Notifications	Allows users to configure the types of notifications PFOS displays. Notifications>Events	<a href="#">Configuring Notifications</a>
	Allows users to acknowledge alarm notifications. Status>Event Notifications>Alarms	<a href="#">Event Notifications</a>
Password management	Allows users to update all users' passwords. <b>Note:</b> Users with <b>only</b> the Password management feature are not able to change other users' passwords in the Web UI (only via other interfaces such as the CLI).	<a href="#">Password Policies</a>
pMesh	Allows users to configure a pfsMesh using the pStack or pStack+ protocols (pStack+ requires the pStack+ license). Status>pfsMesh	<ul style="list-style-type: none"><li><a href="#">pfsMesh</a></li><li><a href="#">pfsMesh Using pStack+</a></li></ul>
Port Groups	Allows users to configure port groups. Configuration>Port Groups	<a href="#">Port Groups</a>
Ports	Allows users to configure port settings. Configuration>Ports Settings	<a href="#">Configuring Ports</a>
PowerSafe	Allows users to configure PowerSafe settings. Configuration>PowerSafe	<a href="#">PowerSafe</a>
Rollback	Allows users to use the Rollback feature to revert to a previously applied configuration. Toolbar>Rollback	<a href="#">Rollback</a>



Component Name	Description	For More Information, Refer To:
SNMP	Allows users to configure SNMP settings including SNMP agent, community, target and user related configuration. Notifications>SNMP	<a href="#">Configuring SNMP for PFOS</a>
System	Allows users to configure Basic Information including device name, location, contact information, and banner text. Global Settings>System>Basic Information	<a href="#">Basic Information Settings</a>
Timing Source	Allows users to configure timing sources, including NTP, and GPS and PTP for PFS 6000s. Global Settings>Timing Sources	<a href="#">Configuring Time Settings</a>
Tool Chain	Allows users to configure simple and advanced inline tool chains. Configuration>Tool Chain	<ul style="list-style-type: none"><li>• <a href="#">Tool Chains</a></li><li>• <a href="#">Simple Tool Chaining</a></li><li>• <a href="#">Advanced Tool Chaining</a></li></ul>
Trace Log	Allows users to change the severity level of trace log facilities (such as flowmapper, load-balance, access-control). Global Settings>System>Trace Log	<a href="#">Trace Log</a>
Traffic Maps	Allows users to configure traffic maps. Configuration>Traffic Maps	<a href="#">Traffic Maps</a>
Triggers	Allows users to configure trigger policies. Configuration>Trigger Policies	<a href="#">Trigger Policies</a>
Tunnel	Allows users to configure L2GRE and/or VXLAN origination/termination tunnels. Configuration>Tunnel Settings	<ul style="list-style-type: none"><li>• <a href="#">L2GRE Tunnel Origination/Termination Support</a></li><li>• <a href="#">VXLAN Tunnel Origination/Termination Support</a></li></ul>
VLAN Settings	Allows users to configure Source Port VLAN Tagging settings (TPID Ether type and Starting VLAN ID). Global Settings>System>Source Port VLAN Tagging	<a href="#">Source Port VLAN Tagging</a>

## Add a New User

**Note:** PFOS supports a maximum of 100 users.

1. On the Access Control page, click **Users**, and then click **Add**.
2. Enter the user name, and then click **Add**. User names support upper and lower case alphanumeric ASCII characters and limited special characters. User names cannot contain spaces.
3. Enter a password (that is compliant with [password policies](#)), and then re-enter the same password to confirm.
4. Click the icon to the right of the Role field, select one or more roles to apply, and click **OK**.
5. Click **Apply** in the Toolbar to save the changes to the running configuration.



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

## List Currently Configured Users

1. On the Access Control page, click **Users**.
2. The list of users displays, along with the password dates and invalid login details.

Local user management						
		Add ...		Delete		
Name	Role	Last Password Change	Password Expires	Invalid Login Attempts Count	First Invalid Login Time	Account Lock Time
admin	admin	Oct 12, 2019	Feb 26, 2047	0		
jsmith	role_file_management, role_time_source	Oct 12, 2019	Feb 26, 2047	0		

Showing 1 to 2 of 2

## Delete One or More Users

1. On the Access Control page, click **Users**.
2. In the list of users that displays, click on the desired lines to select one or more users.
3. Click **Delete**. On the confirmation pop-up that displays, click **Yes**.
4. Click **Apply** in the Toolbar to save the changes to the running configuration.

**Note:** The *admin* user cannot be deleted. If PFS Fabric Manager is in use, the *pfmadmin* user should not be deleted.

## Change a Password

**Note:** Only the **admin** user can change the password for **admin**. The password for other users with the Admin role can be changed by any user who has been granted the Admin role.

1. Click the user name on the Access Control page.
2. Enter the new password (that is compliant with [password policies](#)) and re-enter to confirm.
3. Click **Apply** in the Toolbar to save the changes to the running configuration.

## Password Policies

Admins can define system-wide password policies which include [password expiration](#) and [minimum password length and character requirements](#).



## Password Expiration

PFOS enforces a system-wide limit on the maximum number of days before a locally configured user's password must be changed. The default limit is 9,999 days (about 27.4 years), but you can set this limit to any number of days between 1 and 9,999.

### Configure Password Expiration

**Note:** Password expiration limits apply only to local authentication. This setting has no effect on external authentication through RADIUS, TACACS, or LDAP.

1. Open the **Access Policy** tab on the Access Control page and click **Password**.
2. In the Expiration field, enter the number of days user passwords are valid before expiring.

Expiration (days)  x  
Default: 9999  
Valid values: 1—9999  
Maximum number of days between password change (9999)

3. Click **Apply** in the Toolbar to save the changes to the running configuration. The password expiration dates for all local users are updated and can be viewed in the Users tab on the Access Control page.

## Minimum Password Length and Character Requirements

PFOS enforces system-wide settings for minimum password length and minimum number of character types.

### Configure Password Length and Character Requirements

**Note:** Password length and character limits apply only to local authentication. These settings have no effect on external authentication through RADIUS, TACACS, or LDAP. Refer to [Remote Authentication](#) for PFOS password restriction when the login is authenticated by an external RADIUS, TACACS, or LDAP server.

1. Open the **Access Policy** tab on the Access Control page and click **Password**. The Password User access control password policy page appears.

Length  x Uppercase  x Lowercase  x  
Default: 5  
Valid values: 5—128  
Minimum password length  
Numerical  x Special  x Positions Changed  x  
Default: 0  
Valid values: 0—128  
Minimum number of numerical characters required...  
Default: 0  
Valid values: 0—128  
Minimum number of special characters required...  
Default: 0  
Valid values: 1—128  
Minimum number of character positions within t...

2. In the **Minimum** area, specify the following character requirements for user passwords (valid values range from 0-128, except for Length which has a minimum of 5):



- **Length:** Minimum password length (default is 5).
  - **Uppercase:** Minimum number of uppercase letters required (default is 0).
  - **Lowercase:** Minimum number of lowercase letters required (default is 0).
  - **Numerical:** Minimum number of numerical characters required (default is 0).
  - **Special:** 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.
  - **Positions Changed:** 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.
3. Click **Apply** in the Toolbar to save the changes to the running configuration. The password length and character limits for all local users are updated and can be viewed in the Users tab on the Access Control page.

## Notifications about Password Policies

PFOS can notify users of the following events:

- If any password policy length or character requirement parameter is changed
- If a user's password is going to expire in seven days, PFOS can generate Syslog, SNMP, and NETCONF notification warnings about password expiration. The warnings are issued daily at midnight.
- If all seven days pass without changing the password, the user will be prompted to change their password during every login attempt. A notification message is generated that the password has expired for that user.

To receive these warnings, enable user authentication access notifications as desired on the **Notifications > Events > User Notification** page.

To enable just SNMP notifications about password expiration, go to the **Notifications > SNMP > Traps** page, scroll down to the **System** section, and select **Access**.

## Remote Authentication

PFOS users can be defined locally (see [User Access \(Roles and Users\)](#)) and/or on one or more remote AAA servers. This section explains how to configure PFOS for remote user authentication. You can specify which authentication types (Local, [RADIUS](#), [TACACS](#), and [LDAP](#)) are active and the [order in which they are used](#).

### Notes:

- When using remote authentication, it is generally required to configure [remote authorization](#) as well.



- If using [sshpubkeys](#) and remote authentication is configured:
  - Without [Common Criteria Mode](#) or [FIPS Mode](#) enabled, local users can login to PFOS by public key authentication without a password; remote authentication is not needed.
  - With Common Criteria Mode or FIPS Mode enabled, all users need remote authentication to login.
- PFOS cannot support the semicolon (;) or backslash (\) characters in passwords for external authentication through RADIUS, TACACS, or LDAP even though these special characters may be supported at the authentication server.

Refer to the following sections for details:

- [Remote Authentication](#)
- [Add a RADIUS Server](#)
- [Add a TACACS Server](#)
- [Add an LDAP Server](#)
- [CLI Remote Authentication with FIPS or Common Criteria Modes Enabled](#)

## Configure Authentication Order

When remote authentication is configured, PFOS attempts to authenticate users with each configured authentication server. If the server that is next in line is reached but fails to authenticate, the login attempt is refused, and no attempt to try another server is done. If the server is not reachable, PFOS attempts to reach the next server in line. Authentication fails if none of the servers are reachable. Because Local authentication is always reachable, remote AAA servers will not be used if Local authentication is placed first in the authentication order.

You can define the order in which sources are used for authentication. The default is only Local authentication. In a list of multiple authentication types, Local must be either first or last; it cannot be in the middle.

1. Open the **Authentication** tab on the Access Control page.
2. Click the Order entry field to add a new authentication type. Select the type, and click **Add**.
3. Add additional types as needed. Local must be present, and it must be first or last. To change an entry, click it, make another selection, and click **Update**.

The screenshot shows the 'Access Control' page with the 'Authentication' tab selected. Below the tabs, there is a note: 'Authentication related settings, like order, etc.' Under the 'Order' heading, there is a dropdown menu containing 'Local' and 'Radius'. To the right of the dropdown is a separate input field containing 'Ldap'. At the bottom of the 'Order' section is a note: 'Defines the authentication order'. Below the 'Order' section are three buttons: 'Update' (blue), 'Add' (white), and 'Cancel' (white).



## Add a RADIUS Server

Perform the following steps to add a RADIUS Server.

### Prerequisites:

- If using a RADIUS server with FIPS or Common Criteria modes, refer to [CLI Remote Authentication with FIPS or Common Criteria Modes Enabled](#) prior to adding the server.
  - A RADIUS certificate must be installed **prior** to enabling TLS.
- Open the **Radius Server** tab on the Access Control page.
  - Click **Add**, enter either an IP address or a fully qualified domain name to identify the server, and click **Add**. 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.
- Specify the following settings based on the configuration of your RADIUS server:

Setting	Description
Port	Port for access to the server (default 0).
Key	For UDP, this is the AES encrypted string to authenticate to the server. RADIUS keys have the following limitations: <ul style="list-style-type: none"><li>Backslash "\" characters in keys must be entered as a double backslash "\\". For example, the key "test\123" must be entered as "test\\123".</li><li>Keys cannot start with "\$8\$". For example, key "\$8\$TestKey" is not supported.</li></ul> For TLS, PFOS ignores this field and uses an internally defined key. <b>Note:</b> 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.
Timeout	Time after which requests to the server time out (default 30 seconds)
Retransmit	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.
Protocol	Transport protocol: UDP or TLS. A RADIUS certificate must be installed before enabling TLS; see <a href="#">Maintaining Certificate Files</a> for details. <b>Note:</b> PFOS supports RADIUS over TLS functionality when <a href="#">Common Criteria mode</a> is enabled; however, this functionality is not compliant to Common Criteria requirements.

- Click **Apply** in the toolbar to save the changes to the running configuration.

## Add a TACACS Server

Perform the following steps to add a TACACS Server.

**Prerequisite:** If using a TACACS server with FIPS or Common Criteria modes, refer to [CLI Remote Authentication with FIPS or Common Criteria Modes Enabled](#) prior to adding the server.



1. Open the **Tacacs Server** tab on the Access Control page.
2. Click **Add**, enter a name (either an IP address or a fully qualified domain name) to identify the server, and click **Add**. Note that you must have a valid DNS server configuration to be able to configure hostnames.
3. Specify the following settings based on the configuration of your TACACS server:

Setting	Description
Port	Port for access to the server (default 49).
Key	AES encrypted string to authenticate to the server. TACACS keys have the following limitations: <ul style="list-style-type: none"><li>• Backslash "\" characters in keys must be entered as a double backslash "\\\". For example, the key "test\123" must be entered as "test\\123".</li><li>• Keys cannot start with "\$8\$". For example, key "\$8\$TestKey" is not supported.</li></ul>
Service	TACACS service parameter.
Prompts	TACACS prompts parameter.
Timeout	Time after which requests to the server time out (default 30 seconds).
Retransmit	Number of times PFOS attempts to contact the TACACS server (default 3).

4. Click **Apply** in the toolbar to save the changes to the running configuration.

## Add an LDAP Server

Perform the following steps to add a LDAP Server.

**Prerequisite:** If using a LDAP server with FIPS or Common Criteria modes, refer to [CLI Remote Authentication with FIPS or Common Criteria Modes Enabled](#) prior to adding the server.

1. Open the **LDAP Server** tab on the Access Control page.
2. Click **Add**, enter a name (either an IP address or a fully qualified domain name) to identify the server, and click **Add**. Note that you must have a valid DNS server configuration to be able to configure hostnames.

**Note:** If enabling TLS and Certificate Authentication, PFOS requires the fully qualified domain name.



3. Specify the following settings based on the configuration of your LDAP server:

Setting	Description
Port	Port used to connect to the LDAP Server. Authentication fails if using incorrect port numbers.
Timeout	Maximum time (in seconds) that PFS waits for a response from the LDAP server (default 30 seconds).
Retransmit	Number of times PFS attempts to contact the LDAP server (default 3).
TLS	<b>Note:</b> PFOS supports LDAP over TLS functionality when <a href="#">Common Criteria mode</a> is enabled; however, this functionality is not compliant to Common Criteria requirements. Enable - PFOS connects to LDAP server over Transport Layer Security (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. See also <a href="#">Maintaining Certificate Files</a> .
Binding Mode	Select mode for binding to LDAP server: <ul style="list-style-type: none"><li>• Anonymous - allows PFS to connect and search the directory (bind and search) without first authenticating using binding DN and password to log in.</li><li>• Authenticated - PFS connects to the LDAP server using the configured Binding DN and Binding password.</li></ul>
Binding DN	<b>Note:</b> 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	<b>Note:</b> 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.
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.
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.

4. Click **Apply** in the toolbar to save the changes to the running configuration.

## CLI Remote Authentication with FIPS or Common Criteria Modes Enabled

For CLI remote TACACS, RADIUS, or LDAP authentication login under [FIPS](#) and/or [Common Criteria](#) mode, you must configure and apply the external authentication servers and authentication order first (no need to log out), before enabling FIPS or Common Criteria modes.

**Note:** If LOCAL authentication is currently configured with FIPS/Common Criteria mode enabled, deselect FIPS and/or Common Criteria modes on the System>Features page and apply the changes **prior** to performing the following steps.



Perform the following steps.

1. [Add a RADIUS , TACACS server, or LDAP server.](#)
2. [Configure Authentication Order.](#)
3. Apply the settings.
4. From System>Features, select [FIPS Mode](#) and/or [Common Criteria Mode](#).
5. Apply the settings.

## Remote Authorization

**Note:** The details of configuring external AAA servers are beyond the scope of this guide. For more information, refer to the documentation for specific servers.

When using [remote authentication](#), it is generally required to configure remote authorization as well. With remote authorization, the external AAA server also provides user authorization by specifying the name of the user's role.

On RADIUS and TACACS+ servers, the user's role must be specified in a Shell Attribute at Access Control List (ACL), and set as "groups=roleName" (with both double quotes) in which roleName is the name of the role defined at PFOS Access Control. With LDAP, the user is assigned a role if a PFOS role matches the name of a group of which the user is a member. See the Group Attribute setting for details on how LDAP group membership is determined.

**Note:** On RADIUS and TACACS+ servers, when assigning remote users to multiple groups, ensure Access Control List (ACL) group assignment is configured in a one line format, such as "groups=role1,role2,role3".

Authorization role details (the permissions that the role has) must be configured on PFOS. The AAA server will include the role name in its response; PFOS will read the role information from the response and apply the permissions of that role to the user. As noted in [User Access \(Roles and Users\)](#), users with no assigned roles (such as, if no role name is provided by the AAA server) will not have permission to read, write, or execute any commands or functions after logging in. Similarly, if the role name specified by the AAA server does not exist in PFOS, the user will not have permission to read, write, or execute any commands or functions after login.

**Note:** Roles assigned by the AAA server are logged in Syslog (see [Syslog History](#) or show logging CLI command).

## 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

### Limit Concurrent Sessions

Perform the following to limit concurrent sessions.



1. Open the **Access Policy** tab on the Access Control page.
2. In the Login section, click the **Session Limit** checkbox to enable it.
3. In the **Session Limit Max** field, type the number of maximum concurrent sessions you want to limit per user.
4. Click **Apply** in the Toolbar to save the changes to the running configuration.

**Note:** If total current sessions is greater than the configured maximum when you enable this option, PFOS will not allow new sessions and will not end any current sessions. To ensure that total sessions is limited to the configured maximum, NETSCOUT recommends rebooting the device prior to enabling this option. Also, users must close the session properly to decrease the session count. For example, in an SSH session, the user must type exit and press Enter to close the session properly. For a Web session, the user must click the Logout option to close the session properly. Also, if a connection is lost, the particular session may still exist until the idle timeout occurs (default is 30 minutes).

The screenshot shows a configuration interface for 'User login session limit settings'. It includes a 'Session Limit' checkbox (checked), a 'Session Limit Max' input field containing '3', and a note about the default value being 3 with valid values ranging from 1 to 3. The note also specifies that it is the 'Maximum login session limit'.

## User and IP Lockout Settings

You can configure various settings for controlling user and IP lockout caused by failed user login attempts.

Lockout Setting	Description
<b>User Lockout Failed Attempts Max</b>	You can configure the number of <a href="#">failed login attempts</a> that PFOS allows before a user account (local accounts only) or IP address (unknown usernames or remote accounts) is locked out. These settings are enabled by default with a value of 5.
<b>IP Lockout Failed Attempts Max</b>	
<b>User Lockout Disable</b>	When this option is checked, PFOS does not limit the number of failed user login attempts. This option is disabled (unchecked) as a default; therefore, PFOS will lock user accounts based on the configured maximum failed attempts.
<b>IP Lockout Disable</b>	When this option is checked, PFOS does not limit the number of failed login attempts from an IP address. This option is disabled (unchecked) as a default; therefore, PFOS will lock IP addresses based on the configured maximum failed attempts.
<b>User Lockout Duration</b>	You can configure the number of minutes users are locked out after failed login attempts. Valid values are 5-60; 60 is the default.



**Access Control**

Role   Users   **Access Policy**   Client IP Lockout   Firewall Rules   Authentication   Radius Server   Tacacs Server

**>Password** User access control password policy

**Login** User login session limit settings

Session Limit  Enable Login session limit

User Lockout Disable  Disable user lockout based on failed login attempts

User Lockout Failed Attempts Max  x Default: 5 Valid values: 1—5 Number of failed user login attempts before the user is locked out

User Lockout Duration (minutes)  x Default: 60 Valid values: 5—60 Number of minutes the user will be locked out

IP Lockout Disable  Disable IP lockout based on failed login attempts

IP Lockout Failed Attempts Max  x Default: 5 Valid values: 1—5 Number of failed login attempts before an IP address is locked out

## Configure User and IP Lockout Settings

**Note:** The settings do not affect the current failed login count.

1. Open the **Access Policy** tab on the Access Control page.
2. Perform one of the following:
  - To configure maximum login attempts, in the **User Lockout Failed Attempts Max** and/or the **IP Lockout Failed Attempts Max** fields, type the number of failed login attempts you want PFOS to allow before a user is locked out (default is 5).
  - To disable the lockout feature so there is no limit to the number of failed user login attempts, check either of the following **User Lockout Disable** and **IP Lockout Disable** options.
    - **User Lockout Disable** - when this option is checked, PFOS does not limit the number of failed user login attempts.
    - **IP Lockout Disable** - when this option is checked, PFOS does not limit the number of failed login attempts from an IP address.
3. To modify the **User Lockout Duration** (default is 60 minutes), enter a new value between 5-60 minutes. The new duration takes effect immediately and applies to the next user lockout.
4. Click **Apply** in the Toolbar to save the changes to the running configuration. The new settings will take effect when the next login attempt occurs; existing sessions are not affected.

You can view failed login attempts count and times and account lockout times on the [Users](#) and [Client IP Lockout](#) tabs in Access Control.

## Client IP Lockout

This page displays statistics for IP invalid login attempts counts and times.

IP Address	Invalid Login Attempts Count	First Invalid Login Time	IP Lock Time
1.2.3.4	1	2019-10-16T07:52:21-00:00	
4.3.2.1	5	2019-10-16T07:53:19-00:00	2019-10-16T07:54:26-00:00



"IP Lock Time" is the timestamp of the final invalid login attempt from the same client IP address. You can [configure the number of failed login attempts](#) that PFOS allows before an IP address is locked out. Once an IP lockout is triggered, the client will be locked for 60 minutes (this time is not configurable). For example, if the IP Lock Time is "07:54:26"; then the client will be unlocked at "08:54:26".

While a Client IP is locked, the following occurs:

- All traffic from the IP is blocked regardless of protocols (ssh, WebUI etc.).
- All login attempts from the IP are blocked regardless of username.
- Login to serial console from any IP including the locked IP is always allowed.
- All active sessions from the locked IP are kept in active state until they time out.

## Firewall Rules

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 Rules GUI enables you to define rules 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.

The screenshot shows a 'Firewall' configuration window. At the top, there's a header 'Firewall' and a section title 'Rule System firewall rules'. Below this is a toolbar with icons for search, filter, and file operations. A table lists the current rules:

Name	IP	Action	Direction	Remark
ipv4_rule	216.130.207.9/22	deny	ingress	IPv4 deny ingress rule
ipv6_rule	2001:db8:0:b::1a/64	permit	egress	IPv6 permit rule

At the bottom right of the table, it says 'Showing 1 to 2 of 2'.

## Configure Firewall Rules

Perform the following steps to configure firewall rules for your system. Refer to [Firewall Rule Considerations and Limitations](#) for configuration guidelines.

1. Open the **Firewall Rules** tab on the Access Control page.
2. Click **Add**, enter a name to identify the rule, and click **Add**.



## Add new Rule System firewall rules

### ▲ Add new Rule

Name \*   
1 to 64 characters.  
Rule name

**Add** **Cancel**

3. Configure the following parameters for the firewall rule.

## ipv4\_rule ×

IP \*   
Firewall IP address and prefix length

Action \* ▼  
Firewall rule action

Direction \* ▼  
Manage system traffic direction

Remark  ×  
User rule remark

**Note:** Refer to [Firewall Rule Considerations and Limitations](#) for configuration guidelines.

Setting	Description
IP	Network IP address and netmask prefix length. Both IPv4 and IPv6 addresses are supported.
Action	Permit or Deny traffic on specified IP.
Direction	Egress or Ingress traffic.
Remark	Description or comment about the rule.

4. Click **Apply** in the Toolbar to save the changes to the running configuration. The newly created firewall rule is appended to the end of the firewall rule list; it has the lowest priority compared to existing rules.



## Firewall Rule Considerations and Limitations

The following considerations apply to current release of Firewall Rules:

- If no Deny Firewall rules are configured, PFOS grants access permission to all IP addresses.
- PFOS automatically permits the IPv4 and IPv6 gateway addresses configured at [System Network Settings](#).
- When a Deny rule is configured, if no Permit rule for current access exists and the Deny setting will block current access, PFOS will reject the Deny rule.
- To Deny All IP addresses, use the following settings:
  - IPv4: "0.0.0.0/0" can be used to deny all IPv4 addresses.
  - IPv6: "::/0" can be used to deny all IPv6 addresses.
- The priority in which PFOS executes firewall rules is based on the order in which the rules are configured; the first rule configured has highest priority. **Therefore, configure all Permit firewall rules prior to configuring a Deny All firewall rule.** You can view configuration order by using the `show running-config firewall` command or viewing the Access Control>Firewall Rules Web UI.

**Example:** The following Permit rule for IP 172.21.84.246 is listed after (lower priority than) the Deny\_All rule; therefore, access from 172.21.84.246 will never be permitted.

```
firewall rule IPv4_Deny_All
ip 0.0.0.0/0 deny ingress
!
firewall rule Ipv4_172.21.84.246
ip 172.21.84.246/24 permit ingress
!
```

- When a remote authentication is configured for login (such as TACACS, RADIUS or LDAP service), remember to create Permit firewall rules for the authentication server IPs.
- Known limitations:
  - When users login via the serial console to create a Deny All rule, PFOS will prompt them to create a permit rule for IP 127.0.0.1/8. IP 127.0.0.1/8 is an internal loopback and has no impact on the firewall function.
  - Be careful when deleting permit rules when deny rule(s) are currently configured. PFOS allows deleting permission rules for current IP access but the system will not check for conflicts that may terminate current access.

## Configuring Ports

Refer to the following sections for details about configuring ports:

- [Port Classes](#)
- [Using the Port Settings Page](#)
- [Port Groups](#)



## Port Classes

Each port must be assigned to exactly one class. Available port classes vary according to the media type of the physical port. Due to the technical differences in physical ports on a device, not all ports can be all of the class types listed below. The Web UI shows only the options available on any given port.

The following port classes are supported on PFOS 6.x: Span, Monitor, Span-Monitor, Service, pStack, pStack plus, Inline Network, and Inline Monitor.

### Span Ports

A Span port is a unidirectional class of input port that is used to connect to a single output port, such as a switch SPAN port or another monitor port. Span ports forward input traffic through monitor ports to one or more passive monitoring or analysis tools, such as intrusion detection systems.

### Monitor Ports

A Monitor port is a unidirectional output port class that is used to connect to either the Span port on another packet flow switch or network packet broker, or to a single input port on a passive monitoring and/or analysis tool, such as an intrusion detection system.

### Span-Monitor Ports

A Span-Monitor port allows a single fiber port to act as a dual-function port class, where the Rx side acts as a Span port and the Tx side acts as a Monitor port. For advanced ports that are configured as Span-Monitor class, the Features Direction port setting allows you to specify whether features will be applied in either the ingress (the default) or egress direction.

### Service Ports

A Service port is a unidirectional class of an internal port that acts as an intermediary resource supporting the base feature set and special functions when the hardware is present, such as packet de-duplication and protocol de-encapsulation. On the line card port settings page, Service ports do not show any physical characteristics such as link status or speed.

### pStack and pStack plus Ports

pStack and pStack plus ports are bidirectional ports that are used to interconnect systems for providing an auto-sensing, self-healing, topologically pfsMesh architecture for traffic capture. Refer to the following sections for details:

- [Configure pStack Port Settings](#)
- [Configure pStack plus Port Settings](#)



## Inline Network Ports

Inline Network ports are used in pairs and connect inline with a network link. The primary purpose of each port in the pair is to forward network traffic to one or more inline active monitoring or analysis tools via Inline Monitor ports. User-defined VLAN IDs are supported on Inline Network ports with [limitations](#). Every Inline Network port can be paired with only one other Inline Network port. For more information, refer to [Inline Traffic](#).

## Inline Monitor Ports

Inline Monitor ports are used in pairs and connect to an inline active monitoring or analysis tool. The primary purpose is to forward traffic from one or more Inline Network ports to the connected inline tool. Because the outer VLAN in the packet is used to determine the A and B ports in a tool chain, every Inline Monitor Port can be paired with only one other Inline Monitor port. VLAN tagging is disabled on Inline Monitor ports. For more information, refer to [Inline Traffic](#).

## Using the Port Settings Page

The Port Setting page provides a summary view of all configured ports for each line card. Click the buttons along the top of the page to view port settings for different slots.

**Slot 1** Reset Slot ▾

▴ Line Card Settings

Configured Card	pre-configured
Default: unknown-card	
Line Card Model Configured	

▴ Line Card Ports Information

Ports with Class :	Monitor: 3	Span: 46	Span-Monitor: 0	Service: 0	pStack: 2
pStack Plus: 3	Inline-Network: 0	Inline-Monitor: 0			

▴ Line Card Port Settings

Port ID	Name	Class	Link	Speed	VID	XCVR Model	XCVR Type	PWR Rx (dBm)	PWR Tx (dBm)
1-1		Monitor	down	10000	1			-N/A-	-N/A-
1-2		Monitor	down	10000	2			-N/A-	-N/A-
1-3		Span	down	10000	3			-N/A-	-N/A-
1-4		Span	down	10000	4			-N/A-	-N/A-
1-5		Span	down	10000	5			-N/A-	-N/A-
1-6		Span	down	10000	6	INNOLIGHT TR-PX13L-NRS	1G/10GBase-LR	-40.0	-2.58
1-7		Span	down	10000	7			-N/A-	-N/A-
1-8		Span	down	10000	8			-N/A-	-N/A-
1-9		Span	down	10000	9			-N/A-	-N/A-
1-10		Span	down	10000	10			-N/A-	-N/A-
1-11		Span	down	10000	11	FINISAR CORP. FCLF8522P2BTL	1000Base-T	-N/A-	-N/A-
1-12		Span	down	10000	12	FINISAR CORP. FCLF-8521-3	1000Base-T	-N/A-	-N/A-
1-13		pStack	up	10000	13	FINISAR CORP. FTLX8571D3BCL	10GBase-SR	-2.54	-2.01
1-14		Span	down	10000	14			-N/A-	-N/A-
1-15		pStack-plus	up	10000	15	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-1.75	-2.23
1-16		Span	down	10000	16			-N/A-	-N/A-
1-17		Span	up	10000	17	INNOLIGHT TR-PX85S-NRS	1G/10GBase-SR	-4.12	-4.99
1-18		Span	down	10000	18			-N/A-	-N/A-



The *Line Card Settings* section identifies the type of line card currently installed in the specified slot, or Unknown Card. If no card is installed, you can pre-provision the slot by selecting a card type from the drop-down list. If you install a mismatching card type, the card is put in an out-of-service state until you change this setting to match the installed card.

The *Line Card Ports Information* section provides a count of ports with particular classes (Monitor, Span, etc).

The *Line Card Port Settings* section shows the individual ports for the selected slot. The port identifiers correspond to the port identification on the front panel (faceplate) of the line card. The port designation consists of the line card slot position and the port on the line card, such as 1-37. For ports that support [port breakout](#), the format includes a subport designation, such as 1-37.1.

**Note:** To control column display settings in the Line Card Port Settings area, click the Wrench  icon.

A *Reset Slot* button provides the following reset options:

- Reset Slot: Restart the slot similar to a system reboot.
- Clear Slot Configuration: Remove all ports of this slot from traffic maps and load balance groups.
- Shut Down Slot: Take the line card in this slot to the shutdown state. A line card in shutdown state can be unplugged from the chassis.

## Configure Port Settings

**Note:** For PFS 5010-16Xs with limited 16-port capacity licensing, only ports 1-16 can be configured; ports 17 and greater have a "Locked" state.

1. On the Configuration > Port Settings page, click a port ID link to display the settings for the port.  
**Note:** To view settings for other ports, use the arrows on the left and right sides of the page as needed to scroll through the ports for the selected line card, or enter a port number in the Port ID field. Then, either click **Go** or press the Enter key.
2. Configure [Basic](#) settings. If configuring a PFS 6000 Series system with an Advanced-R (40SadvR) line card, configure the [Advanced](#) settings.
3. Click **Apply** in the Toolbar to save the changes to the running configuration.

## Port Settings

When you click a Port ID link on the Port Settings page, you can view specific settings for that particular port. These settings will vary per device and configured options. Three tabs of port settings are available:

- [Basic Tab](#)
- [Advanced Tab](#)
- [References Tab](#)

A *Reset Port* button provides the following options:



- Reset Port: Restart the port.
- Clear Port Configuration: Remove all traffic maps and load balance groups that contain this port.

## Basic Tab

The following figure shows the settings on the Basic tab.

**Port 1-1 Settings**

**Basic**   **Advanced**   **References**

Name: string  
A user friendly port name. Max length is 64.

Class:  Span  Monitor  Span-Monitor  Service  pStack  pStack plus  Inline Network  Inline Monitor

Link State: Auto  
Default: auto  
Port Link state

Speed: Port Speed (Mbps/sec)

Tx Laser: On  
Default: on  
Transmit Laser

FEC:  Default  User Defined  
Forward error correction

FEC Type: cl91  
Default: cl91  
Forward error correction type

VLAN ID:  Default  User Defined

Link: down  
Default: down  
Port Link status

Tunnel Termination:  Tunnel Support  
Default: disable

Timestamp:  Rx

LLDP:  Rx  Tx

**Stripping**

Vlan Tag:  Default: disable  
Select to enable VLAN tag stripping

Vn Tag:  Default: disable  
Select to enable VN tag stripping

VxLAN:  Default: disable  
Select to enable VxLAN tag stripping

L2GRE:  Default: disable  
Select to enable L2GRE stripping

MPLS:  Default: disable  
Select to enable MPLS stripping

[Table 1.2](#) provides descriptions for the Basic port settings.

**Table 3.1 - Basic Tab Settings**

Setting	Description
Name	Assign a name for the port to help identify the devices or network segments that are connected to the unit.

**Table 3.1 - Basic Tab Settings (continued)**

Setting	Description
Class	<p>Specify the type of port:</p> <ul style="list-style-type: none"><li>• Monitor</li><li>• Service</li><li>• Span-Monitor</li><li>• Span (default)</li><li>• Inline Network</li><li>• Inline Monitor</li><li>• pStack (see <a href="#">Configure pStack Port Settings</a>)</li><li>• pStack plus (<b>Note: The pStack+ feature requires the PFS 7000 functionality license.</b>). See <a href="#">pfsMesh Using pStack+</a>.<ul style="list-style-type: none"><li>◦ If pStack plus ports are connected over an IP interface, you must configure a Source IP address and Destination IP address for the trunk (a Gateway IP address is optional). <b>Note:</b> 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.</li><li>◦ If pStack-plus ports are physically connected, PFOS automatically assigns the IP addresses.</li></ul></li></ul> <p><b>Notes for pStack and pStack plus ports:</b></p> <ul style="list-style-type: none"><li>• If switching the port class from <b>pStack to pStack plus</b>, or from <b>pStack plus to pStack</b>, 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.</li><li>• When changing port class from <b>pStack plus without IP</b> to <b>pStack plus with IP</b>, configure port as Span and then as pStack plus with IP.</li><li>• When changing port class from <b>pStack plus with IP</b> to <b>pStack plus without IP</b>, configure port as Span and then as pStack plus without IP.</li></ul>
Features Direction	Specify whether features for this port will be applied in either the Ingress (the default) or Egress direction. Available only when setting Span-Monitor class on advanced ports.

**Table 3.1 - Basic Tab Settings (continued)**

Setting	Description
Link State	<p>Specify the link state for the port:</p> <ul style="list-style-type: none"><li>• Auto: Normal operation.</li><li>• Force Down: Force the link down.</li><li>• Force Up: Force the link up.</li></ul> <p>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 that normally will not acknowledge a link unless something is plugged into the Rx side of the transceiver. Forcing the port to link allows 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. Currently, this capability is not available on SFP-only ports.</p> <p>By default, a Span-Monitor port has the link state AUTO; meaning the link status is calculated based on the connected Rx link. For example, if only the Tx cable is connected, then the link status will be down and the port will not send packets out. Therefore, when a Span-Monitor port is used for connections to two different devices, the recommendation is to configure it as Force-Up so the link status is always "up" irrespective of Rx link. If the link state is configured as Force Down, then the link status will be "down" irrespective of SFP state and Rx link.</p>
Speed	<p>Select the port speed, if the inserted transceiver supports more than one speed.</p> <p><b>Note:</b> PFS 5110s and PFS 5031/7031-56Xs support SFP28, SFP+, and SFP transceivers in ports 1-1 to 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 1-1 (for example, ports 1-1 to 1-4 must all have the same speed). On the Port Settings page, 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).</p>
Tx Laser	Enable/disable the transceiver transmitter for PFS 5000/7000 ports. Disabling the transceiver transmitter for passive or unused ports helps reduce power consumption of the device; refer to <a href="#">Power Savings per Port When Disabling Tx Laser</a> for details.

**Table 3.1 - Basic Tab Settings (continued)**

Setting	Description
Port Breakout	<p>Available on 40G and 100G ports (see exceptions in notes). Select this checkbox to divide this port into multiple subports. Select a breakout option from the dropdown list that displays: 4x10G, 2x50G, or 4x25G. When port breakout is enabled, the subports have identifiers of the form <i>slot-port.num</i>, where <i>slot</i> is the slot number, <i>port</i> is the main port number, and <i>num</i> is an ascending number for each breakout.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"><li>Some PFS models have limited breakout capability on certain ports; refer to <a href="#">Port Breakout Limitations</a> for details.</li><li>PFS 5030-32X/7030-32X and 5031-32X/7031-32X devices also support breakout to 4x1G.</li><li>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.</li><li>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.</li></ul>
FEC	<p>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.</p> <p>FEC is disabled by default (except on certain transceiver types on PFS 504x-32D), which offers the lowest latency delay. FEC is typically disabled with single mode (LR) connections. Refer to <a href="#">Port Speed, Port Breakout Capability, and FEC Support per PFS Model</a> for FEC details.</p>
FEC Type	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), RS-FEC mode (CL91), or RS544 mode depending on the network peer FEC setting and the PFS model. Refer to <a href="#">Port Speed, Port Breakout Capability, and FEC Support per PFS Model</a> for FEC details.
Auto Negotiations	(Visible only for ports with speed 1000) Turn port auto negotiation on or off. Auto negotiation is a requirement in gigabit copper links for proper synchronization between the connected copper gigabit devices.
VLAN Tagging	Keep (Enable) or remove (Disable) the VLAN tag added by PFOS at an ingress port when packets egress out at this port. VLAN tagging is disabled by default (PFOS removes the ingress VLAN tag).

**Table 3.1 - Basic Tab Settings (continued)**

Setting	Description
VLAN ID (VID) <sup>[1]</sup>	To configure a VLAN ID, choose from the following options: <ul style="list-style-type: none"><li><b>Default:</b> PFOS assigns a default VLAN ID based on the Starting VLAN ID configured on the System page; for details, refer to <a href="#">Source Port VLAN Tagging</a>.</li><li><b>User-Defined:</b> You can assign a custom VLAN ID to the port; valid values range 1-4094.</li></ul> <p><b>Note:</b> User-defined VLANs for all the member ports of a <a href="#">Consolidated network group</a> will be ignored. Incoming packets from the member ports are tagged with a <a href="#">Common VLAN ID</a> 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.</p> <p>For VLAN ID behavior over pfsMesh refer to <a href="#">pfsMesh</a> for details.</p>
Tunnel Termination	Enable Tunnel Termination on this port. Tunnel termination is disabled by default. Refer to <a href="#">IP Tunnel Termination</a> for details. <b>Note:</b> Timestamping and Tunnel Termination cannot be enabled on the same port.
Tunnel Termination Library	When Tunnel Termination is enabled, this drop-down list is available. Select a previously-created Tunnel Termination library. Refer to <a href="#">IP Tunnel Termination</a> for details.
Timestamp	(Visible only for certain models) Enable Rx (Ingress/Receive) or Tx (Egress/Transmit) time stamping on this port. Supported timestamp direction options vary depending on the port type; refer to <a href="#">PFS 7000 Timestamping</a> for details. <b>Note:</b> Time stamping and Tunnel Termination cannot be enabled on the same port.
LLDP	Enable LLDP packet reception and transmission on a per-port level for the <a href="#">Neighbor Discovery Using LLDP</a> feature. <b>Note:</b> The Neighbor Discovery Using LLDP feature requires the PFS 7000 functionality license.
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 <a href="#">PFS+PFX Inner Filtering and Inner Load Balancing</a> . <b>Note:</b> Packets sent from a Span-Monitor port that has External Device Tagging enabled are not affected by the VLAN Tagging option on the Monitor or Service port(s) to which they are sent. The VLAN tags added by the PFX are always stripped; <a href="#">Source Port VLAN Tagging</a> is not supported on Span-Monitor ports with External Device Tagging enabled.
Stripping	Enable VLAN tag, Egress VLAN tag, VN tag, L2GRE, VXLAN, or MPLS stripping. Available only on PFS 5000/7000 Series. Refer to <a href="#">Standard Stripping</a> for details.



[1] You can view this VLAN ID in the "VID" column on the Port Settings page or by using the CLI command `show interface <x> eth <y> vid`. 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](#) 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](#) for details about what VLAN ID to expect on egress packets.

### *Port Speed, Port Breakout Capability, and FEC Support per PFS Model*

The following table summarizes supported port speed and breakout capability per PFS model. The table also provides FEC support details: CL74 (FC-FEC), CL91 (RS-FEC), and RS544. Support of the FEC modes varies depending on the PFS model. RS-FEC mode (CL91) is displayed as the default setting when FEC is enabled. However, not all interfaces or breakout ports can support all three FEC modes. When an unsupported FEC Type is selected; the setting will be denied. See also [FEC](#) and [FEC Type](#) settings.

	Supported Port Speeds						100G Breakout		400G Breakout		
	1G	10G	25G	40G	100G	400G	4x25G	2x50G	4x100G (QSFP-DD)	4x100G (QSFPDD-DAC)	2x100G (QSFPDD-DAC)
PFS 5010/7010	•	•		•							
PFS 5100/7100		•	•	•	CL74 CL91		CL74	CL74			
PFS 5101/7101		•	•	•	•						
PFS 5110/7110	•	•	CL74	•	CL74 CL91		CL74 CL91	CL74 CL91			
PFS 5111/7111	•	•	•	•	•						
5120/7120 5121/7121-64X		•	•	•	CL74 CL91		CL74 CL91	CL74 CL91			
PFS 5030/7030-32X PFS 5031/7031-32X		•	•	•	CL74 CL91		CL74 CL91	CL74 CL91			
PFS 5030/7030-54X	•	•	•	•	CL74 CL91		CL74	CL74 CL91			
PFS 5031/7031-56X	•	•	CL74	•	CL74 CL91		CL74 CL91	CL74 CL91			
PFS 504x/704x-32D	•	•	•	•	CL91 RS544	RS544 (Note 1)	CL74 CL91		RS544 (Notes 2,3)	CL91 RS544 (Note 3)	CL91 RS544
PFS 6002	•	•		•	•						
PFS 6010	•	•		•	•						

#### **Notes:**

<sup>1</sup> FEC at 400G on PFS 504x/704x-32D is not configurable, it is always enabled with FEC Type RS544.

<sup>2</sup> CL91 is not supported at 4x100G breakout port even though the setting will not be denied.



<sup>3</sup> Users must enable FEC to bring up the link. Once FEC is enabled, all four breakout ports must be configured with the same FEC Type.

### *Power Savings per Port When Disabling Tx Laser*

PFOS provides a [Tx Laser](#) option for PFS 5000/7000 ports allowing you to disable the transceiver transmitter for passive or unused ports to reduce power consumption of the device. The following table summarizes these power savings; the power savings per port are approximate and may vary between transceivers.

Port Type	Power Savings per Port (mW)	Annual kgCO <sub>2</sub> Emissions Saved per Port (0.475 kgCO <sub>2</sub> e/kWHR)	Annual kWHR Saved per Port
<b>10G SR</b>	200	0.83	1.8
<b>10G LR</b>	334	1.39	2.9
<b>40G SR4</b>	500	2.08	4.4
<b>40G LR4</b>	1000	4.16	8.8
<b>100G SR4</b>	500	2.08	4.4
<b>100G LR4</b>	1200	5.00	10.5
<b>400G DR4</b>	2750	11.44	24.09
<b>400G LR4</b>	2875	11.96	25.185

### *Port Breakout Limitations*

Refer to the following sections for details about port breakout limitations:

- [PFS 5120/7120 Port Breakout Limitations](#)
- [PFS 5121/7121-64X Port Breakout Limitations](#)
- [PFS 5030-54X/7030-54X Port Breakout Limitations](#)

### PFS 5120/7120 Port Breakout Limitations

The PFS 5120/7120 can only support up to 128 logical ports, so the maximum number of breakout ports is limited to 20. The following figure shows the port numbers that can be configured as 4x25G, 4x10G, or 2x50G breakout ports.

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32
33	35	37	39	41	43	45	47	49	51	53	55	57	59	61	63
34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64

= Shaded numbers indicate ports that can have port breakout enabled



## PFS 5121/7121-64X Port Breakout Limitations

The PFS 5121/7121-64X can only support up to 128 logical ports, so the maximum number of breakout ports is limited to 20. The following figure shows the port numbers that can be configured as 4x25G, 4x10G, or 2x50G breakout ports.

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32
33	35	37	39	41	43	45	47	49	51	53	55	57	59	61	63
34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64

= Shaded numbers indicate ports that can have port breakout enabled

## PFS 5030-54X/7030-54X Port Breakout Limitations

The PFS PFS 5030-54X/7030-54X can only support up to 64 logical ports. Ports 51 and 54 are breakout capable and can be configured as 4x25G, 4x10G breakout ports.

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	52
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	53

= Shaded numbers indicate ports that can have port breakout enabled

## Advanced Tab

The following figure shows the settings on the Advanced tab. These features are only supported on the 40-port 10G/1G Advanced-R (40SadvR) line card on the PFS 6000 Series; see [Enhanced Port features](#) for details. The list of available features depends on which ones have been configured on the firmware of the line card.

The screenshot shows the 'Port 10-2 Settings' page with the 'Advanced' tab selected. The interface includes:

- Port and Time Stamping** section:
  - Monitor Output Timestamping: Enabled (checkbox checked)
  - Monitor Output Portstamping: Enabled (checkbox checked)
- Protocol Deduplication** section:
  - De-Duplication: Enabled (checkbox checked)
  - Deduplication Library Settings: L2 (dropdown menu)
  - Default: Settings from De-duplication Library
- A 'Reset Port' button in the top right corner.

[Table 1.4](#) provides descriptions for the Advanced port settings.

**Table 3.3 - Advanced Tab Settings**

Setting	Description
Monitor Output Timestamping	Assigns a time stamp when traffic leaves a monitor port. See <a href="#">Time Stamping</a> for details.
Monitor Output Portstamping	Assigns a port stamp when traffic leaves a monitor port. In the Portstamping Option drop-down list that displays, select <b>One Byte Flat</b> or <b>Two Byte Flat</b> as the portstamping option (Two Byte Flat is the default). See <a href="#">Port Stamping</a> for details.
GeoProbe Time Format	This option is only used for Monitor ports when the PFS is used in GeoProbe G10 deployments. <ul style="list-style-type: none"><li>• Strip TS/PS (Strip timestamp/portstamp): Egress packets have no timestamp and port tag (egress packets are the same as received at ingress port)</li><li>• Include TS/PS (Include VSS timestamp/portstamp): Egress packets have timestamp and/or port tag appended to end of packet</li><li>• GeoProbe TS/PS (Encapsulate using GeoProbe-format timestamp/portstamp): Egress packets have GeoProbe metadata header containing timestamp, port tag, and other information</li></ul>
VN Tag Stripping	Allows you to enable or disable stripping of VN tags when a monitor or service class port is selected.
VLAN Tag Stripping	Allows you to enable or disable stripping of VLAN tags when a monitor or service class port is selected.
Protocol Stripping	Select this checkbox to enable generic stripping. For more information, refer to <a href="#">Protocol De-encapsulation and Stripping</a> .
De-Duplication	Enables or disables deduplication on the port. For more information, refer to <a href="#">Packet Deduplication</a> .
Slicing	Select this checkbox to enable conditional packet slicing and masking. For more information, refer to <a href="#">Conditional Packet Slicing</a> and <a href="#">Conditional Packet Masking</a> .
Extended Load Balancing	Select this checkbox to enable extended load balancing. For more information, refer to <a href="#">Extended Load Balancing</a> . In the drop-down list that displays, select the extended load balancing library (pre-configured or user-defined) to use.



## References Tab

If a specific port is currently in use by traffic maps and/or load balancing groups, the References tab is available. Click this tab to display a list of traffic maps and load balancing groups that use this port.

The screenshot shows the "Port 1-2 Settings" window with the "References" tab selected. The window displays a list of entities using the selected port:

- Maps: TrafficMap #1-2 (Maps that are using this port)
- Load Balancing Groups: Load Balancing Groups that are using this port
- pStack: pStack maps that are using this port
- Port Group(s): Port Group(s) that are using this port
- IP: IP Interfaces using this port
- Triggers: List of triggers using this port
- Powersafe: Module and segment using this port

## Port Groups

You can create groups of network ports, monitor ports, inline network ports, and inline monitor ports, and you can use these groups in traffic maps, instead of — or with — individual ports. This simplifies flow configuration by reducing the number of traffic maps required. Also, you can change the ports that belong to a port group without changing the relevant traffic maps.

Therefore, NETSCOUT recommends that, where possible and practical, you use port groups instead of individual ports in your traffic maps.

There are two kinds of network port groups: *consolidated* (available only on the PFS 6000 Series), in which the ports form a trunk, and *unconsolidated*, which is just a logical entity.

A network port which is part of a network port group trunk cannot be used in any other network port group trunks (such as any other consolidated network port groups). Network ports in an unconsolidated network port group can be part of multiple network port groups.

For details on using port groups in traffic maps, refer to [Traffic Maps](#).



Inline network port groups and inline monitor port groups are used to manage inline traffic. For details, refer to [Inline Traffic](#)

## Port Group Procedures

In the Web UI, you can create port groups and include them in traffic maps.

Network port groups can include network ports, service ports, span-monitor ports, a common VLAN ID. Monitor port groups can include monitor ports, service ports, span-monitor ports, load balance groups, and load balance criteria.

When creating traffic maps, in the Ingress part, you can include input ports as well as network port groups. In the Egress part, you can include monitor ports, monitor port groups, and remote monitor groups. A map-level action indicates the action to be taken on the matching traffic for the flow. The actions are either Drop or Forward.

Refer to the following sections for details:

- [Create a Port Group](#)
- [Change an Existing Port Group](#)
- [Delete a Port Group](#)

Also, for details about Maximum groups per chassis and maximum members per group, refer to [Port Group Resource Limits](#).

## Create a Port Group

Refer to the following sections to create a Port Group:

- [Add a Port Group](#)
- [Port Groups](#)
- Configure Port Group Settings (Settings vary per port group type)
  - [Configure Port Group Details - Network Port Group](#)
  - [Configure Port Group Details - Monitor Port Group](#)
  - [Configure Port Group Details - Inline Network Port Group](#)
  - [Configure Port Group Details - Inline Monitor Port Group](#)

### Add a Port Group

1. Go to the Port Groups page.
2. Click the tab for the type of port group that you want to create: **Network, Monitor, Inline Network, or Inline Monitor**.
3. Click **Add**.



Port Groups			
Network	Monitor	Inline Network	Inline Monitor
			Add ... Delete
Name	Consolidate	Common Vlan	Error Code
NPG1	disable		None

4. In the Name field, enter a name to identify the new port group, and click **Add**.

**Note:** If you are creating a Monitor port group and it will be used in pfsMesh as a remote monitor group, ensure that the monitor group name is unique to avoid conflict with other monitor group names and so it is easily identifiable within pfsMesh. Refer to [Configure Monitor Output with a pfsMesh](#) for details.

5. Continue with [Port Groups](#).

### Select Ports

1. To select the ports that will be in the port group, click **Configure** in the Ports section.

### network-grp1

Ports \* **configure** Selected Output Ports: Consolidate **Disable**  
Ports selection Default: disable  
For tcam resource optimization

Common Vlan **uint32** Error Code None  
Valid values: 1—4094 Default: None  
Vlan for Logical Links

Ref Map List of traffic maps using the port-group

2. Drag and drop ports into the Selected Ports section as desired. When you are done, click



OK.

**Select ports to use (drag-n-drop):**

Ports selection

Slot:  1  2  3  4  5  6  7  8  9  10  all

Available Ports					Selected Ports
8-3	8-4	8-5	8-6	8-7	8-1
8-8	8-9	8-10	8-11	8-12	
8-13	8-14	8-15			

A red circle highlights port 8-2 in the Available Ports list, and a red arrow points from it to the Selected Ports list, indicating it has been selected.

- Continue with one of the following sections to configure port group settings (settings vary per port group type):
  - [Configure Port Group Details - Network Port Group](#)
  - [Configure Port Group Details - Monitor Port Group](#)
  - [Configure Port Group Details - Inline Network Port Group](#)
  - [Configure Port Group Details - Inline Monitor Port Group](#)

#### Configure Port Group Details - Network Port Group

After [selecting ports](#), following these steps to configure Network Port Group details.

- Configure **Consolidation** (Only Available on PFS 6000 Series) by selecting **Enable** to create a trunk.

**Note:** If pStack is enabled, (that is, the PFS has a port with Class = pStack), 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.*



2. Configure **Common VLAN ID** (Only Available on PFS 6000 Series) by specifying a value from 1 to 4094 (optional). This VLAN ID must be same as the user-defined VLAN ID of all member ports.
3. Click **Apply** in the toolbar to save the settings to the running configuration.

The screenshot shows the 'network-grp1' configuration page. At the top, there are tabs for 'Ports' (selected) and 'configure'. Below that, 'Selected Output Ports' are set to 1-3, 1-4. The 'Consolidate' section has 'Enable' selected with a note: 'Default: disable' and 'For tcam resource optimization (Disable)'. Under 'Common Vlan', the value '102' is entered, with a note: 'Valid values: 1—4094' and 'Vlan for Logical Links'. The 'Error Code' field is set to 'None' with a note: 'Default: None'.

### Configure Port Group Details - Monitor Port Group

Follow these steps to configure Monitor Port Group details.

1. Select a Monitor port to add to the group.
2. To add optional load balance group for pfsMesh to use at remote node, select **Load Balancing Criteria** first.  
These criteria are used only by traffic maps to remote destinations (via pfsMesh). If the monitor group is used locally in a map, specify load balancing criteria in the map itself.
3. Optionally select a **Load Balance Group**. Tunnel load balance groups are not supported in monitor port groups.
4. Select pfsMesh **Enable** to allow this port group to be visible across a pfsMesh. Select **Disable** if you want this port group to only be visible to the node on which it was created. Refer to [Configure Monitor Output with a pfsMesh](#) for details.
5. Click **Apply** in the toolbar to save the settings to the running configuration.

The screenshot shows the 'monitor-grp1' configuration page. At the top, there are tabs for 'Ports' (selected) and 'configure'. Below that, 'Selected Output Ports' are set to 1-5, 1-6. The 'Lb Criteria' section shows 'IP\_Dest' with a note: 'Load-balance criteria ()'. The 'Load Balance Groups' section shows 'passive-A-LBG' with a note: 'Load-balance groups ()'. The 'pfsMesh' section has 'Enable' selected with a note: 'Default: enable' and 'pfsMesh Visibility enable/disable'. The 'Status' section shows 'PortGroupNameResolved' with a note: 'Default: PortGroupNameResolved' and 'Port group status'.



### Configure Port Group Details - Inline Network Port Group

After [selecting ports](#), follow these steps to configure Inline Network Port Group details.

1. Enable or disable adding **VLAN tags** to the packets being forwarded from the Inline Network ports. When this option is disabled (VLAN tags are not added):
  - Packets leaving the tool chain will be load balanced among either the A-side or B-side ports in the Inline Network group, depending on the packet's direction. There should be only one Inline Network Port Group in a map to a tool chain; the packet egress will be load balanced among the Inline Network ports in the group.
  - Tools used by one Inline Network port group (VLAN tag disabled) should not be shared with another tool chain.
  - For the associated inline maps and toolchains, packets replicated to and out of their passive monitor ports will not carry VLAN tags.
2. The **Power Safe** option must be set when the Inline Network port is connected to the External PowerSafe TAP.
3. Specify the **A Port** in this group.
4. Specify the **B Port** in this group.
5. Click **Apply** in the toolbar to save the settings to the running configuration.

A Port	B Port	Link Safe
10-11	10-12	Disabled

### Configure Port Group Details - Inline Monitor Port Group

After [selecting ports](#), follow these steps to configure Inline Monitor Port Group details.

1. In the Port Pair section, click **Add** to specify the A-side port in this group.
2. In the B Port section, select the B-side port in this group.



3. In the A and B Health Monitor Library sections, optionally specify the name of a health monitor library to use on that side of the port pair. If no health monitor libraries are specified, then the default health check status is "up." For information on health checks and procedures to create health checks, refer to [Health Check Profiles](#).
4. In the LinkSafe section, enable or disable [LinkSafe](#) for this group.
5. Load balancing among port pairs of an inline monitor port group is determined by the load balancing criteria specified in the inline traffic map that uses the port group. For details, refer to [Inline Traffic Maps](#). The load balance traffic failover behavior among port pairs of an inline monitor port group is to redistribute the traffic.
6. You can prioritize a specific port pair over other port pairs in the inline monitor port group by assigning a **weight** to it (valid values 0-100). PFOS uses the weight value within an algorithm to calculate the percentage of traffic distribution to forward to these ports. See [Load Balance Weighted Calculation](#) for details.

The screenshot shows the configuration for port pair 10-10. It includes fields for B Port (10-11), A Health Monitor Library (asc1), B Health Monitor Library (asc2), Link Safe (Enable), A Health Check Status (up), B Health Check Status (up), and Weight (0).

7. Click **Apply** in the toolbar to save the settings to the running configuration.

#### Change an Existing Port Group

1. From the Port Groups page, click the tab for the type of port group that you want to change: **Network, Monitor, Inline Network, or Inline Monitor**.
2. Click the name of the port group that you want to change.
3. Specify the new settings. Refer to the previous section to see which settings are available for each type of port group.
4. Click **Apply**.

#### Delete a Port Group

1. From the Port Groups page, click the tab for the type of port group that you want to create: **Network, Monitor, Inline Network, or Inline Monitor**.



2. Click on the line containing the port group that you want to delete. The line is highlighted with a gray background.
3. If you want to delete additional port groups, control-click on the lines containing those filters, or shift-click to select a range of lines. Each line you select is highlighted with a gray background.
4. Click **Delete**.
5. A confirmation prompt displays. Click **Yes** to confirm the deletion of all selected port groups, or click **No** to cancel the deletion.

Port Groups		
Network	Monitor	Inline Network
		<input type="button" value="Add ..."/>
		<input type="button" value="Delete"/>
Name	A Error Code	B Error Code
AG-1	None	None
AG-2	None	None
FW	None	None
IMPG1	None	None
IMPG2	None	None
IPS	None	None
SSI_1	None	None

### Port Group Resource Limits

Port Group Type	Maximum Groups per chassis	Max Members per Group
Network	PFS 5000/7000: 64 PFS 6000: <ul style="list-style-type: none"><li>• Consolidated: 16</li><li>• Non-consolidated: 48-64</li></ul>	Up to 64 ports
Monitor	64	No port limitation
Inline Network	32	Up to 128 ports
Inline Monitor	32	Up to 64 ports

## 4 Base Features and Tasks

This section describes the features and configuration tasks for the main PFOS features that are available on all supported hardware. [Configuration Task Flow](#) shows the order in which to configure the filtering, load balancing, and traffic mapping features.

- [Traffic Maps](#)
- [Traffic Filtering](#)
- [Traffic Load Balancing](#)
- [Trigger Policies](#)
- [Source Port VLAN Tagging](#)
- [IP Tunnel Termination](#)
- [pfsMesh](#)

**Note:** You must click **Apply** at the top of the Web UI to save configuration settings to the running configuration. To have changes persist through a reboot, you must also save them to the startup configuration by clicking **Copy to Startup**. See [Configuration File Types](#) for information on the running, startup, and saved configuration files.

### About 200G Port Groups

Some base feature configuration considerations depend on whether those ports belong to the same 200G port group.

A “200G port group” is a set of adjacent ports on a PFS 6000 series line card that support a total of 200G in bandwidth; 200G port groups do not apply to the PFS 5000/7000 series. The number of ports in a 200G port group depends on the type of line card and the bandwidth of each individual port, and the number of 200G port groups per line card depends on the type of line card, as shown in the following table:

**Table 4.1 - 200G Port Groups per Line Card**

Line Card	Port Groups	
36S6Qstd	When 40G breakout is not used: Group 1: Ports 1-20 Group 2: Ports 21-37 Group 3: Ports 38-42	When 40G breakout is used: Group 1: Ports 1-20 Group 2: Ports 21-40 Group 3: Ports 41-60

**Table 4.1 - 200G Port Groups per Line Card (continued)**

Line Card	Port Groups	
15Qstd	When 40G breakout is not used: Group 1: Ports 1-5 Group 2: Ports 6-10 Group 3: Ports 11-15	When 40G breakout is used: Group 1: Ports 1-20 Group 2: Ports 21-40 Group 3: Ports 41-60
6Cstd, 6Q28std	Group 1: Ports 1-2 Group 2: Ports 3-4 Group 3: Ports 5-6	
40SadVR	Group 1: Ports 1-20 Group 2: Ports 21-40	

## Traffic Maps

A traffic map associates input ports with output ports and automatically applies filtering and load balancing rules to the traffic that enters the system. Traffic maps can be used to aggregate, filter, and balance traffic, or any combination of these.

The Traffic Map section lists all existing traffic maps and allows you to create new maps and modify existing ones.

Name	Description	Type	Mode	Filter	Input Ports	Network Port Groups	Monitor Port Groups	Output Ports	Output LBGs	Load Balance Criteria	Map Status - State
MAP-1		Monitor	Basic	AAA	1-11	NPG-1	MPG-1	1-31	LBG-1	IP_Dest_Src	enable
MAP-1A		Monitor	Basic	SIP	1-11	NPG-1		1-32			enable
MAP-1C		Monitor	Basic	nonmatch		NPG-1		1-33			enable
MAP-2		Monitor	Basic	AAA	1-12	NPG-2	MPG-2	1-21	LBG-1	IP_Dest_Src	enable
MAP-2A		Monitor	Basic	unfiltered	1-12	NPG-2		1-22			enable

Showing 1 to 5 of 5

## Traffic Map Processing

Creating a traffic map requires selecting criteria to filter the incoming traffic from a set of input ports across an individual PFS chassis. A single copy of the traffic can be redirected to any one or a combination of Monitor Ports, Load-Balance Groups, Tunnels or Remote Monitor Port Groups.

PFOS processes traffic maps in the order in which they were created; older traffic maps are processed first. You can also modify the order existing maps are processed; refer to [Change the Processing Order of Traffic Maps](#) for details. The first traffic map for a given input port processes all incoming traffic from the input port specified in the filter. Each subsequent map processes the traffic that did not match (therefore, passed through) the previously processed filter from the same given input port. Traffic is processed using this filtering precedence except for traffic maps configured with Unfiltered or Nonmatch filters; see [Special Filters: Unfiltered and Nonmatch](#) for details about differences in filter preference for these special filters.

### Example 1 – Traffic Maps with Filtering on Same Input Ports

In this example, if input port 1-1 is mapped to output port 1-7 with a filter called HTTP applied in Map-1, and a second filter called TCP is also applied to input port 1-1 to output port 1-8 in Map-2, the second map filter is applied only to the remaining traffic passing through from the first filter.



Name	Type	Description	Mode	Filter	Input Ports	Output Ports	Action
Map-1	Monitor	<ul style="list-style-type: none"> <li>Raw unfiltered traffic from input port 1-1 is processed against HTTP filter.</li> <li>Packets matching HTTP filter are forwarded to Port 1-7</li> <li>Packets not matching HTTP filter are processed by Map-2 (TCP filter)</li> </ul>	Basic	HTTP	1-1	1-7	Forward
Map-2	Monitor	<ul style="list-style-type: none"> <li>Traffic not matching HTTP filter from input port 1-1 is processed against TCP filter.</li> <li>Packets matching TCP filter are forwarded to Port 1-8</li> <li>Packets not matching TCP filter are passed through to the next maps with the same input ports/groups.</li> </ul>	Basic	TCP	1-1	1-8	Forward

## Example 2 – Traffic Maps with Filtering on Different Input Ports

In this example, if the TCP filter in Map-2 is applied to a different input port such as port 1-2 and to output port 1-8, then the TCP filter is applied to all incoming traffic from port 1-2.

Name	Type	Description	Mode	Filter	Input Ports	Output Ports	Action
Map-1	Monitor	<ul style="list-style-type: none"> <li>Raw unfiltered traffic from input port 1-1 is processed against HTTP filter.</li> <li>Packets matching HTTP filter are forwarded to Port 1-7</li> <li>Packets not matching HTTP filter are passed through to the next maps with the same input ports/groups.</li> </ul>	Basic	HTTP	1-1	1-7	Forward
Map-2	Monitor	<ul style="list-style-type: none"> <li>Raw unfiltered traffic from input port 1-2 is processed against TCP filter.</li> <li>Packets matching TCP filter are forwarded to Port 1-8</li> <li>Packets not matching TCP filter are passed through to the next maps with the same input ports/groups.</li> </ul>	Basic	TCP	1-2	1-8	Forward

## Merging Traffic Maps

If multiple traffic maps have the same set of input ports and filters, then internally their output ports are also merged; this functionality is called "Map Merge".

When creating traffic maps, every separate map that you create is displayed as its own unique entry, even if the input port(s), filter, and enable/disable/trigger settings are the same. You can



direct PFOS to consolidate existing traffic maps into fewer traffic maps that perform the same function for traffic maps that have the same input port(s), filter, and enable/disable/trigger (active, inactive) settings combination.

When traffic maps are merged, PFOS performs all possible consolidations. You cannot limit the set of traffic maps that are considered for merging.

### About Traffic Maps and Service Ports

Service ports can be both input ports and output ports relative to a traffic map. If a service port is selected in the input ports configuration of a traffic map, it adheres to the described properties of an input port. If it is selected in the output ports configuration, it will adhere to the output port properties.

### About Traffic Maps and Span-Monitor Ports

Span-Monitor ports can be both input ports and output ports relative to a traffic map. Unlike a Service port, a single Span-Monitor port can be configured as both ingress and egress on the same traffic map.

You cannot change the class of a port that is part of a traffic map if the new settings would conflict with the current ones. For example, if port 1-1 is configured as Span-Monitor class and is part of the Input Ports group, then you cannot change it to Monitor class because it would become an output port. However, you could change that port to Span class because it would still be an input port.

## Traffic Map Procedures

Refer to the following sections for details:

- [Create a Traffic Map](#)
- [Change the Processing Order of Traffic Maps](#)
- [Merge Traffic Maps](#)
- [Delete Traffic Maps](#)
- [View Traffic Map Status](#)
- [View Remote Monitor Group Status](#)
- [View Output pStack Interface](#)

### Create a Traffic Map

Before you define traffic maps, set up the filters, load balance criteria, and load balance groups that you want to include. See [Traffic Filtering](#) and [Traffic Load Balancing](#).

1. Go to the Traffic Maps page, and click **Add**.
2. Enter a name to identify the map, and click **Add** to save the map and display the settings.



3. In the Type drop-down list, select **Monitor** or **Inline Monitor** to define the type of traffic map. The rest of this procedure describes a Monitor traffic map. For details on creating an Inline Monitor map, refer to [Inline Traffic Maps](#).

**map9** ×

Description	<input type="text" value="string"/> 1 characters or more. A string description of map	Type	<input type="button" value="Monitor"/> <input type="button" value="..."/> Default: Monitor A map type
Mode	<input type="button" value="Basic"/> <input type="button" value="..."/> Default: Basic Map mode Basic/Extended	Filter	<input type="button" value="..."/>
Ingress	<input type="button" value="configure"/> Input port(s)	Selected Ingress :	
Egress	<input type="button" value="configure"/> Output port(s)	Selected Egress:	
Load Balance Criteria	<input type="button" value="..."/> Load-balance criteria		
Output Load Balance Groups	<input type="button" value="Add an entry ..."/> Output load-balance groups		
Action	<input checked="" type="radio"/> Forward <input type="radio"/> Drop Default: Forward Action to take for filter	<input type="button" value="Map Status"/> Map status	
	<input type="button" value="Output pStack Interface"/> Output pStack interfaces for given list of input ports	<input type="button" value="Remote Monitor Group Status"/> Remote monitor group status	
<b>State</b>			
<input type="radio"/> Enable <input type="radio"/> Disable <input type="radio"/> Trigger Profile			
<b>Mirror Session</b> Configures mirror-session for the map			
<input type="button" value="Add an entry ..."/> List of mirror-session			

4. Select a map mode, either **Basic** or **Extended**. To use traffic maps with extended load balancing on advanced line cards, you must select Extended. The default value is Basic.
5. Select a filter from the Filter Selection pull-down list.
6. Click **configure** in the Ingress section.



7. Select the slot number to show the available ports and port groups for that slot. Select **Input port(s)** or **Network group(s)** as desired. The lists of available ports and port groups depend upon the type of traffic map and the features available on the line card in the selected slot. Drag ports to the Selected Ingress Ports section, and/or drag port groups to the Selected Ingress Groups section. You can select multiple line card slots and their associated ports as output ports for your traffic map.

**Select ports to use (drag-n-drop):**

Input ports(s)  Network group(s)

Slot:  1  2  3  4  5  6  7  8  9  10  all

Available Ports					Selected Ingress	
8-3	8-4	8-5	8-6	8-7	8-1	Ports
8-8	8-9	8-10	8-11	8-12	8-2	Groups
8-13	8-14	8-15			NPG1	

**OK** **Cancel** **Clear All**



8. Click **OK**.
9. Click **configure** in the Egress section, and repeat the port selection process.
10. For a Basic traffic map only, to optionally add a previously-created remote monitor group on another connected system for pfsMesh output:
  - a. Click **configure** in the Remote Monitor Groups section.
  - b. In the Remote Nodes section, select a remote node or **all**.
  - c. Drag one or more remote monitor group names to the Selected Remote Monitor Groups section.
  - d. Click **OK**.

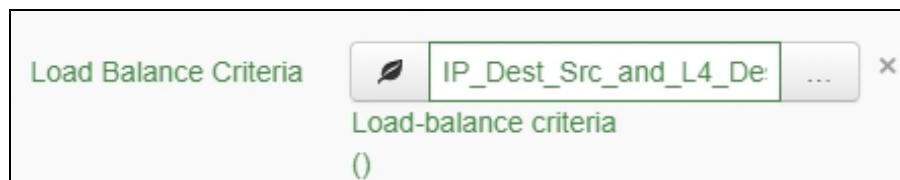


11. To optionally add load balance criteria and groups:

- First select the **Load Balance Criteria** to be used for load balance by clicking "..." to select one of existing LB criteria from a pop up list.



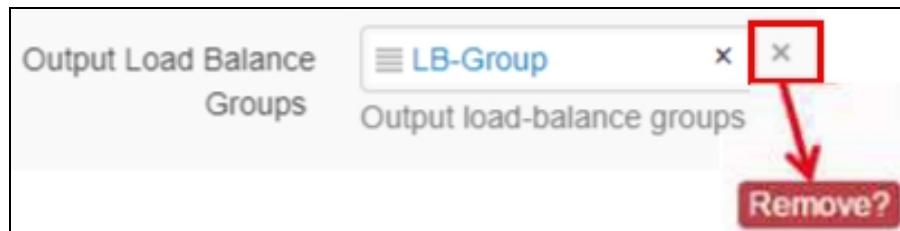
- Select the criterion, and click **OK** to update the entry.



- Click **Add an entry** in the Output Load Balance Group area.
- Select the load balance group and click **Add**. Click **Update** to update an existing entry.
- To add another entry, click **Add**.



- To remove an entry, click the X in the entry field. To remove the full list, click the X to the right and click **Remove** as prompted.



12. To specify the action to take when a match occurs on this traffic map, select either **Forward** (the default) or **Drop**.



13. Set the current state of the map: Enable, Disable, or Trigger Profile. To enable the traffic map based on the outcome of a trigger profile, perform the following:
  - a. Select **Trigger Profile**.
  - b. Select the **Name** of the trigger profile to be monitored for this map.
  - c. Select the **State** of the trigger profile you want to enable the map (active/inactive).

14. If you want to associate a Port Mirroring and Packet Slicing with the traffic map, perform the following:
  - a. In the Mirror Session area, click **Add an Entry...**
  - b. In the empty field that appears, double-click to display a list of configured mirror sessions.
  - c. Select the name of the mirror session that you want to associate with this traffic map and click **Update**.

15. Click **Apply**. The traffic map is now automatically applied.

## Change the Processing Order of Traffic Maps

By default, traffic maps are processed in the order in which they were created; the oldest traffic map is processed first. You can change the order in which traffic maps are processed using one of two methods:

- [Reorder Traffic Maps Using Drag-and-Drop](#)
- [Reorder Traffic Maps Using Move Button](#)

### Reorder Traffic Maps Using Drag-and-Drop

You can reorder traffic maps on the same page by clicking-and-dragging the maps in the list.

1. From the Traffic Maps page, in the Traffic Map list, position the cursor on any item in the list.



2. Click and hold to drag the item to the desired position in the list.

Traffic Map										
Name	Description	Type	Mode	Filter	Input Ports	Network Port Groups	Monitor Port Groups	Output Ports	Remote Monitor Groups	Other
map-TC-SSL	for-bypass-drop	inline-monitor	Basic							
map-		inline-	Basic							

### Reorder Traffic Maps Using Move Button

Use the Move button to move a traffic map from one page to another page when you have more than 10 traffic maps and they are displayed on multiple pages.

1. From the Traffic Maps page, in the Traffic Map list, click the line containing the traffic map that you want to move. The line is highlighted with a gray background.
2. Click **Move**. In the drop-down list that displays, select **Cut**, the only valid option at this point.

Traffic Map										
Name	Description	Type	Mode	Filter	Input Ports	Network Port Groups	Monitor Port Groups	Output Ports	Remote Monitor Groups	Other
map1		Monitor	Basic	unfiltered	10-5					
map2		Monitor	Basic	unfiltered	10-8				10-9	
map3		Monitor	Basic	unfiltered	10-10				10-11	

3. Click another item in the list of traffic maps, either on the same page or a different page.
4. Click **Move**. In the drop-down list that displays, select either **Insert before** or **Insert after** as desired.

Traffic Map										
Name	Description	Type	Mode	Filter	Input Ports	Network Port Groups	Monitor Port Groups	Output Ports	Remote Monitor Groups	Other
map1		Monitor	Basic	unfiltered	10-5					
map2		Monitor	Basic	unfiltered	10-8				10-9	
map3		Monitor	Basic	unfiltered	10-10				10-11	



## Merge Traffic Maps

1. From the Traffic Maps page, click **Merge**.
2. All possible traffic map merges are performed, and the list of traffic maps updates to show the result. The changes are applied automatically, and you do not need to click **Apply**.

Name	Description	Type	Mode	Filter	Input Ports	Network Port Groups	Monitor Port Groups	Output Ports	Remote Groups
amap1	amap1	Monitor	Basic	unfiltered	1-3			1-5	
amap2	amap2	Monitor	Basic	unfiltered	1-3			1-6	
amap3	amap3	Monitor	Basic	unfiltered	1-3			8-5	

Name	Description	Type	Mode	Filter	Input Ports	Network Port Groups	Monitor Port Groups	Output Ports	Remote Groups
amap1	amap1	Monitor	Basic	unfiltered	1-3			1-5, 1-6, 8-5	

## Delete Traffic Maps

1. From the Traffic Maps page, click the line containing the traffic map that you want to delete. The line is highlighted with a gray background.
2. If you want to delete additional traffic maps, control-click on the lines containing those traffic maps, or shift-click to select a range of lines. Each line you select is highlighted with a gray background.
3. Click **Delete**.
4. A confirmation prompt displays. Click **Yes** to confirm the deletion of all selected traffic maps, or click **No** to cancel the deletion.

Are you sure you want to delete the selected entries?

Name	Description	Type	Mode	Filter	Input Ports	Network Port Groups	Monitor Port Groups	Output Ports	Remote Monitor Groups	Output LBGs	Inline Network Group	Load Balance Criteria	Input Tunnels	Output Tunnels	Map Status - State
map_118_to_117		Monitor	Basic	unfiltered	1-17			1-31	PG117_A						enable
map_118_to_116_and_117		Monitor	Basic	mac_dest	1-22, 1-33, 1-35, 1-42				PG116, PG117_B						enable
map_118_to_233		Monitor	Basic	IP_src	1-40, 1-43				PG6010						enable



## View Traffic Map Status

1. From the Traffic Maps page, click the name of the traffic map that you want to view.
2. On the map page, scroll down to the bottom and click **Map Status**.

### Map Status

Map status

▲ Status Per Flow

Ingress	Error Code	Mgid
1-15	None	6

Showing 1 to 1 of 1

## View Remote Monitor Group Status

1. From the Traffic Maps page, click the name of the traffic map that you want to view.
2. On the map page, scroll down to the bottom and click **Remote Monitor Group Status**.

### Remote Monitor Group Status

Remote monitor group status

▲ Status Per Remote Monitor Group

Remote monitor group status

Remote Port Group	Status	Destination Node ID	Destination Node
rpg@115	RemotePortGroupResolved	E8EC4100	PFS5101-115
rpg@110	RemotePortGroupNotFound	0	
rpg@129	RemotePortGroupResolved	F316C100	PFS5111-129

Showing 1 to 3 of 3

Possible status values:

- **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.

## View Output pStack Interface

1. From the Traffic Maps page, click the name of the traffic map that you want to view.
2. On the map page, scroll down to the bottom and click **Output pStack Interface**.



## Output pStack Interface

Output pStack interfaces for given list of input interfaces

Path

pStack Path Index	Input Ports	Network Portgroups	Output pStack Ports	Output pStack Plus Tunnels
0	1-22, 1-33, 1-35, 1-42		1-30, 1-40	67108864

Status: None  
Default: None  
pStack path status

Possible status values:

- **None** – Default status. 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.

## Traffic Filtering

Traffic filtering allows you to limit the types of traffic sent to monitoring tools based on user-specified criteria.

Filtering is especially important when traffic aggregation is involved. Traffic aggregation helps to increase network visibility for monitoring, security, and acceleration tools by providing a way for the tools to see traffic from multiple network access points simultaneously. This benefit can quickly become problematic, however, as bandwidth increases on the aggregate pipes.

By default, PFOS copies all traffic received on the network input ports and forwards it to the output monitor ports, as defined by traffic map settings. By adding filters to the traffic, you can determine which packets are passed to the output ports based on packet content.

With filtering disabled (the default setting), all input port packets are copied to the appropriate monitor or service ports. With filtering enabled, only selected packets are copied to the monitor ports, based upon user-specified packet filtering conditions. Only the monitor or service port output is affected.

Each filter consists of a set of user-specified data values, which are compared to the data in each packet.

The comparison values are specified for standard packet fields (such as the MAC destination address field). Packets that contain the specified data values in the specified packet fields result in a filter match (true). Packets that do not contain the specified data values are a non-match (false).

You can configure a filter expression so that only matching packets are copied (to monitor only the specified type of packet), or so that all packets except matching packets are copied (to monitor all except the specified type of packet).



Each input port can be configured with its own set of filters, or the entire chassis can be configured with a single set of filters that applies to all input ports.

**Note:** You configure filters for [Health Check Profiles](#) within the Health Check GUI.

## Forwarding Filters Library

The Forwarding Filters page displays a list of the currently defined filters and allows you to define new ones. To view details for an existing filter, click its user-defined name.

Forwarding Filters			
^ Forwarding Filter			
Name	Description	Used in Maps	Expression
IPDest		1	IP Dest 192.0.0.1
IPSrc		0	IP Source 192.85.1.2
nonmatch		1	
unfiltered		2	

## Filtering Workflow

Use the following process to set up filtering:

1. Decide how your traffic should be filtered.
2. Create appropriate filters in the Filters page (see “Add a new filter” below).
3. Create traffic mappings that use the filter conditions you created (see [Traffic Maps](#)).

### Add a new filter

1. From the Forwarding Filters page, click **Add**.
2. In the Name field, enter a name to identify the new filter.
3. Click **Add** to open the Filter Expression page.



Forwarding Filter Expression [Advanced Topic Help](#)

**Filter Expression Builder**

Expression Builder  
Monitor packets to/from:

Layer-2 / Layer-3 Settings

MAC Destination: [ ] -or- [ ]  
Mask: [ ] -or- [ ]  
and [ ]  
MAC Source: [ ] -or- [ ]  
Mask: [ ] -or- [ ]

IP Destination: [ ] -or- [ ]  
Mask: [ ] -or- [ ]  
and [ ]  
IP Source: [ ] -or- [ ]  
Mask: [ ] -or- [ ]

Layer 2: EType: [ ] Shortcuts: [ ] VLAN ID: [ ] Tag Priority: [ ] Layer 3: TOS Class: [ ] IPv6 Flow: [ ]

Using protocols:

**Layer-4 Protocol Settings**

Any/Ignore  TCP  UDP  SCTP  ICMP  IGMP  OSPF  RSVP  ARP  RARP  Custom  
Specify other IP Protocol (IPv4/Next Header (IPv6)): [ ]

With ports:

Specify additional Layer 4 Destination Port(s): [ ] -or- [ ] -or- [ ] -or- [ ]  
Specify additional Layer 4 Source Port(s): [ ] -or- [ ] -or- [ ] -or- [ ]

Layer-4 Src/Dest Port Settings

Include custom offset:

Header: None offset: [ ] value: [ ] mask: [ ]

Custom Offset Filter Settings

4. On the Filter Expression page, configure values to define the filter expression. As you specify values or click from one field to another, the Filter Expression field at the top of the page automatically fills in the resulting expression. For example, if you select TCP in the Using protocols section, it is added to the filter expression as IP protocol 6 (the IP protocol number for TCP).

Forwarding Filter Expression [Advanced Topic Help](#)

**IP Protocol 6**

Expression Builder  
Monitor packets to/from:

Layer-2 / Layer-3 Settings

MAC Destination: [ ] -or- [ ]  
Mask: [ ] -or- [ ]  
and [ ]  
MAC Source: [ ] -or- [ ]  
Mask: [ ] -or- [ ]

IP Destination: [ ] -or- [ ]  
Mask: [ ] -or- [ ]  
and [ ]  
IP Source: [ ] -or- [ ]  
Mask: [ ] -or- [ ]

Layer 2: EType: 8055 Shortcuts: [ ] VLAN ID: [ ] Tag Priority: [ ] Layer 3: TOS Class: [ ] IPv6 Flow: [ ]

Using protocols:

**TCP**  Any/Ignore  UDP  SCTP  ICMP  IGMP  OSPF  RSVP  ARP  RARP  Custom  
Specify other IP Protocol (IPv4/Next Header (IPv6)): [ ]

5. Alternatively, you can enter a filter expression directly into the Filter Expression field, or you can edit a filter expression that has been created by specifying values in the other sections of the Filter Expression page. See [Constructing Filter Expressions](#) for descriptions of the fields on this page.
6. Click **Apply** in the toolbar to save the settings to the running configuration.



### Change an existing filter

1. From the Filters page, click the name of the filter that you want to change.
2. Specify the new settings.
3. Click **Apply**.

### Delete one or more existing filters

1. From the Filters page, click on the line containing the filter that you want to delete. The line is highlighted with a gray background.
2. If you want to delete additional filters, control-click on the lines containing those filters, or shift-click to select a range of lines. Each line you select is highlighted with a gray background.
3. Click **Delete**.
4. A confirmation prompt displays. Click **Yes** to confirm the deletion of all selected filters, or click **No** to cancel the deletion.

The screenshot shows a modal dialog titled "Forwarding Filters". At the top, it says "Are you sure you want to delete the selected entries?". Below this are two buttons: "Yes" (highlighted in blue) and "No". The main area contains a table with columns "Name" and "Expression". The table rows are:

Name	Expression
nonmatch	
sdfsd	IP Protocol 6
tcp	IP Protocol 6
udp	IP Protocol 17
unfiltered	

Changing or deleting a filter automatically applies the change to all ports to which the filter was already applied. You cannot delete a filter that is currently in use by a filter map. If you try to do so, PFOS displays an “illegal reference” error when you try to apply the change.

## Constructing Filter Expressions

A filter condition expression is specified with packet field names and values to be compared against the packet field:

packet-field value

Multiple comparisons can be joined using the keywords AND or OR. NETSCOUT recommends that, when creating filter expressions, you always use parentheses to indicate the desired order in which the expression will be evaluated. If you do not use parentheses, the expression will be evaluated from left to right, which might not be the result you want. For example:

```
( mac source 00AA00112233 or Ethernet source 00AA00112234 or Ethernet destination 00AA00112235 ) and (destination IP address 1.2.3.4 or source IP address 1.2.3.4) and IP protocol 6
```



**Caution:** NETSCOUT does not recommend creating filter expressions that include overlapping of IPv4 address ranges, VLAN ranges, or TCP/UDP port ranges. Although PFOS does not report an error message for overlapping range configuration, when PFOS processes the filter, packets matching the overlapping range may have unexpected results in forwarded traffic.

Prior to PFOS 6.4.1, the maximum length of filter expressions on all PFS platforms is limited to 4000 characters when not in a pfsMesh. For PFOS 6.4.1 and later, PFS 5000/7000 platforms can support up to 32000 characters; however, PFS 6000 platforms still support only 4000 characters due to a hardware limitation. PFOS processes filter expressions that are more than 4000 characters for a PFS 6000 within a pfsMesh differently, depending on PFOS version; refer to the following table for details.

**Table 4.2 - Filter Expression Character Limits**

	<b>PFOS 6.4.1 and Later</b>	<b>Prior to PFOS 6.4.1</b>
<b>PFS Devices without pfsMesh</b>		
PFS 5000/7000s	32000 max characters	4000 max characters
PFS 6000s	4000 max characters	4000 max characters
<b>PFS Devices in a pfsMesh</b>		
PFS 5000/7000s in a pfsMesh	32000 max characters	4000 max characters
PFS 6000s Used as Transmit or Destination Node	4000 max characters  When a filter expression with more than 4000 characters is received from PFS 5000/7000s, PFS 6000s will not parse the filter and the error message "HWErrorOnTransitOrDestination" will display at the originating (head) node.	4000 max characters  When a filter expression with more than 4000 characters is received from PFS 5000/7000s: <ul style="list-style-type: none"><li>If PFS 6000s <b>can</b> parse the first 4000 characters of the filter, the filter only processes the characters that were successfully parsed. No error message displays at the originating (head) node.</li><li>If PFS 6000s <b>cannot</b> parse the first 4000 characters of the filter, the entire filter will be dropped and the error message "HWErrorOnTransitOrDestination" will display at the originating (head) node.</li></ul>



The following table shows the fields available to define filter expressions.

**Table 4.3 - Fields Available to Define Filter Expressions**

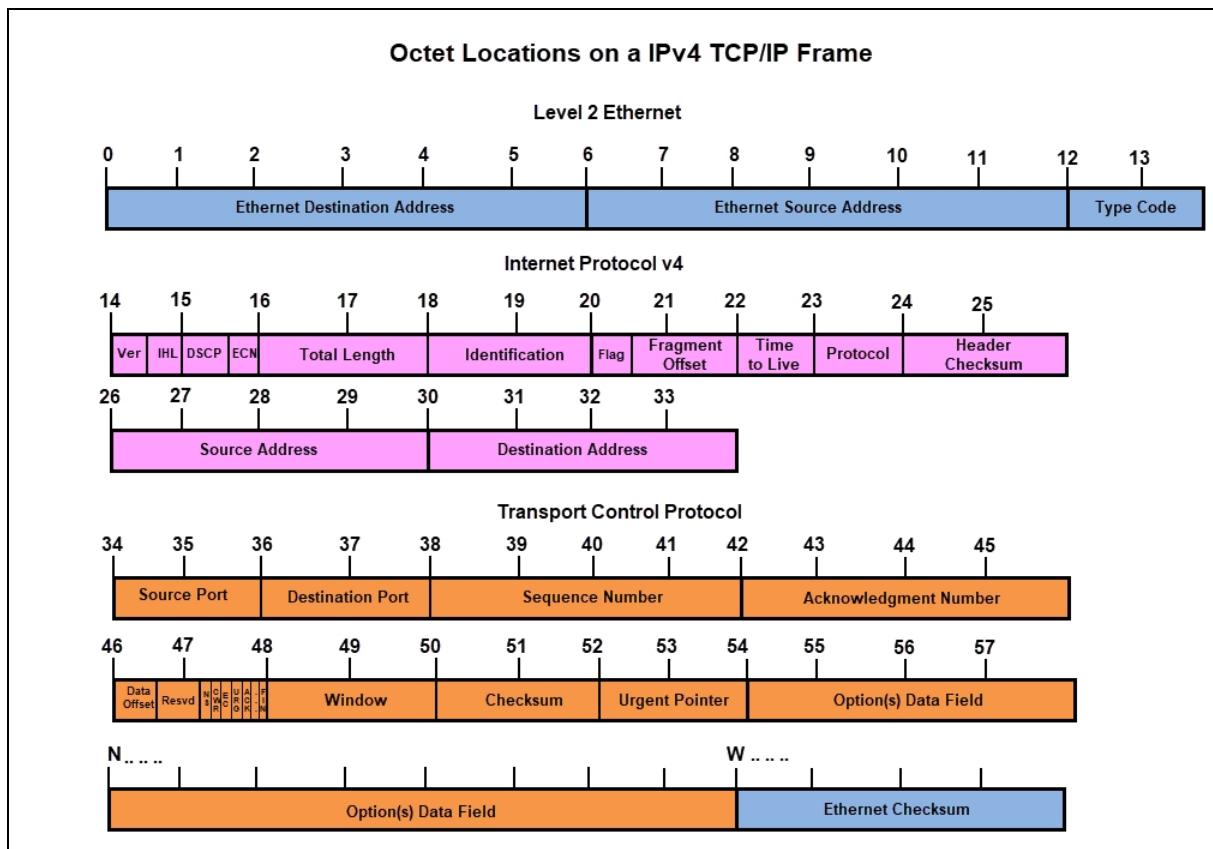
Packet field	Description
MAC source address and mask	Ethernet (IEEE 802.3 - Layer 2) source and destination address. You can use the following keywords: <ul style="list-style-type: none"><li>• AND/OR to combine source and destination conditions.</li><li>• bidi/bidirection to configure address as bidirectional</li></ul>
MAC destination address and mask	
IP source address and mask	IP (Layer 3) source and destination address (if an IP packet). You can use the following keywords: <ul style="list-style-type: none"><li>• AND/OR to combine source and destination conditions.</li><li>• bidi/bidirection to configure address as bidirectional</li></ul>
IP destination address and mask	
Source port	Layer 4 source and destination ports. You can use the following keywords: <ul style="list-style-type: none"><li>• AND/OR to combine source and destination conditions.</li><li>• bidi/bidirection to configure port as bidirectional</li></ul>
Destination port	
EType	Ethernet Type. Use the Shortcuts pull-down list to restrict the EType settings to a particular protocol.
VLAN ID	Enter the IEEE 802.1q VLAN ID (if a tagged packet).
Tag Priority	Enter the IEEE 802.1p/q priority (if a tagged packet).
Layer 3 TOS/Class	Enter the type of service (TOS) class for the filter.
IPv6 flow	Enter the IP Flow field (if an IPv6 packet).
Using Protocols	Select a protocol.
Specify other IP Protocol (IPv4)/Next Header (IPv6)	If the desired protocol is not listed, enter the IP protocol number of the desired protocol.
TCP flag type	Filter packets based on various combinations of TCP flags.
Include custom offset	See <a href="#">Custom Offset Filters</a>

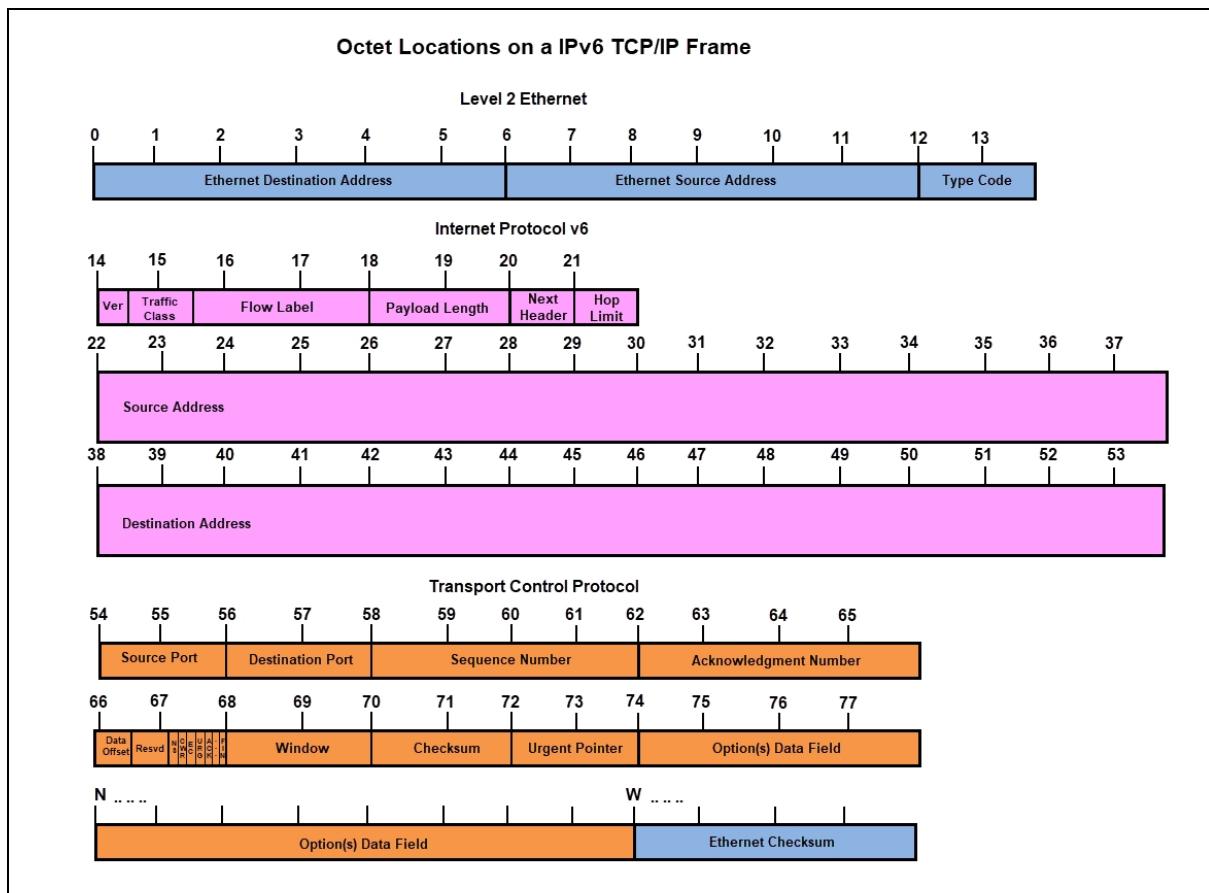
**Note:** PFS platforms DO NOT support VLAN, Layer-2, or Layer-3 filtering on packets with more than two VLAN tags; refer to [Filtering on Packets with Multiple VLAN Tags](#).



## Octet Locations on a TCP/IP Frame for IPv4 and IPv6 Packets

Refer to the following graphics for octet location details.





## Packet Fields

For a complete list of packet field names and syntax that can be used in a filter expression, refer to [PFOS Packet Fields in Filter Expressions](#).

## Special Filters: Unfiltered and Nonmatch

Two built-in filters cannot be deleted or modified:

- **(Nonmatch):** This filter allows user to get visibility of all the traffic which does not match any custom filter on specific network ports (Input Ports).
- **(Unfiltered):** This filter allows user to get visibility of all the traffic on specific network ports (input ports).

PFOS always assigns maps with these two filters as the lowest priority, regardless of map priority. See [Filter Precedence](#) for details about how PFOS processes filters.

## Filter Expression Examples

The following filter matches only HTTP request packets:

```
ip protocol 6 and tcp destination port 80
```



The following filter matches only FTP packets (FTP control or FTP data):

```
ip protocol 6 and tcp destination port 20-21
```

To monitor all traffic to or from a particular node/PC, the system's Ethernet/MAC address (00AA00123456 in this example) can be used in a filter expression such as this:

```
mac source 00AA00123456 or mac destination 00AA00123456
```

Alternatively, the node's IP address could be used (1.2.3.4 in this example):

```
ip source 1.2.3.4 or ip destination 1.2.3.4
```

To monitor one particular connection, conversation, or session between two nodes, (1.2.3.4 and 5.6.7.8 in this example), use an expression like this:

```
(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)
```

To monitor one particular TCP/IP protocol (HTTP in this example), use an expression such as this, which filters IP protocol 6 (TCP) and IP port 80 (HTTP):

```
ip protocol 6 and (tcp source port 80 or tcp destination port 80)
```

In a combination of the above, monitor a particular protocol (such as HTTP) from one particular node (such as 1.2.3.4):

```
(ip source 1.2.3.4 or ip destination 1.2.3.4) and ip protocol 6 and (tcp source port 80 or tcp destination port 80)
```

Configure a filter with the inner VLAN ID 4095:

```
inner vlan 4095
```

Configure a filter with the inner VLAN tag ID 88a8:

```
inner tag 88a8
```

Configure a filter with the inner priority 0:

```
inner priority 0
```

Configure filter to check whether SYN and ACK are set:

```
(type TCPSYN) and (type TCPACK)
```

Configure filter to check whether SYN is not set and ACK is set:

```
(type TCPNotSYN) and (type TCPACK)
```

Configure filter to check whether SYN or ACK is set:

```
(type TCPSYN) or (type TCPACK)
```



## Filtering Bi-directional Traffic

Use `bidi` or `bidirection` commands to simplify filter expression for bidirectional traffic:

Filter for Bi-Directional Traffic	Simplified Expression by Using <code>bidi</code> Command
<code>(src ip 10.10.10.1 and src port 80) or (dest ip 10.10.10.1 and dest port 80)</code>	<code>bidi (src ip 10.10.10.1 and src port 80)</code>
<code>(src ip 10.10.10.1 and dest port 80) or (dest ip 10.10.10.1 and src port 80)</code>	<code>bidi (src ip 10.10.10.1 and dest port 80)</code>
<code>(src ip 10.10.10.1 or dest port 80) or (dest ip 10.10.10.1 or src port 80)</code>	<code>bidirection (src ip 10.10.10.1 or dest port 80)</code>
<code>(src mac 00:00:00:00:00:11 and dest ip 10.1.1.1) or (dest mac 00:00:00:00:00:11 and src ip 10.1.1.1)</code>	<code>bidirection (src mac 00:00:00:00:00:11 and dest ip 10.1.1.1)</code>
<code>(src ip 10.10.10.1 or dest ip 10.10.10.1) and (src port 80 or dest port 80)</code>	<code>bidi (src ip 10.10.10.1) and bidi (src port 80)</code>

## Filter Precedence

Filter precedence refers to the order in which PFOS processes configured traffic map filters. PFOS processes filters in the order the maps appear in the GUI. As you add maps when applying several filters to the same input ports, you are applying the filtering to traffic that did not match (passed through) the previously processed filter. In this manner, PFOS sequentially applies filters to the same traffic, whittling it down to smaller amounts of unmatched traffic.

However, regardless of the order maps appear in the GUI, internally, maps with the built-in filters "Nonmatch" and "Unfiltered" will always be processed last as shown in the following filter precedence order:

1. Maps with User-defined forwarding filters
2. Maps with "Non-match" special filters
3. Maps with "Unfiltered" special filters

The "whittling it down" technique can be used to apply an "is not" filter in that you would apply a filter that has no monitor output and create the next row with a "non-match" filter condition that is mapped to the desired output port. A traffic map with no monitor output port behaves as a map with action = "Drop" described in Step 12 of [Traffic Map Procedures](#). However, if an "Unfiltered" filter is applied to a map for the same input port; "drop" and "forward with no monitor port" will behave very differently; as shown in the examples below.



## Example 1

The following table shows example maps with configured filters.

Name	Type	Description	Mode	Filter	Input Ports	Output Ports	Action
Map-1	Monitor	Packets matching Filter A are sent to port 1-11	Basic	Filter-A	1-1	1-11	Forward
Map-2	Monitor	Packets not matching either Filter A or Filter B are sent to port 1-12	Basic	nonmatch	1-1	1-12	Forward
Map-3	Monitor	All packets except those matching Filter B are sent to port 1-13	Basic	unfiltered	1-1	1-13	Forward
Map-4	Monitor	Packets matching Filter B are dropped	Basic	Filter-B	1-1		Drop

The following table shows the order in which PFOS actually processes the filters. Note that PFOS processes Non-match and Unfiltered maps after all other forwarding filters have been processed.

- Map-1: Traffic at Input port 1-1 hits Filter-A and is forwarded to Output port 1-11.
- Map-4: Traffic at Input port 1-1 hits Filter-B and is dropped.
- Map-2 with Filter="nonmatch" sends all remaining traffic to output port 1-12 (remaining traffic is traffic that was not forwarded by Filter-A and not dropped by Filter-B).
- Map-3 with filter="unfiltered" sends all traffic to output port 1-13 except the traffic that was dropped by Filter-B in Map-4.

Name	Type	Description	Mode	Filter	Input Ports	Output Ports	Action
Map-1	Monitor	Packets matching Filter A are sent to port 1-11	Basic	Filter-A	1-1	1-11	Forward
Map-4	Monitor	Packets matching Filter B are dropped	Basic	Filter-B	1-1		Drop
<b>Map-2</b>	<b>Monitor</b>	<b>Packets not matching Filter A or Filter B to are sent to port 1-12</b>	<b>Basic</b>	<b>nonmatch</b>	<b>1-1</b>	<b>1-12</b>	<b>Forward</b>
<b>Map-3</b>	<b>Monitor</b>	<b>All packets except those matching Filter B are sent to port 1-13</b>	<b>Basic</b>	<b>unfiltered</b>	<b>1-1</b>	<b>1-13</b>	<b>Forward</b>

As described above, in map configurations that include the Drop Action on the same port as the Unfiltered filter, PFOS processes the Drop Action first; therefore, only the packets not matching the filter used in a map with Drop action encounter the Unfiltered filter. When you want a filter to drop traffic and it has the same input port as the Unfiltered filter, it is recommended you configure a forward map without an output port rather than using the Drop Action. Applying a filter in a map without an output port will allow the traffic not matching the filter to be forwarded on the next filter in the process rather than being dropped altogether. See [Example 2](#) for details.



## Example 2

The following table shows example maps with configured filters.

Name	Type	Description	Mode	Filter	Input Ports	Output Ports	Action
Map-1	Monitor	Packets matching Filter A are sent to port 1-11	Basic	Filter-A	1-1	1-11	Forward
Map-2	Monitor	Packets not matching Filter A or Filter B are sent to port 1-12	Basic	nonmatch	1-1	1-12	Forward
Map-3	Monitor	All packets except those matching Filter B are sent to port 1-13	Basic	unfiltered	1-1	1-13	Forward
Map-4	Monitor	Packets matching Filter B are dropped	Basic	Filter-B	1-1		Forward

The following table shows the order in which PFOS actually processes the filters. Note that PFOS processes Non-match and Unfiltered maps after all other forwarding filters have been processed.

- Map-1: Traffic at Input port 1-1 hits Filter-A and is forwarded to Output port 1-11.
- Map-4: Traffic at Input port 1-1 hits Filter-B and is forwarded to an undefined port (that behaves as dropping the packets).
- Map-2 with filter="nonmatch" sends all remaining traffic to output port 1-12 (remaining traffic is traffic that was not forwarded by Filter-A and not dropped by Filter-B).
- Map-3 with filter="unfiltered" sends all traffic to output port 1-13 including the packets matched by Filter-B that were forwarded to an undefined port at Map-4.

Name	Type	Description	Mode	Filter	Input Ports	Output Ports	Action
Map-1	Monitor	Packets matching Filter A are sent to port 1-11	Basic	Filter-A	1-1	1-11	Forward
Map-4	Monitor	Packets matching Filter B are sent to nowhere (no defined port)	Basic	Filter-B	1-1		Forward
<b>Map-2</b>	<b>Monitor</b>	<b>Packets not matching Filter A or Filter B are sent to port 1-12</b>	<b>Basic</b>	<b>nonmatch</b>	<b>1-1</b>	<b>1-12</b>	<b>Forward</b>
<b>Map-3</b>	<b>Monitor</b>	<b>All packets are sent to port 1-13</b>	<b>Basic</b>	<b>unfiltered</b>	<b>1-1</b>	<b>1-13</b>	<b>Forward</b>

## Understanding PFS Filter Resources

One of the key features of NETSCOUT's Packet Flow Switches is their ability to filter packets at line rate. This section describes how the PFS filter resources work and are utilized. This section only applies to the PFS 5000 and 7000 series; however, many of the same concepts also apply to the PFS 6000 series (but some details are, in some cases, significantly different).



NETSCOUT's PFOS makes working with traffic map filters intuitive and as seamless as possible, but in complex configurations it can be beneficial to understand how the switching hardware implements filtering so as to ensure the desired filtering can be achieved within the limits of the filter resources (see [Filter Resource Limits](#) for details on each platform's filter resource limits). Most users do not need to know filter resource details (PFOS manages the filter resources for them); however, advanced users or users who encounter filter resource limits may find this information useful.

## Filter Elements

The basic unit of a filter is a filter element. This is a single filter field without modifiers, for example "ip dest 10.1.2.3". Note that the optional masks on some filter elements (such as, in the filter "ip dest 10.0.0.0/8") do not affect filter resource usage. The [special filters "unfiltered"](#) and ["nonmatch"](#) each count as a single filter element. Thus, every traffic map thus uses at least one filter resource.

## Range Elements

Layer 4 (TCP/UDP/SCTP) port filters use a special table that allows ranges of ports to be selected while using a single filter resource (for example, a port range of 80-100 would use only a single filter resource). This table supports up to 32 ranges; if more than 32 layer 4 port ranges are utilized on the PFS 5000 and 7000 series, then PFOS will use additional filter resources to cover the range. PFOS intelligently uses masks to minimize the number of resources used; for example, a port range of 80-100 that does not fit in the special 32-range table would use 3 filter resources. In other words, once the range table is full, port ranges that do not fit in the table are automatically translated into a more complex filter.

The VLAN filter element also supports ranges on the PFS 5000 and 7000 series. As with port ranges, PFOS intelligently uses masks to minimize the number of filter resources used; for example, a filter of "vlan 200-300" uses 7 resources.

The IP address filter elements also support ranges on the PFS 5000 and 7000 series. As with the other ranges, PFOS intelligently uses masks to minimize the number of filter resources used; for example, a filter of "10.10.10.7-10.10.10.13" takes 3 resources.

## Calculating Filter Resource Usage

This section explains how to approximate the number of filter resources that a given configuration will use.

## Basic Filter Resource Usage Rules

As described in [Filter Elements](#), each traffic map will use at least one filter resource (including when using the built-in `unfiltered` and `nonmatch` filters).

The number of filter resources used by a traffic map is not dependent on the number of ingress (Span) or egress (Monitor) ports or the usage (or non-usage) of port groups unless the ingress ports are on different "pipes" (see the subsections on pipes in [Filter Resource Limits](#) for details). When ingress ports for a traffic map are spread across multiple pipes, the filter resources must be allocated on each pipe that has one or more ingress ports used in the traffic map. For



example, if a filter uses 4 filter resources, then a traffic map using that filter with ingress ports on 2 pipes will allocate 4 filter resources on each pipe for a total of 8 (4x2) filter resources. As such, when possible, it makes sense to keep ingress ports that are used in the same traffic map(s) together on the same pipe.

Each traffic map using a given filter will allocate the number of filter resources required by that filter. For example, if a filter uses 4 filter resources, 3 traffic maps using that filter will utilize 12 (4x3) filter resources. As such, when possible, it makes sense to combine traffic maps that use the same filter into one traffic map.

### Filter Resource Usage with Multi-Element Filters

To calculate the number of filter resources used by a filter which uses the AND and OR operators to combine multiple filter elements, follow these steps while retaining any grouping parenthesis:

1. Expand any expressions using the `bidi()` keyword with the equivalent filter without `bidi()`. See [bidi examples](#) for details.
2. Replace each VLAN or IP address filter element that includes a range (such as, “`vlan 200-300`”) with either “1” (for simplicity) or (for a more accurate approximation) the integer result of `log2()` on the number of VLAN IDs or IP addresses covered by the range. **Note:** This simplification is inaccurate for large IP address ranges (such as, where the range crosses multiple bytes).
3. Replace each filter element (including any custom offset filters) with the number 1 (that is, replace “`ip dest 192.168.0.250`” with “1”).
4. Replace each AND operator with the multiplication symbol (“`x`”).
5. Replace each OR operator with the addition symbol (“`+`”).
6. Solve the resulting mathematical expression.

For example, the filter “`ip source 192.168.0.250 OR ip dest 192.168.0.250`” becomes “ $1 + 1$ ” meaning that this filter will use 2 filter resources.

Note that the calculation steps do not take into account the special filter resource usage of the layer 4 (TCP/UDP/TCP) port filter when more than 32 ports or port ranges are used. See [Range Elements](#) for details.

The following table shows a few more examples of how combining the AND and OR operators affects the resulting number of filter resources. The last few examples show that care should be taken when using AND to combine multiple sub-expressions that use the OR operator.

Filter Expression	Filter Resources	Explanation
A	1	$1 = 1$
A and B and C and D and E	1	$1 \times 1 \times 1 \times 1 \times 1 = 1$
A or B or C or D or E	5	$1+1+1+1+1 = 5$
(A and B) or (C and D)	2	$(1 \times 1) + (1 \times 1) = 2$
(A or B) and (C or D)	4	$(1+1) \times (1+1) = 4$
(A or B or C or D) and (E or F or G) and (H or I or J)	36	$(1+1+1+1) \times (1+1+1) \times (1+1+1) = 36$



## Filter Resources Usage by pStack and pStack+

pStack and pStack+ use PFS filters to move packets through a pfsMesh to their final destination. This section explains how pStack and pStack+ use filter resources on the head, transit, and end nodes used by a traffic map using pfsMesh.

### Filter Usage on Head Nodes

When a traffic map is created and its destination is or includes a remote (pfsMesh-visible) port group the filter resources used on the originating (or head) node are the same as described in the previous sections. The filter is used unmodified in order to achieve the selection of packets that the user requested.

### pStack Filter Usage on Transit and End Nodes

When a packet traveling through a pfsMesh arrives at a transit or end node, it will arrive via a pStack port (pStack+ ports behave quite differently, see [pStack+ Filter Usage on Transit and End Nodes](#)) which may be carrying traffic for many different traffic maps, possibly from the same ingress port(s) as the packet in question. In order to differentiate packets from the various traffic maps, PFOS will install modified versions of the user's filter on each transit node and the end node in the traffic map's path. The filters PFOS installs on each transit and end node are modified to include a VLAN tag which pStack uses internally to indicate the ingress port of the traffic; one filter is installed for each ingress port.

For example, if a user sends traffic from PFS A to a port group on PFS C via PFS B using the filter "ip dest 10.1.2.3 OR ip src 10.1.2.3" then PFOS will install the user's original filter on PFS A and, for each ingress port on PFS A, one filter of the form "vlan N AND (ip dest 10.1.2.3 OR ip src 10.1.2.3)" on the transit and end nodes where N is the VLAN ID assigned by pStack to the ingress port on PFS A. The following table shows pStack filter resource usage on the head, transit, and end nodes with a filter that uses 5 filter resources for different numbers of ingress ports.

Number of Ingress Ports	Head Node Filter Resources	Transit Node(s) Filter Resources	End Node Filter Resources
1	5	5	5
2	5	10	10
4	5	20	20

### pStack+ Filter Usage on Transit and End Nodes

When a packet traveling through a pfsMesh arrives at a transit or end node via a pStack+ port, pStack+ is able to differentiate packets from different traffic maps without relying on the user's filter. Transit and end nodes will not use any *user* filter resources to move the packets from the ingress pStack+ port to the egress port(s). pStack+ will use one filter resource on pStack+ ingress plus one filter resource on pStack+ egress, both from the control (group 10) filter resources, for each traffic map. The following table shows pStack+ filter resource usage on the head, transit, and end nodes with a filter that uses 5 filter resources for different numbers of ingress ports.

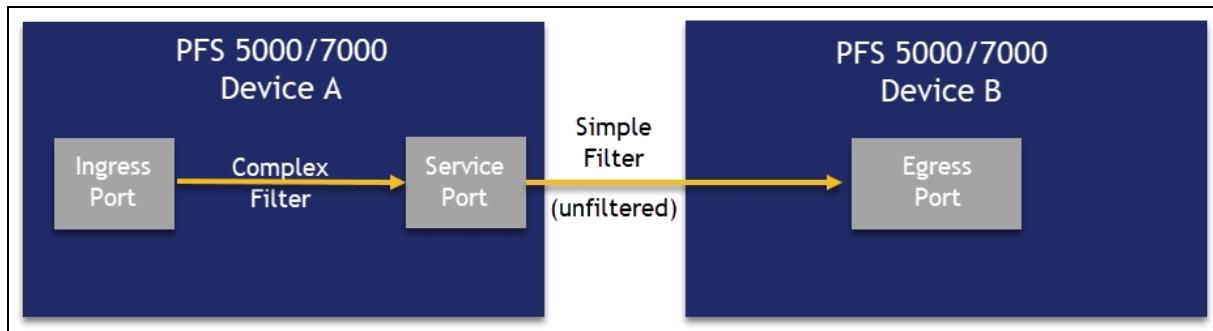


Number of Ingress Ports	Head Node Filter Resources	Transit Node(s) Filter Resources	End Node Filter Resources
1	5 (user) +1 (control)	2 (control)	1 (control)
2	5 (user) +1 (control)	2 (control)	1 (control)
4	5 (user) +1 (control)	2 (control)	1 (control)

## Limiting pStack Filter Usage

As described above, pStack (but not pStack+) will install the traffic map's filter on each node in the pfsMesh path; transit and end nodes will have the filter applied once for each ingress port in the traffic map. If filter resources become a limitation on the transit and end nodes, upgrading from pStack to pStack+ is the simplest solution. Another solution is to simplify the filter used in that traffic map. This can be achieved either by simplifying the original filter itself or by adding a Service port on the head (originating) node between the ingress port and the final destination. The complex filter is used to select traffic from the ingress port and send it to the (local) Service port. A new traffic map is then created to send the traffic from the Service port to the remote destination using a very simple filter (often unfiltered). Thus, when pStack installs the necessary filters on the transit and end nodes it will do so using a very simple filter that uses minimal filter resources. Reducing the number of ingress ports in the traffic map (by aggregating several ingress ports' traffic into a Service port) will also reduce filter resource usage on transit and end nodes.

The following graphic illustrates how filter resources used by pStack can be optimized by inserting a Service port between the ingress and egress ports.



## Filter Resource Limits

Standard filter expression resource limits vary by platform. Refer to the following sections for filter resource limit details:

- [PFS 5010/7010 Filter Resource Limits](#)
- [PFS 51xx/71xx Filter Resource Limits](#)
- [PFS 503x/703x-32X, PFS 5031/7031-56X, and PFS 5030/7030-54X Filter Resource Limits](#)
- [PFS 5040/7040-32D Filter Resource Limits](#)



- [PFS 5041/7041-32D Filter Resource Limits](#)
- [PFS 6000 Series Filter Resource Limits](#)

## PFS 5010/7010 Filter Resource Limits

Standard filter expression resource limits are 12,288 entries per system. The following graphic shows the PFS 5010/7010 current filter resource usage report. To access the report, click **Filter Resources** at the top of the PFOS Web UI Traffic Maps page.

Filter Resources						
UDF Bytes Occupied:		4 / 32				
Ranges Used/Supported:		0 / 32				
TCAM Information:						
Group	Priority	TCAM Total	TCAM Used	TCAM Free	Bits Used	Group Mode
0	7ffff	1024	145	879	32	Single
10	7fff5	5120	4	5116	294	Double
20	7ffeb	12288	5109	7179	142	Single
MODE: sip-mode						
Status: ALL FLOWS ARE IN WORKING STATE						

For the 5010/7010, each system can support:

- UDF (User Defined Filter) is for Custom Offset filters:
  - A total of up to 32 UDF bytes may be defined.
  - Each UDF may contain up to 16 bytes.
  - Maximum offset value is 127; match up to the 128th byte from the start of a packet.
  - System uses 4 bytes when Tunnel functionality is enabled (including IP Tunnel Termination, L2GRE or VxLAN tunnel, and pStack+).
- **Note:** Tunnel functionality is enabled as a default; to disable, see the [Tunnel](#) option on the Global Settings > System>Features page.
  - Each UDF setting may start from an even or odd offset.
  - Hardware program always starts at even offset and occupies even numbers of bytes.
- For example, “Offset 1 0xA0B” will use 4 bytes as offset (0,1)=0x000A and offset (2,3)=0xB00.
- TCP-UDP Port Range settings without using extra TCAM is up to 32 different ranges. Once it reaches 32 ranges, users can configure additional port ranges, but each port range may consume one or more filter entries.



- TCAM Information:
  - *Group 0* is used for source or destination IPv4 or IPv6 addresses when [Map Profile](#) is set to SIP or DIP or SIP-IPv6 or DIP-IPv6 mode.
    - SIP or DIP mode can support 1024 IPv4 only addresses or 1024 IPv6 only addresses; or 512 of mixing IPv4 and IPv6 addresses.
    - SIP-IPv6 or DIP-IPv6 mode can support 1024 IPv6 addresses; no IPv4 addresses will be added to the group.
  - *Group 10* filters are internal filters for control packets. These filters are for internal use only and do not apply to users. With system default configuration only Group 10 is created.
  - *Group 20* and onward are used for user's filters with the following capabilities:
    - 12,288 filter entries if each Field Selector has been used once (all groups are single slice).
    - 6144 or 4096 entries if filter expression is more complicated and uses multiple Field Selectors (some groups are double slices).
    - A new group is created when total match condition bits (Qset bits) are more than 320 bits, or if a new filter condition needs to be programmed at a different group per hardware restriction. The new group is for QSet bits in new maps; it excludes QSet bit used before the new map.
- “Mode” displays current [map profiles](#) that can be configured to extend current filter capability.
- “Status” indicates if current traffic map running configuration has an error. If Status shows FEW FLOWS ARE IN ERROR STATE, use the CLI command `show map map_status` to read all map status.



## PFS 51xx/71xx Filter Resource Limits

Standard filter expression resource limits are 2,560 entries per pipe (refer to [PFS 51xx/71xx Pipes](#)). The following graphic shows the PFS 5100/7100 current filter resource usage report. To access the report, click **Filter Resources** at the top of the PFOS Web UI Traffic Maps page.

Filter Resources							
UDF Bytes Occupied:		0 / 32					
Ranges Used/Supported:		0 / 32					
Group	Priority	TCAM Total	TCAM Used	TCAM Free	Bits Used	Group Mode	
PIPE: 1 (#1-21 to #1-24 and #1-29 to #1-32)							
0	7ffff	1024	1	1023	128	Single	
10	7fff5	1024	4	1020	278	Double	
20	7ffeb	2560	3	2557	106	IntraSliceDouble	
PIPE: 2 (#1-1 to #1-4 and #1-9 to #1-12)							
1	7fff1	1024	1	1023	128	Single	
11	7fff4	1024	4	1020	278	Double	
30	7ffe1	2560	3	2557	106	IntraSliceDouble	
PIPE: 3 (#1-5 to #1-8 and #1-13 to #1-16)							
2	7fffd	1024	1	1023	128	Single	
12	7fff3	1024	4	1020	278	Double	
40	7ffd7	2560	3	2557	106	IntraSliceDouble	
PIPE: 4 (#1-17 to #1-20 and #1-25 to #1-28)							
3	7fff1	1024	1	1023	128	Single	
13	7fff2	1024	4	1020	278	Double	
50	7ffcd	2560	3	2557	106	IntraSliceDouble	
MODE: sip-mode							
Status: ALL FLOWS ARE IN WORKING STATE							

When a system [Map Profile](#) is configured as SIP (Source) or DIP (Destination) mode; each pipe can support up to 1024 source or destination IPv4 or IPv6 entries. When a Map Profile is configured as Auto mode; once Source or Destination IPs reach 1024 entries, system will automatically convert the Map Profile to Legacy mode.



For the PFS 51xx/71xx series, each system can support:

- UDF (User Defined Filter) is for Custom Offset filters:
  - A total of up to 32 UDF bytes may be defined.
  - Each UDF may contain up to 16 bytes.
  - Maximum offset value is 127; match up to 128th byte from the start of a packet
  - System uses 4 bytes when Tunnel functionality is enabled (including IP Tunnel Termination, L2GRE or VxLAN tunnel, and pStack+).
- **Note:** Tunnel functionality is enabled as a default; to disable, see the [Tunnel](#) option on the Global Settings > System > Features page.
  - Each UDF setting may start from an even or odd offset
  - Hardware program always starts at even offset and occupies even numbers of bytes.
- For example, “Offset 1 0x0A0B” will use 4 bytes as offset (0,1)=0x000A and offset (2,3)=0xB00.
- TCP-UDP Port Range settings without using extra TCAM is up to 32 different ranges. Once it reaches 32 ranges, users can configure additional port ranges, but each port range may consume one or more filter entries.
- TCAM Information:
  - *Group 0, 1, 2, and 3* are used for source or destination IPv4 or IPv6 addresses when [Map Profile](#) is set to SIP or DIP or SIP-IPv6 or DIP-IPv6 mode.
    - SIP or DIP mode can support 1024 IPv4 only addresses or 1024 IPv6 only addresses; or 512 of mixing IPv4 and IPv6 addresses.
    - SIP-IPv6 or DIP-IPv6 mode can support 1024 IPv6 addresses; no IPv4 addresses will be added to the group.
  - *Group 10, 11, 12, and 13* filters are internal filters for control packets. These filters are for internal use only and do not apply to users. With system default configuration only Group 10, 11, 12, and 13 are created.
  - *Group 20 to Group 29* and *Group 30 to Group 39* and *Group 40 to Group 49* and *Group 50 to Group 59* are used for user's filters at each pipe.
    - 2560 entries if total match condition bits (Qset bits) are 160 bits or less (Group Mode: IntraSliceDouble/Single)
    - 768 entries if total match condition bits (Qset bits) are between 160 and 480 bits (inclusive). (Group Mode: Double/Triple)
    - 512 entries in a new group (mode Triple).
    - A new group will be created when total match condition bits (Qset bits) exceed 480 bits, or if a new filter condition needs to be programmed at a different group per hardware restriction. The new group is for QSet bits in new maps; it excludes QSet bits used before the new map.
  - “Mode” displays the current [map profiles](#) that can be configured to extend current filter capability.
  - “Status” indicates if current traffic map running configuration has an error. If Status shows FEW FLOWS ARE IN ERROR STATE, use the CLI command `show map map_status` to read all map status.



## PFS 51xx/71xx Pipes

PFS 51xx/71xx filter resources are divided into four pipes. Filter resources are utilized on the source port(s) of any traffic map. The following table explains which ports are in which pipe on the various 51xx/71xx PFS devices:

PFS	Pipe	Ports
<b>5100/7100</b>	1	1-21 to 1-24 1-29 to 1-32
	2	1-1 to 1-4 1-9 to 1-12
	3	1-5 to 1-8 1-13 to 1-16
	4	1-17 to 1-20 1-25 to 1-28
<b>5110/7110</b>	1	1-49 to 1-50 1-52 to 1-53
	2	1-1 to 1-12 1-17 to 1-24
	3	1-13 to 1-16 1-25 to 1-36
	4	1-37 to 1-48 1-51 1-54
<b>5120/7120</b>	1	1-9 to 1-12 1-21 to 1-24 1-41 to 1-44 1-53 to 1-56
	2	1-1 to 1-8 1-33 to 1-40
	3	1-13 to 1-20 1-45 to 1-52
	4	1-25 to 1-32 1-57 to 1-64



PFS	Pipe	Ports
<b>5121/7121-64X</b>	1	1-1 to 1-2 1-9 to 1-14 1-33 to 1-34 1-41 to 1-46
	2	1-3 to 1-8 1-15 to 1-16 1-35 to 1-40 1-47 to 1-48
	3	1-17 to 1-18 1-25 to 1-30 1-49 to 1-50 1-57 to 1-62
	4	1-19 to 1-24 1-31 to 1-32 1-51 to 1-56 1-63 to 1-64



## PFS 503x/703x-32X, PFS 5031/7031-56X, and PFS 5030/7030-54X Filter Resource Limits

The following graphic shows the PFS 503x/703x-32X current filter resource usage report. To access the report, click **Filter Resources** at the top of the PFOS Web UI Traffic Maps page.

Filter Resources						
UDF Information: 24 Used/32 Supported						
UDF Type	Bytes Used	Max Bytes				
MAC	0	4				
L4	0	16				
L2WITHVLAN	0	16				
UNKNOWNL3	8	28				
MPLS	0	16				
IPv4	0	16				
IPv6	0	14				
KNOWNNONIP	0	28				
UNKNOWNL4	0	22				
GRE	0	16				
GREERSSPAN	16	16				
Ranges Used/Supported: 0 / 32						
TCAM Information:						
Group	Priority	TCAM Total	TCAM Used	TCAM Free	Bits Used	Group Mode
0	7ffff	512	6	506	160	IntraSliceDouble
10	7fff5	1536	5	1531	310	Triple
20	7ffeb	1536	8	1528	402	Triple
21	7ffea	1536	5	1531	226	Double
PIPE: 1 (#1-1 to #1-16)						
11	7fff4	2304	5	2299	310	Triple
30	7ffe1	2304	3	2301	302	Double
PIPE: 2 (#1-17 to #1-32)						
MODE: sip-mode						
Status: ALL FLOWS ARE IN WORKING STATE						



The following graphic shows the PFS 5030/7030-54X current filter resource usage report.

Filter Resources					
+ UDF Information: 24 Used/32 Supported					
UDF Type	Bytes Used	Max Bytes			
MAC	0	4			
L4	0	16			
L2WITHVLAN	0	16			
UNKNOWNL3	8	28			
MPLS	0	16			
IPv4	0	16			
IPv6	0	14			
KNOWNNONIP	0	28			
UNKNOWNL4	0	22			
GRE	0	16			
GREERSSPAN	16	16			
+ Ranges Used/Supported: 0 / 32					
+ TCAM Information:					
Group	Priority	TCAM Total	TCAM Used	TCAM Free	Bits Used
					Group Mode
10	7fff5	1536	8	1528	310
20	7ffeb	1536	7	1529	434
21	7ffea	1536	9	1527	302
+ MODE: legacy					
Status: ALL FLOWS ARE IN WORKING STATE					

For the PFS 503x/703x series, each system can support:

- UDF (User Defined Filter) is for Custom Offset filters:
  - A total of up to 32 UDF bytes may be defined.
  - The number of bytes supported by each custom offset filter varies by packet type up to a maximum of 16 bytes.
  - [Starting offset](#) varies across packets based on packet type (L2/L3/L4) and protocol associated to each packet type.
  - Maximum offset value is 127; match up to the 128th byte from the start of a packet.
  - [Inner filters](#) also use custom offset filters internally; the number of UDF bytes used varies depending on which inner filters are used.
- TCP-UDP Port Range settings without using extra TCAM is up to 32 different ranges. Once it reaches 32 ranges, users can configure additional port ranges, but each port range may consume one or more filter entries.



- PFS 503x/703x series (except [PFS 5030/7030-54X](#)) TCAM Information:
  - *Group 0* and *Group 1* are used for source or destination IPv4 or IPv6 addresses when [Map Profile](#) is set to SIP or DIP or SIP-IPv6 or DIP-IPv6 mode.
    - SIP or DIP mode can support 1024 IPv4 only addresses or 1024 IPv6 only addresses; or 512 of mixing IPv4 and IPv6 addresses.
    - SIP-IPv6 or DIP IPv6 mode can support 1024 IPv6 addresses; no IPv4 addresses will be added to the group.
  - *Group 10* and *Group 11* filters are internal filters for control packets. These filters are for internal use only and do not apply to users. With system default configuration only Group 10 and 11 are created.
  - *Group 20* to *Group 29* and *Group 30* to *Group 39* are used for user's filters at each pipe.
    - 6912 entries if total match condition bits (Qset bits) are 160 bits or less (Group Mode: IntraSliceDouble/Single)
    - 2304 entries if total match condition bits (Qset bits) are between 160 and 480 bits (inclusive). (Group Mode: Triple)
    - A new group will be created when total match condition bits (Qset bits) exceed 480 bits, or if a new filter condition needs to be programmed at a different group per hardware restriction. The new group is for QSet bits in new maps; it excludes QSet bits used before the new map.
- PFS 5030/7030-54X (Single Pipe) TCAM Information:
  - *Group 0* is used for source or destination IPv4 or IPv6 addresses when [Map Profile](#) is set to SIP or DIP or SIP-IPv6 or DIP-IPv6 mode.
    - SIP or DIP mode can support 1024 IPv4 only addresses or 1024 IPv6 only addresses; or 512 of mixing IPv4 and IPv6 addresses.
    - SIP-IPv6 or DIP IPv6 mode can support 1024 IPv6 addresses; no IPv4 addresses will be added to the group.
  - *Group 10* filters are internal filters for control packets. These filters are for internal use only and do not apply to users. With system default configuration only Group 10 is created.
  - *Group 20* to *Group 29* are used for user's filters in single pipe.
    - 6912 entries if total match condition bits (Qset bits) are 160 bits or less (Group Mode: IntraSliceDouble/Single)
    - 2304 entries if total match condition bits (Qset bits) are between 160 and 480 bits (inclusive). (Group Mode: Triple)
    - A new group will be created when total match condition bits (Qset bits) exceed 480 bits, or if a new filter condition needs to be programmed at a different group per hardware restriction. The new group is for QSet bits in new maps; it excludes QSet bits used before the new map.
- “Mode” displays the current [map profiles](#) that can be configured to extend current filter capability.
- “Status” indicates if current traffic map running configuration has an error. If Status shows FEW FLOWS ARE IN ERROR STATE, use the CLI command `show map map_status` to read all map status. See example output in [PFS 503x/703x Custom Offset Error Handling](#).



## PFS 503x/703x Pipes

PFS 5031/7031-56X and PFS 503x/703x-32X filter resources are divided into two pipes; the PFS 5030/7030-54X only has one pipe. Filter resources are utilized on the source port(s) of any traffic map. The following table explains which ports are in which pipe on the PFS 503x/703x devices:

PFS	Pipe	Ports
<b>503x/703x-32X</b>	1	1-1 to 1-16
	2	1-17 to 1-32
<b>5031/7031-56X</b>	1	1-1 to 1-12 1-25 to 1-36 1-53 to 1-56
	2	1-13 to 1-24 1-37 to 1-52
<b>5030/7030-54X</b>	1	1-1 to 1-54



## PFS 5040/7040-32D Filter Resource Limits

The following graphic shows the PFS 5040/7040-32D current filter resource usage report. To access the report, click **Filter Resources** at the top of the PFOS Web UI Traffic Maps page.

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)							
1	1	18431	1	18430	0	Single	
10	7fff5	10239	4	10235	262	Double	
20	7ffeb	18431	2	18429	74	Single	
PIPE: 2 (#1-1 to #1-8)							
2	2	18431	1	18430	0	Single	
11	7fff4	10239	4	10235	262	Double	
30	7ffe1	18431	2	18429	74	Single	
PIPE: 3 (#1-13 to #1-20)							
3	3	18431	1	18430	0	Single	
12	7fff3	10239	4	10235	262	Double	
40	7ffd7	18431	2	18429	74	Single	
PIPE: 4 (#1-25 to #1-32)							
4	4	18431	1	18430	0	Single	
13	7fff2	10239	4	10235	262	Double	
50	7ffcd	18431	2	18429	74	Single	
MODE: legacy							
Status: ALL FLOWS ARE IN WORKING STATE							



For the PFS 5040/7040 series, each system can support:

- UDF (User Defined Filter) is for Custom Offset filters:
  - A total of up to 19 UDF bytes may be defined.
  - The number of bytes supported by each custom offset filter varies by packet type up to a maximum of 16 bytes.
  - [Starting offset](#) varies across packets based on packet type (L2/L3/L4) and protocol associated to each packet type.
  - Maximum offset value is 127; match up to the 128th byte from the start of a packet.
  - [Inner filters](#) also use custom offset filters internally; the number of UDF bytes used varies depending on which inner filters are used.
- TCP-UDP Port Range settings without using extra TCAM is up to 32 different ranges. Once it reaches 32 ranges, users can configure additional port ranges, but each port range may consume one or more filter entries.
- TCAM Information:
  - *Groups 1-4* are for internal system use only; display filters to drop packets not matching user configured traffic maps.
  - *Group 10-13* filters are internal filters for control packets. These filters are for internal use only and do not apply to users. With system default configuration only Group 10 and 11 are created.
  - *Group 20 to Group 29* and *Group 30 to Group 39* and *Group 40 to Group 49* and *Group 50 to Group 59* are used for user's filters at each pipe.
    - 18431 entries if total match condition bits (Qset bits) are 160 bits or less (Group Mode: Single)
    - 8191 entries if total match condition bits (Qset bits) are between 160 and 280 bits (inclusive). (Group Mode: Double)
    - 4095 entries if total match condition bits (Qset bits) are between 280 and 446 bits (inclusive). (Group Mode: Triple)
    - A new group will be created when total match condition bits (Qset bits) exceed 446 bits, or if a new filter condition needs to be programmed at a different group per hardware restriction. The new group is for QSet bits in new maps; it excludes QSet bits used before the new map.
  - “Mode” displays the current [map profiles](#) that can be configured to extend current filter capability.
  - “Status” indicates if current traffic map running configuration has an error. If Status shows FEW FLOWS ARE IN ERROR STATE, use the CLI command `show map map_status` to read all map status.



## PFS 5040/7040-32D Pipes

PFS 5040/7040-32D filter resources have 8 pipes with 4 ports each for data traffic and 4 pipes with 8 ports each for ingress packet processing for filters. Filter resources are utilized on the source port(s) of any traffic map. The following table explains which ports are in which pipe on the PFS 5040/7040-32D devices:

<b>PFS</b>	<b>Pipe</b>	<b>Ports</b>
<b>5040/7040-32D</b>	1	1-21 to 1-24
		1-9 to 1-12
	2	1-1 to 1-4
		1-5 to 1-8
	3	1-13 to 1-16
		1-17 to 1-20
	4	1-25 to 1-28
		1-29 to 1-32



## PFS 5041/7041-32D Filter Resource Limits

The following graphic shows the PFS 5041/7041-32D current filter resource usage report. To access the report, click **Filter Resources** at the top of the PFOS Web UI Traffic Maps page.

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 (#1-1 to #1-8)						
1	1	1023	1	1022	0	Single
10	7fff5	1023	4	1019	262	Double
20	7ffeb	9215	9215	0	50	Single
PIPE: 2 (#1-9 to #1-16)						
2	2	1023	1	1022	0	Single
11	7fff4	1023	4	1019	262	Double
30	7ffe1	9215	9215	0	50	Single
PIPE: 3 (#1-17 to #1-24)						
3	3	1023	1	1022	0	Single
12	7fff3	1023	4	1019	262	Double
40	7ffd7	9215	9215	0	50	Single
PIPE: 4 (#1-25 to #1-32)						
4	4	1023	1	1022	0	Single
13	7fff2	1023	4	1019	262	Double
50	7ffcd	9215	9215	0	50	Single
MODE: legacy						
Status: ALL FLOWS ARE IN WORKING STATE						

For the PFS 5041/7041 series, each system can support:

- UDF (User Defined Filter) is for Custom Offset filters:
  - A total of up to 19 UDF bytes may be defined.
  - The number of bytes supported by each custom offset filter varies by packet type up to a maximum of 16 bytes.
  - [Starting offset](#) varies across packets based on packet type (L2/L3/L4) and protocol associated to each packet type.
  - Maximum offset value is 127; match up to the 128th byte from the start of a packet.
- TCP-UDP Port Range settings without using extra TCAM is up to 32 different ranges. Once it reaches 32 ranges, users can configure additional port ranges, but each port range may consume one or more filter entries.



- TCAM Information:
  - Groups 1-4 are for internal system use only; display filters to drop packets not matching user configured traffic maps.
  - Group 10-13 filters are internal filters for control packets. These filters are for internal use only and do not apply to users. With system default configuration only Group 10 and 11 are created.
  - Group 20 to Group 29 and Group 30 to Group 39 and Group 40 to Group 49 and Group 50 to Group 59 are used for user's filters at each pipe.
    - 9215 entries if total match condition bits (Qset bits) are 160 bits or less (Group Mode: Single)
    - 4095 entries if total match condition bits (Qset bits) are between 160 and 280 bits (inclusive). (Group Mode: Double)
    - 2047 entries if total match condition bits (Qset bits) are between 280 and 446 bits (inclusive). (Group Mode: Triple)
    - A new group will be created when total match condition bits (Qset bits) exceed 446 bits, or if a new filter condition needs to be programmed at a different group per hardware restriction. The new group is for QSet bits in new maps; it excludes QSet bits used before the new map.
- “Mode” displays the current [map profiles](#) that can be configured to extend current filter capability.
- “Status” indicates if current traffic map running configuration has an error. If Status shows FEW FLOWS ARE IN ERROR STATE, use the CLI command `show map map_status` to read all map status.

## PFS 5041/7041-32D Pipes

PFS 5041/7041-32D filter resources have eight pipes with four ports each for data traffic and four pipes with eight ports each for ingress packet processing for filters. Filter resources are utilized on the source port(s) of any traffic map. The following table explains which ports are in which pipe on the PFS 5041/7041-32D devices:

PFS	Pipe	Ports
<b>5041/7041-32D</b>	1	1-1 to 1-4
		1-5 to 1-8
	2	1-9 to 1-12
		1-13 to 1-16
	3	1-17 to 1-20
		1-21 to 1-24
	4	1-25 to 1-28
		1-29 to 1-32



## PFS 6000 Series Filter Resource Limits

Standard filter expression resource limits are 12,544 entries per [200G port group](#). The following graphic shows the PFS 6000 Series current filter resource usage report. To access the report, click **Filter Resources** at the top of the PFOS Web UI Traffic Maps page.

Resource Processing Log LC Slot	Port Range	Range Checker Elements Max	Elements Used	Custom/Offset Elements Max	Elements Used	Group ID	Filtering Elements Pool	Allocated	Used	Free	Load Balance Criteria				
											L2	L3	L4	InPort	
1	1 to 2	24	0	30	0	6272	SRCMAC	DSTMAC	ETYPE	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT	Excluded
	3 to 4	24	0	30	0		SRCMAC	DSTMAC	ETYPE	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT	Excluded
	5 to 6	24	0	30	0		SRCMAC	DSTMAC	ETYPE	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT	Excluded
2	1 to 20	24	0	30	0	6272	SRCMAC	DSTMAC	ETYPE	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT	Excluded
	21 to 37	24	0	30	0		SRCMAC	DSTMAC	ETYPE	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT	Excluded
	38 to 42	24	0	30	0		SRCMAC	DSTMAC	ETYPE	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT	Excluded
3	1 to 20	24	0	30	0	6272	2	3072	2200	872	SRCIP	DSTIP			Excluded
	21 to 37	24	0	30	0		2	6272	2048	1320	728	SRCIP	DSTIP		Excluded
	38 to 42	24	0	30	0		2	6272	1024	4	1020	SRCIP	DSTIP		Excluded
4	1 to 20	24	0	30	0	6272	2	3072	2200	872	SRCIP	DSTIP			Excluded
	21 to 37	24	0	30	0		2	6272	2048	1320	728	SRCIP	DSTIP		Excluded
	38 to 42	24	0	30	0		2	6272	1024	4	1020	SRCIP	DSTIP		Excluded
5	1 to 20	24	0	30	0	6272	2	3072	2240	832	SRCIP	DSTIP			Excluded
	21 to 37	24	0	30	0		2	6272	2048	1352	696	SRCIP	DSTIP		Excluded
	38 to 42	24	0	30	0		2	6272	1024	48	976				Excluded
6	1 to 20	24	0	30	0	6272	2	3072	2240	832	SRCIP	DSTIP			Excluded
	21 to 37	24	0	30	0		2	6272	2048	1352	696	SRCIP	DSTIP		Excluded
	38 to 42	24	0	30	0		2	6272	1024	48	976				Excluded
7	1 to 20	24	0	30	0	6272	2	1024	7	1017					Excluded
	21 to 37	24	0	30	0		2	6272	1024	15	1009				Excluded
	38 to 42	24	0	30	0		2	6272	1024	20	1004				Excluded
8	1 to 20	24	0	30	0	6272	SRCMAC	DSTMAC	ETYPE	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT	Excluded
	21 to 37	24	0	30	0		SRCMAC	DSTMAC	ETYPE	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT	Excluded
	38 to 42	24	0	30	0		SRCMAC	DSTMAC	ETYPE	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT	Excluded
9	1 to 20	24	0	30	0	6272	SRCMAC	DSTMAC	ETYPE	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT	Excluded
	21 to 40	24	0	30	0		SRCMAC	DSTMAC	ETYPE	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT	Excluded
	21 to 40	24	0	30	0		18	1024	2	1022	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT
10	1 to 20	24	0	30	0	6272	SRCMAC	DSTMAC	ETYPE	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT	Excluded
	21 to 40	24	0	30	0		SRCMAC	DSTMAC	ETYPE	SRCIP	DSTIP	IPPROTOCOL	SRCPORT	DSTPORT	Excluded

For the PFOS 6000, each 200G port group can support:

- “Range Checker Elements” display the usage of “TCP-UDP Port Ranges”. Maximum is 24 different setting ranges.
- “Custom Offset Elements” display the usage of “User Defined Filter” (UDF).
  - A total of up to 30 UDF bytes may be defined.
  - Each UDF may contain up to 16 bytes.
  - Maximum offset value is 63; match up to the 64th byte from any L2, L3 or L4 header.



- “Filter Pool” displays the maximum filter entries with current running configuration. The maximum capability depends on the complexity of the filter expression:
  - 12,544 filter entries if filters use Group-2 only; without IPv6 (Group-1) or Control Group-10.
  - 10,496 filter entries if filters use Group-2 and Control Group-10; without IPv6 (Group-1).
  - 6,272 filter entries if filters contain IPv6 (Group-1) but no Control Group-10.
  - 3,136 filter entries if filters contain any of the following:
    - IPv6 (Group-1) with Group-2
    - IPv6 (Group-1) with Control Group-10
    - IPv6 (Group-1) with Group-2 and Control Group-10

**Notes:**

- Group-1 is used for IPv6 filter setting only
- Group-2 is used for all non-IPv6 filter settings
- Control Group-10 is for system control packets when either [pfsMesh](#) or [IP Tunnel Termination](#) is enabled. (IP Tunnel Termination is enabled as a default; to disable, see the [Tunnel](#) option on the Global Settings > System>Features page).

## Custom Offset Filters

**Note:** This section provides information about custom offset filters for PFS 6000 Series and PFS 5000/7000 Series, excluding PFS 503x/703x-32X, PFS 5031/7031-56X, 5030/7030-54X and PFS 504x/704x-32D devices. For these devices refer to the following sections:

- [Custom Offset Filters for PFS 503x/703x-32X, PFS 5031/7031-56X, and 5030/7030-54X](#)
- [Custom Offset Filters for PFS 504x/704x-32D](#)

Custom offset filtering (often referred to as user-defined filtering) allows you to create a byte filter window beginning at the start of the MAC, IP, L4 (TCP or UDP) header for comparison with all packets that pass through the filter. The “Header” offset setting can also be applied to MPLS packets; it behaves as shown in the following examples:

UDF Offset Header		5010 or 5100				6010			
Packet Format		L2-IP-L4	L2-MPLS-IP-L4	L2-MPLS-MPLS-IP-L4	L2-IP-GRE or L2-IP-ERSPAN	L2-IP-L4	L2-MPLS-IP-L4	L2-MPLS-MPLS-IP-L4	L2-IP-GRE or L2-IP-ERSPAN
Config	MAC	MAC header	MAC	MAC	MAC header	MAC header	MAC	MAC	MAC header
	IP	IP header	MPLS	1st MPLS	IP header	IP header	MPLS	1st MPLS	IP header
	L4	TCP or UDP header	MPLS	1st MPLS	GRE header	TCP or UDP header	IP Header	IP Header	End of GRE header

The following graphic shows the Custom Offset settings on the Forwarding Filter configuration page.



Include custom offset:

Header:	None	offset:	value:	mask:
---------	------	---------	--------	-------

## Match Filter

You can specify an offset from the beginning of the window and the desired hexadecimal data pattern to be compared to receive packets. Valid values can be a hexadecimal string (1-32 hex characters) or an IPv4 decimal address or an IPv6 hex address. The format of a match filter is:

```
offset decimal-offset hex-pattern or decimalIPv4-pattern or hexIPv6-pattern
```

Refer to the following table for examples:

ip offset 15 02	Matches the single byte pattern 02 against the last byte of the IPv4 source address (15 bytes past the start of the IPv4 header).
14 offset 28 10.20.30.1	Matches the specified IPv4 source address inside a GTP-U header (28 bytes past the start of the UDP header).
14 offset 28 2001:0db8:85a3:0000:0000:8a2e:0370:7334	Matches the specified IPv6 source address inside a GTP-U header (28 bytes past the start of the UDP header).

In PFOS, the maximum offset from the start of the packet is:

- For PFS 6000 Series systems, 63 bytes.
- For PFS 5000/7000 Series systems, 127 bytes.

## Filter Masks

Filter masks allow you to isolate single bits or groups of bits as desired for filtering on partial bytes. A mask is a qualifier for the data pattern entered in bits. This causes the specified value to be logically ANDed with the packet data. The result is compared with the comparison data entered; if this data matches, the filter sees a match. Valid values can be a hexadecimal string (1-32 hex characters) or an IPv4 decimal netmask or an IPv6 hex netmask.

Masking when creating custom offset filters is similar to creating a subnet mask in IP networking. The concept is the same: creating a hexadecimal or decimal value which looks for packets that contain that hexadecimal or decimal string. The difference is that using masking for filter creation allows you to select blocks of addresses rather than identifying specific IP addresses one at a time.

The format of a filter mask is:

```
offset decimal-offset hex-pattern or decimalIPv4-pattern or hexIPv6-  
pattern [ mask hex-mask or decimalIPv4-mask or hexIPv6-mask]
```

Refer to the following table for examples:



ip offset 15 01 mask 01	Matches the value 1 in the low-order bit of the last byte of the IPv4 source address (15 bytes past the start of the IPv4 header).
14 offset 28 10.20.30.0 mask 255.255.255.0	Matches values in the 10.20.30.0/24 network in the IPv4 source address inside a GTP-U header (28 bytes past the start of the UDP header).
14 offset 28 2001:0db8:85a3:0000:0000:0000:0000 mask ffff:ffff:ffff:ffff:0000:0000:0000:0000	Matches values in the 2001:0db8:85a3:0000/64 network in the IPv6 source address inside a GTP-U header (28 bytes past the start of the UDP header).

## Custom Offset Filters for PFS 503x/703x-32X, PFS 5031/7031-56X, and 5030/7030-54X

**Note:** While some MAC and L4 [custom offset filter configurations for other 5000/7000 devices](#) are still valid for PFS 503x/703x-32X, PFS 5031/7031-56X, and 5030/7030-54X devices, NETSCOUT recommends you use the specific Custom Offset Filter configuration components (keywords, offset values, and range of values) described in this section that are only compatible with PFS 503x/703x devices.

Custom offset filtering for PFS 503x/703x devices is different from other PFS devices due to the 503x/703x internal switch design. This design supports more granularity on different packet types such as VxLAN, GRE, etc.; therefore, PFS 503x/703x-32X, PFS 5031/7031-56X, and 5030/7030-54X devices support custom offset filters based on the actual header of the application protocol.

The PFS 503x/703x packet parsing logic determines the abstract packet types; offsets for extraction vary depending on packet type. For example, for MPLS packets, up to five MPLS labels can be parsed for payload, compared to other PFS 5000/7000 devices where offset is based on each label.

PFS 503x/703x devices also reduce the maximum chunks (or bytes) of data that can be parsed per selected application in the custom offset configuration for the incoming packet; these per-packet format limits are described in [PFS 503x/703x Custom Offset Tokens and Offsets](#).

In addition to standard tokens [mac(l2)/ip(l3)/tcp or udp(l4)] used for UDF filters, PFS 503x/703x devices support the following tokens to qualify based on packet types. The [Filter Resource page](#) shows the UDF bytes utilized and maximum bytes available per packet type.

- L2withVlan
- KnownNonIp
- Unknownl3
- IPv4
- IPv6
- MPLSheader
- UnknownL4
- GRE
- GreErspan



## PFS 503x/703x Custom Offset Tokens and Offsets

**Note:** These custom offsets are only supported on PFS 503x/703x platforms. Maps using these offsets cannot be used to send traffic to remote destinations over pStack in a heterogenous environment (that is, a pStack topology having non-503x/703x platforms). If a user wants to send traffic to remote destinations from 503x/703x platforms based on custom offset filters, the user must use pStack+ connections instead of pStack connections.

PFS 503x/703x maintains 16 bits 0xffff to store a maximum of 32 custom offset bytes (as 16 chunks of data where each chunk is 2 bytes). The bits used to program custom offset filters are shared between packet formats. Therefore, it is recommended to configure offsets in order from layer-2, layer-3, layer-4, application specific packet types to utilize 32 bytes. In best case, all 32 custom offset bytes can be utilized as per the recommended order; in worst case, 26 bytes can be utilized.

The recommended order is shown in the following table.

Config Order	Token	Start Offset	Offset and Value	Example
1	L2	Start of first byte of L2 header	Offset: 0-62 (decimal) Maximum of 4 bytes	"l2 offset 12 0x88a8" is used to qualify on outer TPID value from start of the packet.
2	L2withvlan	Single Outer Tag/Inner Tag (SOT/IT) packets: 14 bytes from Start of L2 header. Double Tag (DT) packets: 18 bytes from Start of L2 header.	Offset: 0-126 (decimal) Maximum of 16 bytes	"l2withvlan offset 0 64" is used to qualify on outervlan =100 for SOT/IT packets and Innervlan=100 for DT packets
3	UnknownL3	Start of inner header's first byte after unknown Ethertype. Valid only for unknown L3 protocols ETHERTYPE != ( IPv4   IPv6   MiM   ARP   RARP   MPLS   FCoE   Pause   1588   NSH )	Offset: 0-108 (decimal) Maximum of 28 bytes	"unknownl3 offset 16 10.1.2.3" is used to qualify on SrcIP for double tagged packet with inner tpid 88a8/9100. VNTag also needs to use "UnknownL3" and adjust offset from "Eth Type" "unknownl3 offset 18 10.1.2.3" is used to qualify on SrcIP for VNTag (eth type 8926)
4	MPLSheader	Start of first byte of L3/data after MPLS header. Supports filtering of L3/data for packets encapsulated in up to five MPLS labels.	Offset: 0-102 (decimal) Maximum of 16 bytes	"mplsheader offset 12 10.1.2.3" is used to qualify on SrcIP of IPv4 header encapsulated in 1-5 MPLS labels.



Config Order	Token	Start Offset	Offset and Value	Example
5	IPv6	Start of first byte of L3 header for IPv6.	Offset: 0-108 (decimal) Maximum of 14 bytes	"ipv6 offset 56 20.1.2.3" is used to qualify on DstIp of Inner IPv4 header
6	IPv4	Start of first byte of L3 header for IPv4.	Offset: 0-108 (decimal) Maximum of 16 bytes	"ipv4 offset 32 10.1.2.3" is used to qualify on SrcIP of Inner IPv4 header
7	KnownNonIp	Start of first byte after Known non-ip EtherType (other than Known IPv4/6 and FCoE/Mim/MPLS tunnels).	Offset: 0-108 (decimal) Maximum of 28 bytes	"knownnonip offset 14 10.1.2.3" is used to qualify on ARP packet sender ip address.
8	UnknownL4	Start of first byte of unknown L4 header. Valid when PROTOCOL != ( TCP   UDP   IP_EXTN_HDR   GRE   SCTP )	Offset: 0-102 (decimal) Maximum of 22 bytes	"unknownl4 offset 4 00112233" is used to qualify on custom packet L4 header.
9	GRE	Start of first byte of payload <i>after</i> GRE header.	Offset: 0-102 (decimal) Maximum of 16 bytes	"gre offset 26 10.1.2.3" is used to qualify on SrcIP of L2IPv4 payload encapsulated in a GRE packet.
10	GreErspan	Offset starts from first byte of GRE header in packet.	Offset: 0-102 (decimal) Maximum of 16 bytes	"GreErspan offset 42 10.1.2.3" is used to qualify on SrcIP of payload encapsulated in a GRE ERSPAN packet (or other GRE packet not matched by the GRE token above) with GREERSPAN protocol header size 16 bytes.
11	L4	Start of first byte of L4 header. Valid only for TCP/UDP packets.	Offset: 0-126 (decimal) Maximum of 16 bytes	"l4 offset 20 30" is used to qualify on GTP protocol type present in TCP packet. "l4 offset 14 64" is used to qualify on VNID present in VxLAN packet.

## PFS 503x/703x Custom Offset Error Handling

The following table describes the error messages PFOS may encounter when processing PFS 503x/703x custom offsets.



Error String	Purpose
MaxUserDefinedFilterLimitReached	UDF bytes allocated count reached the max limit per system.
PktFmtMaxUserDefinedFilterLimitReached	UDF bytes allocated count reached the max limit per packet format type.
UserDefinedFilterInvalid	Error during allocation of UDF: <ul style="list-style-type: none"><li>• UDF create error</li><li>• UDF chunk bitmap allocation failure due to conflict with unavailable chunk bitmap</li><li>• UDF chunk requested exceeds the maximum available chunks per packet format.</li></ul>
Input offset : 110 exceeds max_offset 102 supported for packet	When the start offset for a specific token/packet type exceeds the maximum offset limit.

Once the map is configured using a filter with custom offset configurations, you can verify the map status using the `show map map_status` command to check whether the filter installation is successful or not:

```
PFS7031-56X# show map map_status
Map
Name STATE INGRESS ERROR CODE MGID
-----
m1 enable 1-53 None 0
map2 enable 1-33 UserDefinedFilterInvalid 0
```

## Custom Offset Filters for PFS 504x/704x-32D

PFS 5040/7040-32D and 5041/7041-32D devices have similar Custom Offset Filter configurations as the [Custom Offset Filters for PFS 503x/703x-32X, PFS 5031/7031-56X, and 5030/7030-54X](#), although some differences exist. The PFS 504x/704x do not support the *KnownNonIP* token; the remaining differences are listed in [PFS 504x/704x Custom Offset Tokens and Offsets](#).

You can view the UDF bytes utilized and maximum bytes available per packet type on the [5040/7040-32D Filter Resources page](#) and the [5041/7041-32D Filter Resources page](#).

### PFS 504x/704x Custom Offset Tokens and Offsets

**Note:** These custom offsets are only supported on PFS 504x/704x platforms. Maps using these offsets cannot be used to send traffic to remote destinations except L4 UDF filters over pStack in a heterogenous environment (that is, a pStack topology having non-504x/704x platforms).

PFS 504x/704x support 1-byte and 2-byte chunks, with a system wide limitation of 7 2-byte chunks and 5 1-byte chunks with a total of 19 bytes of UDF support.

The recommended order is shown in the following table.



Config Order	Token	Start Offset 504x/704x	Example	Offset and Value	Comments
1	L2	Start of first byte of L2 Ethertype	"l2 offset 0 0800" is used to qualify on outer TPID value from start of Ethertype	Offset: 0-63 (decimal) Maximum of 8 bytes	Start Offset: Same as 503x/703x.  Offset and Value: L2 also takes resources from both UnknownL3 and IPv6 UDF tokens.
2	L2withvlan	Single Outer Tag/Inner Tag packets: 12 bytes from Start of L2 header  Double Tag packets: 16 bytes from Start of L2 header	"l2withvlan offset 2 0064" is used to qualify on outer vlan =100 for SOT/IT packets and Innervlan=100 for DT packets	Offset: 0-126 (decimal) Maximum of 16 bytes	Start Offset: See <a href="#">503x/703x</a> <a href="#">L2withvlan</a> for differences.
3	UnknownL3	Start of inner header's first byte after unknown Ethertype. Valid only for unknown L3 protocols ETHERTYPE != ( IPv4   IPv6   MiM   ARP   RARP   MPLS   FCoE   Pause   1588   NSH )	"unknownl3 offset 16 10.1.2.3" is used to qualify on SrcIP for double tagged packet with inner tpid 88a8/9100.	Offset: 0-108 (decimal) Maximum of 18 bytes	Start Offset: Same as 503x/703x.  Offset and Value: UnknownL3 also takes resources from L2 UDF token.
4	IPv4	Start of first byte of L3 header for IPv4.	"ipv4 offset 32 10.1.2.3" is used to qualify on SrcIP of Inner IPv4 header	Offset: 0-108 (decimal) Maximum of 19 bytes	Start Offset: Same as 503x/703x.
5	IPv6	Start of first byte of L3 header for IPv6.	"ipv6 offset 56 20.1.2.3" is used to qualify on DstIp of Inner IPv4 header	Offset: 0-108 (decimal) Maximum of 8 bytes	Start Offset: Same as 503x/703x.  Offset and Value: IPv6 also takes resources from L2 UDF token.



Config Order	Token	Start Offset 504x/704x	Example	Offset and Value	Comments
6	MPLSheader	Start of first byte of L3/data after MPLS header. Supports filtering of L3/data for packets encapsulated in up to four MPLS labels.	"mplsheader offset 12 10.1.2.3" is used to qualify on SrcIP of IPv4 header encapsulated in 1-4 MPLS labels"	Offset: 0-102 (decimal) Maximum of 8 bytes	Start Offset: Same as 503x/703x.
7	UnknownL4	Start of first byte of unknown L4 header. Valid when PROTOCOL != (TCP   UDP   IP_EXTN_HDR   GRE   SCTP)	"unknownl4 offset 4 00112233" is used to qualify on custom packet L4 header.	Offset: 0-102 (decimal) Maximum of 19 bytes	Start Offset: Same as 503x/703x.
8	GRE	Start of first byte of GRE header.	"gre offset 30 10.1.2.3" is used to qualify on SrcIP of L2IPv4 payload encapsulated in a GRE packet.	Offset: 0-102 (decimal) Maximum of 19 bytes	Start Offset: See <a href="#">503x/703x GRE</a> for differences.
9	L4	Start of first byte of L4 header. Valid only for TCP/UDP packets.	"l4 offset 20 30" is used to qualify on GTP protocol type present in TCP packet. "l4 offset 14 64" is used to qualify on VNID present in VxLAN packet.	Offset: 0-127 (decimal) Maximum of 19 bytes	Start Offset: Same as 503x/703x.

## Filtering on Packets with Multiple VLAN Tags

PFS 6000 series and PFS 5000/7000 series have different VLAN/Layer-3/Layer-4 filter capability based on the following factors:

- Number of VLAN tags and TPID of user data packets
- System TPID
- Destination Type
  - [Local Destination](#)
  - [Remote Destination over pfsMesh](#)
  - [Inline Tool Chains](#)

**Note:** PFS platforms DO NOT support VLAN, Layer-2, or Layer-3 filtering on packets with more than two VLAN tags.



## Local Destination

The table below displays if VLAN or Layer-3/Layer-4 filter settings are supported for packets with single or double VLAN tags arriving at local PFS 6000 and PFS 5000/7000 platforms. Note for PFS 6000s, the support varies per system TPID setting; for PFS 5000/7000s, the support is consistent per system TPID setting.

		PFS 6000 Series Capability with Different System TPIDs			PFS 5000/7000 Series Capability with Different System TPIDs		
Ingress Packets VLAN TPID		8100	9100	88A8	8100	9100	88A8
<b>Single VLAN TPIDs</b>	8100+IP	OK	OK	OK	OK	OK	OK
	9100+IP		OK		OK	OK	OK
	88A8+IP			OK	OK	OK	OK
<b>Double VLAN TPIDs</b>	8100+8100+IP	OK	OK	OK	OK	OK	OK
	8100+9100+IP		OK				
	8100+88A8+IP			OK			
<b>Double VLAN TPIDs</b>	9100+8100+IP		OK		OK	OK	OK
	9100+9100+IP		OK				
	9100+88A8+IP						
<b>Double VLAN TPIDs</b>	88A8+8100+IP			OK	OK	OK	OK
	88A8+9100+IP						
	88A8+88A8+IP			OK			

## Remote Destination over pfsMesh

**Note:** Packets forwarded over pfsMesh with pStack+ connections are based on tunnels, so these filtering limitations do not apply. Refer to [pfsMesh Using pStack+](#) for details.

Packets forwarded over pfsMesh using a pStack connection have an extra VLAN tag added so the next Node can segregate flows received from different sources. Therefore, user data packets without a VLAN tag become packets with one VLAN tag over pfsMesh, and user data packets with one VLAN tag become packets with double VLAN tags over pfsMesh. These scenarios have the following possible limitations:

- User data packets with double VLAN tags cannot be configured with VLAN or Layer-3/Layer-4 filters in traffic maps to remote destination over pfsMesh with pStack connections; it is recommended users configure nonmatch or unfiltered maps to remote nodes.
- User data packets with a single VLAN tag can be configured with VLAN or Layer-3/Layer-4 filters in traffic maps to remote destination only if system TPID and user's VLAN TPID match those in the following table.



	<b>PFS 6000 is Transit or Destination Node with System TPID of:</b>			<b>PFS 5000 or 7000 over pStack is Transit or Destination Node with System TPID of:</b>		
<b>User Packets VLAN TPID</b>	<b>8100</b>	<b>9100</b>	<b>88A8</b>	<b>8100</b>	<b>9100</b>	<b>88A8</b>
No VLAN	OK	OK	OK	OK	OK	OK
8100+IP	OK	OK	OK	OK	OK	OK
9100+IP	X	OK	X	X	X	X
88A8+IP	X	X	OK	X	X	X

**Notes:**

- PFOS does not support VLAN or Layer-3/Layer-4 filtering in traffic maps over pStack for user packets with more than two VLAN tags; it is recommended users configure nonmatch or unfiltered maps to remote nodes.
- All nodes in a pfsMesh must be configured to use the same System TPID.

For packets to reach a remote destination, ensure *each* transit node *and* the destination node support the user data packet VLAN TPID. For example, consider the following traffic map configuration:

- Filtering:** Layer-3/Layer-4 filter to forward packets over pfsMesh
- Transit Node:** PFS 5000
- Destination Node:** PFS 6000
- User Data Packets:** VLAN TPID 9100

When the VLAN TPID 9100 tagged packets are forwarded to the PFS 5000 transit node, Layer-3/Layer-4 filtering is not supported (see table) even though the PFS 6000 destination node can support TPID 9100. In this configuration, only VLAN TPID 8100 tagged packets can be filtered and delivered to remote destinations.

## Inline Tool Chains

Inline Network port groups have a configurable option for VLAN tag enable/disable. By default VLAN tagging is enabled at all inline network port groups. This VLAN tag helps tool chains segregate the flows. If VLAN tagging is enabled, all packets entering inline toolchains carry one extra VLAN tag so the system can determine traffic destination when exiting tools.

Therefore, user data packets without a VLAN tag become packets with one VLAN tag over inline tool chain, and user data packets with one VLAN tag become packets with double VLAN tags over inline tool chain. These scenarios have the following possible limitations:

- User data packets with double VLAN tags cannot be configured with VLAN or Layer-3/Layer-4 filters in inline tool chain.
- User data packets with a single VLAN tag can be configured with VLAN or Layer-3/Layer-4 filters in inline tool chain only if system TPID and user's VLAN TPID match those in the following table.



	PFS 6000s with System TPID of:			PFS 7000s with System TPID of:		
User Packets VLAN TPID	8100	9100	88A8	8100	9100	88A8
No VLAN	OK	OK	OK	OK	OK	OK
8100+IP	OK	OK	OK	OK	OK	OK
9100+IP	X	OK	X	X	X	X
88A8+IP	X	X	OK	X	X	X

The VLAN Tag setting can be disabled to avoid adding an extra VLAN tag to traffic forwarded to tools. If disabling VLAN tagging, users can configure additional filter settings at exit tools to specify the destination inline network port. Refer to [Inline Traffic](#) for more details.

## Traffic Load Balancing

The session-based, flow-aware load balancing feature distributes traffic across multiple output ports or tunnels. You can configure output ports or tunnels to output traffic as a single load balance group, with their output approximately evenly distributed throughout the group. The network traffic can be spread in real time across multiple output ports or tunnels. Up to 128 Load Balance Groups can be created per PFS.

Output from a load balance group maintains packet order (first in, first out) within a given conversation or flow (any single data stream between point A and point B) and guarantees a consistent output port or tunnel, so a packet sniffer or other monitoring tool sees all packets in each single flow. PFOS utilizes [Load Balance Criteria](#) to distribute different flows to different ports/tunnels within the group, effectively balancing the traffic across all ports/tunnels of the group.

Consider the following when planning your load balancing strategy:

- Load is distributed based on dividing the filtered or unfiltered traffic into 64 buckets (non-weighted distribution), regardless of how many output ports are in the monitor group. This means that load balance groups of up to 64 ports can be defined.
- There is no certainty that traffic from different source addresses or sessions will have the same or equivalent volumes. Therefore, in situations where the volume of traffic is not even across sources or sessions, the load distribution is unlikely to be evenly divided across the output ports.

Extended load balancing capabilities are available on PFS 6000 systems with one or more advanced line cards. For more information, refer to [Extended Load Balancing](#).

PFOS also supports a PFS+PFX solution that enables load balancing based on Inner VLAN tag; refer to [PFS+PFX Inner Filtering and Inner Load Balancing](#) for details.



## Load Balance Criteria

PFOS provides pre-defined load balance criteria which you can view on the Load Balance Criteria page.

Load Balance Criteria					
^ Load Balance Criteria					
Name	Source Port	Layer 2	MPLS	Layer 3	Layer 4
ELB	exclude	disable	enable	enable	enable
IP_Dest	exclude	enable	enable	enable	enable
IP_Dest_Src	exclude	enable	enable	enable	enable
IP_Dest_Src_and_L4_Dest_Src	exclude	enable	enable	enable	enable
IP_Dest_and_L4_Dest	exclude	enable	enable	enable	enable
IP_Src	exclude	enable	enable	enable	enable
IP_Src_and_L4_Src	exclude	enable	enable	enable	enable
MAC_Dest_Etype_Port	include	enable	enable	enable	enable
MAC_Dest_Src_Etype_Port	include	enable	enable	enable	enable
MAC_Src_Etype_Port	include	enable	enable	enable	enable
PFX	exclude	enable	enable	enable	enable

Showing 1 to 11 of 11

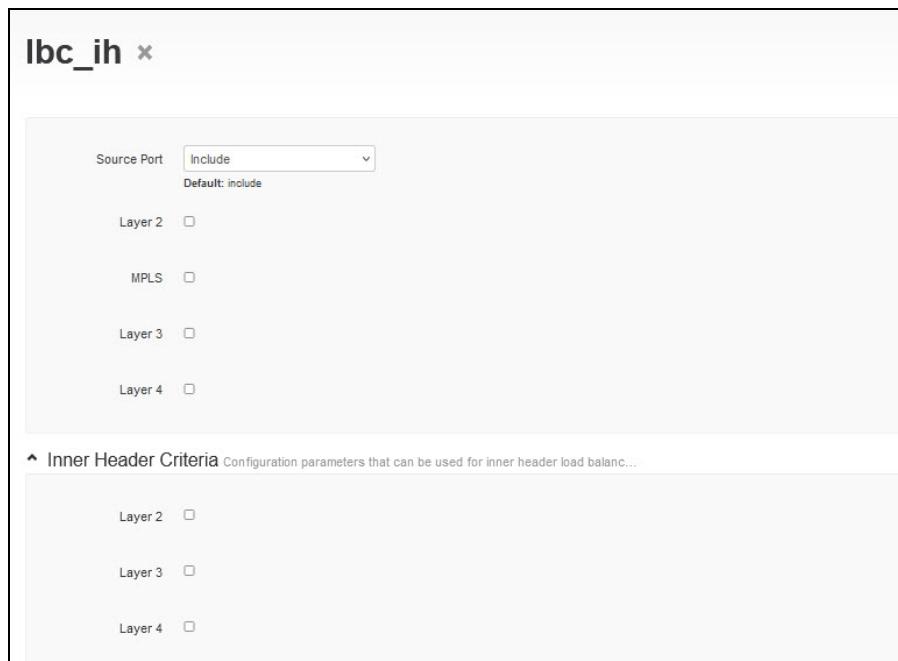
Users can also [define their own criteria](#) by selecting the specific criteria to be used in traffic maps. The following graphics are example Load Balancing Criteria configuration settings. Supported settings vary per PFS model; refer to [Load Balance Criteria](#).

LBC1 \*

Source Port	<input type="button" value="Include"/>	Default: include Select 'include' option to have the best load...
Layer 2	<input checked="" type="checkbox"/>	Layer 2 Header Keys <input type="checkbox"/> Destination MAC Address <input type="checkbox"/> Source MAC Address <input type="checkbox"/> Ethertype
MPLS	<input checked="" type="checkbox"/>	Mpls Header Keys <input type="checkbox"/> Label 1 <input type="checkbox"/> Label 2 <input type="checkbox"/> Label 3
Layer 3	<input checked="" type="checkbox"/>	Layer 3 Header Keys <input type="checkbox"/> Destination IP Address <input type="checkbox"/> Source IP Address <input type="checkbox"/> IP Protocol
Layer 4	<input checked="" type="checkbox"/>	Layer 4 Header Keys <input type="checkbox"/> Destination Port <input type="checkbox"/> Source Port

▲ Custom Criteria Configuration parameters that can be used for custom-hash feature

Type	<input type="button" value="uint16"/>	Packet layer field to use for custom-hash algo...	Offset	<input type="button" value="uint16"/>	Valid values: 0—127	Length	<input type="button" value="uint16"/>	Valid values: 1—4	Length in bytes from the base of configured pa...
------	---------------------------------------	---	--------	---------------------------------------	---------------------	--------	---------------------------------------	-------------------	---



PFOS determines flow association by examining selected fields within each packet and applying a [hashing algorithm](#) to consistently separate and distribute traffic to specific ports or tunnels.

Selected headers (Layer 2, MPLS, 3 and 4) and inner headers (Layer 2, 3, and 4) and their associated elements (Load Balance Criteria) determine which header information will be used for traffic maps that have that load balance group as an output.

Additionally, PFOS provides Custom Criteria parameters as part of load balance criteria configuration. Custom Criteria load balancing provides hash-based traffic distribution based on any 1- to 4-byte value in the first 127 bytes of the packet data. For example, to load-balance traffic based on TEID values in GTP-U traffic, the custom hash feature can be configured to point to the TEID field of the GTP-U packets.

**Note:** PFS devices only support one Load Balance Criteria configured with custom-criteria per device.

Refer to [Load Balancing Considerations](#) for configuration limitations and considerations for Load Balance Criteria.

## Load Balance Groups and Failover Actions

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. When a port or tunnel in a load balancing group goes down or becomes unavailable, one of these failover actions can be taken:

- **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 member – traffic is not rebalanced or redistributed.  
**Note: The Drop failover action is not supported for load-balanced tunnels.**
- **Round Robin** - 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. Note the following for Round Robin load balancing criteria:
  - Round Robin is not based on a hash algorithm so it is not an option under Load Balance Criteria. Round Robin is an option under Failover Action when creating a load balance group. Once a load balance group is configured with Round Robin as the Failover Action, PFOS evenly distributes traffic using the round robin method to each LBG member during normal operation and if a failover occurs. In addition, when a load balance group with Round Robin is configured in a traffic map, the load balance criteria used in the map has no impact on traffic distribution.
  - Round Robin is not supported for PFS 5010/7010, PFS 504x-32D/704x-32D, PFS 6010, and PFS 6002 devices.
  - Round Robin is not supported for load-balanced tunnels.
  - Because PFOS performs Round Robin traffic distribution on a per-packet basis, it should only be configured when in network scenarios having homogeneous tools/servers/links receiving the traffic where packet order is not an issue.
  - Because Round Robin traffic distribution is not flow-specific, there is potential for out-of-order packets or multiple copies of the same packet at the receiving system if they are transmitted in different paths.
  - A traffic map can only have one Round Robin LBG as Egress. That is, Round Robin will not work if additional Egress ports, Monitor port groups, Remote Monitor port groups, or additional LBGs are configured, including if a traffic map using a Round Robin LBG is merged with another map.
- **Weighted Redistribute** - redistribute the traffic to remaining load balance weighted ports, without disturbing the traffic. See [Load Balance Weighted Calculation](#) for details.

**Note: The Weighted Redistribute failover action is only available for load-balanced ports, it is not supported for load-balanced tunnels. It is not applicable for PFS 6000s.**

Examples of using Weighted Redistribute load balance to manage port distribution include:

- Handling various port speed distribution imbalance by assigning more weight to higher speed ports and lower weight to low speed ports.
- Prioritizing a specific port over other ports.

## About Load Balancing and Filtering

PFOS distinguishes between load balancing and filtering as separate yet complementary processes that can be applied independently or together as needed, depending on the monitoring application. With load balancing and filtering both applied, traffic is evenly distributed from selected filtered criteria across the load balance group.



## Load Balance Weighted Calculation

**Weighted Load Balance is only available for load-balanced ports, it is not supported for load-balanced tunnels. It is not applicable for PFS 6000s.**

Users configure weight values per port, which PFOS uses to calculate the percentage of traffic each port should receive.

$$\text{Port Percentage (Pi)} = (\text{Wi} / \Sigma(\text{W})) * 100$$

**Wi** is the user-defined weight

**$\Sigma\text{W}$**  is the sum of all the port weights in the group.

For example, a user configures a group with ports and weights:

Port	Weight
1-1	20
1-2	30
1-3	0

Using the calculation for each weighted port we find the percentage traffic for each port:

**Port 1-1:**  $(20 / (20+30)) * 100 = 40\%$

**Port 1-2:**  $(30 / (20+30)) * 100 = 60\%$

**Port 1-3:**  $(0 / (20+30)) * 100 = 0\%$

## Load Balancing Workflow

Follow this process to set up load balancing. After completing these tasks, load balancing is applied automatically. Refer to [Load Balancing Considerations](#) for configuration limitations and considerations for Load Balance Criteria.

1. [Define Load Balance Criteria](#)
2. [Create Load Balance Groups with Ports](#) or [Create Load Balance Groups with Tunnels](#). **(The Load Balance Tunnel feature requires the PFS 7000 functionality license)**  
**(Note:** Ports and tunnels cannot be in same load balance group).
3. [Define a traffic map that has a load balance group as the output](#).

### Define Load Balance Criteria

As part of load balancing configuration, users select specific [load balance criteria](#) to [configure traffic maps](#). Users can select from pre-defined or user-defined Load Balance Criteria. Perform the following steps to define custom load balance criteria. Refer to [Load Balancing Considerations](#) for configuration limitations and considerations for Load Balance Criteria.

1. From the Load Balance Criteria page, click **Add**.
2. In the Name field, enter a name to identify the new entry.
3. Click **Add** to create the entry and display the settings.



## LBC1 ×

Source Port  Default: include  
Select 'include' option to have the best load-...

Layer 2  Layer 2 Header Keys  Destination MAC Address  Source MAC Address  Ethertype

MPLS  Mpls Header Keys  Label 1  Label 2  Label 3

Layer 3  Layer 3 Header Keys  Destination IP Address  Source IP Address  IP Protocol

Layer 4  Layer 4 Header Keys  Destination Port  Source Port

4. Select from the Source Port menu to 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.
5. Select the header levels (Layer 2, MPLS, Layer 3, or Layer 4) for each of the criteria you want to include. Base your selections on the headers that are best suited for even traffic distribution in your network. When you select a layer, you must also select at least one header key from the list that displays to the right of the layer. These are used in the [hashing algorithm](#) and are the same for all traffic maps you define for which you select this load balance criteria.

**Note:** If Layer 4 criteria are used for standard load balancing on a PFS 6000 Series system, then packets are balanced, but sessions are *not* maintained. For a workaround, use Layer 3 criteria instead.

6. **PFS 7040-32D and 7041-32D Only:** In addition to selecting outer headers as load balance criteria, you can select the Inner Header levels (Layer 2, Layer 3, or Layer 4) as load balance criteria for L2GRE, L3GRE, L3 MPLS, and VXLAN packets. Base your selections on the headers that are best suited for even traffic distribution in your network. When you select a layer, you must also select at least one header key from the list that displays to the right of the layer. These are used in the [hashing algorithm](#) and are the same for all traffic maps you define for which you select this load balance criteria.

**Note:** Inner header criteria configuration is only supported for L2GRE, L3GRE, L3 MPLS, and VXLAN packets; existing load balance criteria is not affected.

Inner Header Criteria Configuration parameters that can be used for inner header load balanc...

Layer 2  Layer 2 Header Keys  Destination MAC Address  Source MAC Address  Ethertype

Layer 3  Layer 3 Header Keys  Destination IP Address  Source IP Address  IP Protocol

Layer 4  Layer 4 Header Keys  Destination Port  Source Port



7. If configuring a custom hash, define the following Custom Criteria (this feature has limited support; refer to [Load Balancing with Custom Hash](#)).

- **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).

Type	Offset	Length
Packet layer field to use for custom-hash algo...	uint16 Valid values: 0—127 Offset in bytes from the base of configured pa...	uint16 Valid values: 1—4 Length in bytes from the configured offset to ...

8. Click **Apply**. To add additional entries, click **New Load Balance Criteria** in the upper right corner of the page.

## Create Load Balance Groups with Ports

You can configure up to 64 output ports to output traffic as a single load balance group, with their output approximately evenly distributed throughout the group. The network traffic can be spread in real time across multiple output ports (such as 10G to 1G).

1. From the Load Balance Groups page, click **Add**.
2. In the Name field, enter a name to identify the new entry.
3. Click **Add** to create a new group and display the settings.
4. Add text to describe the group in the **Description** field.



Ibg2 × Load balancing groups

New Load Balance Group...

Basics References Ref Trigger

Description string  
1 characters or more.

Failover Action Rebalance the load among active members - traffic will be disturbed ▾  
Default: Rebalance  
Failover action when any port in LBG goes offline

Type Monitor ▾  
Default: Monitor  
Load-balance group type

Ports/Tunnels **configure** Selected Ports/Tunnels:  
Ports selection

Pfx  Enable/Disable PFX Mode in LBG

Error Code None  
Default: None

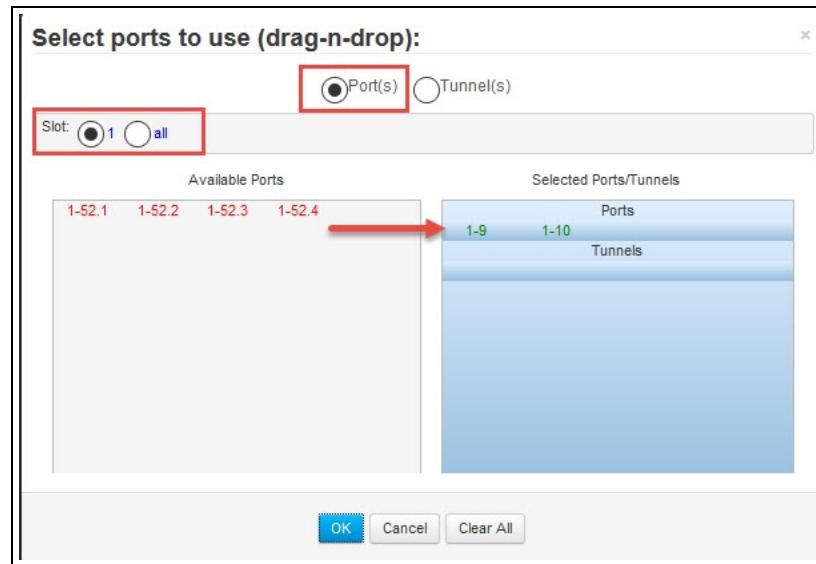
Oper Status Down  
Default: Down

▲ Port Status

Port	Error Code	Oper Status
Table is empty		

**Note:** The "Pfx" option is used in PFS/PFX inner load balancing configurations. When enabled, distribution of traffic is based on VLAN tags added by PFX appliance. Refer to [PFS+PFX Inner Filtering and Inner Load Balancing](#) for details.

- From the Failover Action pull-down list, select the [Load Balance Groups and Failover Actions](#) for the system to take if a member of the group is unavailable. By default, the type is set to Monitor, which is the only port class supported for load balancing.  
**Note:** If the load balance group will be used in a map with a custom hash load balance criteria, Rebalance failover is recommended.
- Click **configure** to open the port/tunnel selection dialog box. Select the **Ports** radio button to display the available ports.



7. Select the appropriate Slot and drag the desired ports from the Available Ports area to the Selected Ports area. Select additional slots and ports as needed.



8. If you selected the Weighted distribution option as the Failover Action, perform the following to configure weights for the ports in the group:
  - a. Select the **Port Weight** option at the top of the page (this option only appears if Failover Action is set to Weighted distribution). See [Load Balance Weighted Calculation](#) for details.

Igb2 \*

Basics Port Weight References Ref Trigger

Description string  
1 characters or more.

Failover Action Weighted redistribute ▾  
Default: Rebalance  
Failover action when any port in LBG goes offline

- b. Click **Add** to display the Add a New Port Weight page. Select a port and click **Add**.

Add new Port Weight Weights per port

▲ Add new Port Weight

Port ▾  
1-9  
1-10

Add Cancel

- c. Define a weight for this port. Configure additional port weights as needed.

1-9 \*

Weight \* uint16  
Valid values: 0—100  
Weight of the specific port in the group

9. Click **Apply** to save the load balance group configuration.
10. [Define a traffic map that has a load balance group as the output.](#)

## Create Load Balance Groups with Tunnels

**Note:** This feature requires the PFS 7000 functionality license.

You can configure up to 64 output tunnels to output traffic as a single load balance group, with their output approximately evenly distributed throughout the group. The network traffic can be spread in real time across multiple tunnels.



1. From the Load Balance Groups page, click **Add**.
2. In the Name field, enter a name to identify the new entry.
3. Click **Add** to create a new group and display the settings.
4. Add text to describe the group in the **Description** field.

Ibg2 × Load balancing groups

New Load Balance Group...

Basics References Ref Trigger

Description string  
1 characters or more.

Failover Action Rebalance the load among active members - traffic will be disturbed  
Default: Rebalance  
Failover action when any port in LBG goes offline

Type Monitor  
Default: Monitor  
Load-balance group type

Ports/Tunnels configure Selected Ports/Tunnels:  
Ports selection

Pfx  Enable/Disable PFX Mode in LBG

Error Code None  
Default: None

Oper Status Down  
Default: Down

▲ Port Status

Port	Error Code	Oper Status
Table is empty		

**Note:** The "Pfx" option is used in PFS/PFX inner load balancing configurations. When enabled, distribution of traffic is based on VLAN tags added by PFX appliance. Refer to [PFS+PFX Inner Filtering and Inner Load Balancing](#) for details.

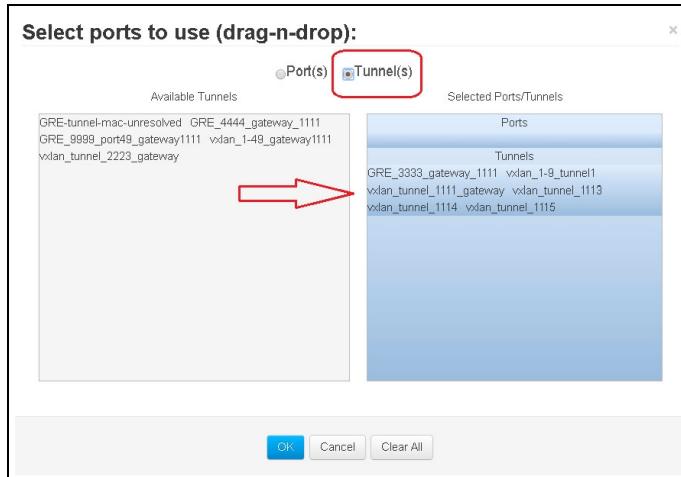


5. From the Failover Action pull-down list, select the [failover action](#) for the system to take if a member of the group is unavailable. By default, the Type is set to Monitor, which is the only port class supported for load balancing.

**Notes:**

- Weighted Load Balance is not supported for load-balanced tunnels.
- If the load balance group will be used in a map with a custom hash load balance criteria, Rebalance failover is recommended.

6. Click **configure** to open the port/tunnel selection dialog box. Select the
7. Select the **Tunnels** radio button to display the available tunnels. A Load Balance Group can contain both L2GRE and VXLAN tunnels combined in one group.



8. Click **OK** to save your selections and return to the Load Balance Groups page.
9. Click **Apply** to save the load balance group configuration.
10. Define a [traffic map](#) that has a load balance group as the output. When adding a tunnel load balance group as a map's output, the following limitations apply:
  - No other output ports are supported
  - No port load balance groups are supported
  - Only one tunnel load balance group is supported

## Delete Load Balance Groups

1. From the Load Balance Groups page, click on the line containing the load balance group that you want to delete. The line is highlighted with a gray background.
2. If you want to delete additional load balance groups, control-click on the lines containing those load balance groups, or shift-click to select a range of lines. Each line you select is highlighted with a gray background.
3. Click **Delete**.
4. A confirmation prompt displays. Click **Yes** to confirm the deletion of all selected load balance groups, or click **No** to cancel the deletion.



## Load Balancing Considerations

Load balancing has the following limitations:

- A port can only be in one Load Balance Group at a time.
- A Load Balance Group can contain up to 64 ports.
- Up to 128 Load Balance Groups can be created per PFS.

Refer to the following sections for more information:

- [Load Balance Criteria](#)
- [Load Balancing with Span-Monitor Ports](#)
- [Load Balancing with Custom Hash](#)
- [Load Balance Groups used as Mirror Session Destinations](#)

### Load Balance Criteria

- For each layer (2, MPLS, 3, or 4) in the Load Balance Criteria, only one criterion per layer can be applied per device (on the PFS 5000/7000 series) or [200G port group](#) (on the PFS 6000 series).
- All ports within the same device (on the PFS 5000/7000 series) or 200G port group (on the PFS 6000 series) that are feeding load-balance groups must use the same criterion for each layer.
- PFS 5000/7000 series ports that are used in a Load Balance Group (LBG) cannot be used as the output port in another traffic map; traffic from such a traffic map will be partially forwarded to the output port depending on the LBG hash result. See [Hash Algorithm](#) for details about available hash algorithm options you can choose for load balancing.
- Load balancing can include values of 1 to 3 MPLS labels; for 5040/7040-32D and 5041/7041-32D, values of 1 to 7 labels are supported. If MPLS label values are included in the load balancing criteria then Layer 3 (but not Layer 4) criteria can be applied to MPLS-L3 packets; Layer 3 and Layer 4 criteria will not apply to MPLS-L2 packets.
- If MPLS criteria are selected, packets without MPLS labels will be load balanced based on any other criteria that are selected; if no other criteria are selected then packets that do not have MPLS labels will be sent to just one of the load balance destinations.
- On PFS 5000/7000 series if L2 criteria are combined with criteria from other layers (for example Layer 3 and Layer 4) the Layer 2 criteria will not contribute to the load balancing.
- The PFS 7040-32D and 7041-32D devices support additional inner header [Load Balance Criteria](#) for L2GRE, L3GRE, L3 MPLS, and VXLAN packets. Inner header criteria configuration is only supported for L2GRE, L3GRE, L3 MPLS, and VXLAN packets; existing load balance criteria is not affected.

### Load Balancing with Span-Monitor Ports

Span-Monitor ports can be included in a load balance group. Span-Monitor ports configured in a load balance group will only transmit packets. But if the same Span-Monitor port is configured at the ingress end of a traffic map, it can receive packets.



You cannot change the class of a port that is part of a load balance group if the new settings would conflict with the current ones. For example, if port 1-1 is configured as a Span-Monitor and is part of the Ports group, then you cannot change it to Span class because it would become an input port. However, you could change that port to Monitor class because it would still be an output port.

## Load Balancing with Custom Hash

- The PFS 503x/703x-32X, PFS 5031/7031-56X devices, and PFS 5040/7040-32D and 5041/7041-32D devices do not support Custom Hash for Load Balancing.
- When PFS is rebooted after a [Custom Hash feature](#) setting change from Disable to Enable, verify the following in case traffic map with custom-offset filter fails:
  - Verify traffic map installation status
  - Modify custom-offset filter configuration
- When configuring custom-criteria for load balance criteria, users must also enable additional configuration based on type of application intended for traffic distribution. For example in the case of GRE traffic, VxLAN traffic, or IP-in-IP traffic, the "IP Protocol" in Layer 3 load balance criteria must also be enabled. For MPLS traffic, "Ethertype" in Layer 2 load balance criteria must also be enabled. If the application is only VxLAN then enable the Layer 4 fields.
- The PFS 5010/7010 device does not support the custom-hash feature for GRE and VxLAN traffic.
- PFS devices only support one Load Balance Criteria configured with custom criteria per device.
- When an odd offset value is defined for the custom hash, then traffic distribution with a hash length of 1 may not work properly.
- For **pStack** maps, when using Load Balancing Criteria, Custom Criteria with Type = L2 in remote monitor port group, use one of the following configurations to avoid traffic distribution issues:
  - On remote node with custom criteria type = L2, set the offset value as X + 4, where X is the offset set at the head node where the map was created.
  - Create a Service port at the destination Node with Source Port VLAN tagging disabled. Use the Service port as the destination of the pStack map. Then create an unfiltered map from the Service port to the Load Balance Group with the Custom Offset Load Balance Criteria.
- For **pStack+** maps, when using Load Balancing Criteria, Custom Criteria with Type = L2/L3/L4 in remote monitor port group, use the following configurations to avoid traffic distribution issues:
  - Create a Service port at the destination Node with Source Port VLAN tagging disabled. Use the Service port as the destination of the pStack+ map. Then create an unfiltered map from the Service port to the Load Balance Group with the Custom Offset Load Balance Criteria.



## Trigger Policies

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
- Send notifications based on events
- Automatically place the network access into a failsafe state based on trigger policy outcomes.
- Automatically configure the External Powersafe TAP to control traffic flow based on trigger policy outcomes ([PowerSafe Trigger Mode](#)).

The system continuously monitors these conditions and manages actions based on the outcome of these conditions.

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 Option](#) and [Combination \("Combo"\) Triggers](#)).

Up to 64 user-defined trigger policies can be created on a single system. Each trigger policy has one of two states:

- **Active**: indicates the condition defined in the trigger **has** occurred.
- **Inactive**: indicates the condition defined in the trigger has **not yet** occurred.

## Trigger Type Settings

The following trigger types can be defined to monitor any one of the following conditions:

- [Link State Triggers](#)
- [Health Check Triggers](#)
- [Overflow Drop Triggers](#)
- [Bandwidth Utilization Triggers](#)
- [Combination \("Combo"\) Triggers](#)
- [PPS Threshold Triggers](#)

### Link State Triggers

You can define a Link State policy to trigger when one or more specified port links are online or offline. You can define the following options:

- Any one or all of the selected link ports to be in an Online state.
- Any one or all of the selected link ports to be in an Offline state.
- [Trigger Timer Settings](#)



- [Port Selection](#)
- [Trigger Actions](#)

If **ANY** is selected, this functions as a logical OR across the links. If **ALL** is selected, this functions as a logical AND across the links.

The screenshot shows a configuration interface for trigger actions. At the top, there are five radio buttons: Linkstate (selected), Healthcheck, Overflow, BandwidthUtilization, and Combo. Below these, under the heading "Trigger Link", is a dropdown menu set to "Any Offline". A note below says "Condition to activate trigger when link goes offline/online". Under "Active Set Time", there is a field with the value "5" and a note "Default: 5 Valid values: 0-30 Time to monitor whether the conditions are met persistently before setting active". Under "Active Clear Time", there is another field with the value "5" and a note "Default: 5 Valid values: 0-30 Time to monitor whether the conditions are not met persistantly before setting inactive".

## Health Check Triggers

You can define a Health Check policy to trigger when health check status fails to enable logical link down of the port pairs in the inline monitor port group.

For health check triggers, the basic unit is an inline monitor port pair. One inline monitor port pair has up to two health check profiles, one for each port. When any port health check profile of a port pair fails/is down, the port pair is logically down.

In the case when no health check profile is applied to a port of an inline monitor port pair, this port's health check state is shown as down but it would not affect associated triggers' state or cause load balance failover.

You can define the following options:

- Monitor health check of either any or all of the inline monitor port-pairs.
- [Trigger Timer Settings](#)
- [Port Selection](#)
- [Trigger Actions](#)



Linkstate  Healthcheck  Overflow  BandwidthUtilization  Combo

Trigger Healthcheck

Default: all  
Condition to activate trigger when healthcheck fails on any/all inline monitor ports

Active Set Time   
Default: 5  
Valid values: 0-30  
Time to monitor whether the conditions are met persistently before setting active

Active Clear Time   
Default: 5  
Valid values: 0-30  
Time to monitor whether the conditions are not met persistantly before setting inactive

## Overflow Drop Triggers

You can define an Overflow Drop policy to trigger when port overflow drops occur on one or more specified ports. You can define the following options:

- [Trigger Timer Settings](#)
- [Port Selection](#)
- [Trigger Actions](#)

Linkstate  Healthcheck  Overflow  BandwidthUtilization  Combo

Active Set Time   
Default: 5  
Valid values: 0-30  
Time to monitor whether the conditions are met persistently before setting active

Active Clear Time   
Default: 5  
Valid values: 0-30  
Time to monitor whether the conditions are not met persistantly before setting inactive

## Bandwidth Utilization Triggers

You can define a Bandwidth Utilization policy to trigger when bandwidth utilization of one or more specified ports exceeds user-defined limits.

- The direction to be monitored - receive (RX) or transmit (TX)
- The minimum level threshold, below which the trigger is activated. Enter 0% utilization to disable the minimum level of Bandwidth threshold.
- The maximum level threshold, above which the trigger is activated. Enter 100% utilization to disable the maximum level of Bandwidth threshold.
- [Trigger Timer Settings](#)
- [Port Selection](#)



- Trigger Actions

The screenshot shows the configuration for a BandwidthUtilization trigger. At the top, there are five radio buttons: Linkstate, Healthcheck, Overflow, BandwidthUtilization (which is selected), and Combo. Below this, the 'Direction' is set to 'Tx'. The 'Min' value is set to 0. The 'Max' value is set to 100. The 'Active Set Time' and 'Active Clear Time' both have a value of 5. Detailed descriptions for each field are provided below the input fields.

Setting	Description
Direction	Tx
Min	0
Max	100
Active Set Time	5
Active Clear Time	5

## Combination ("Combo") Triggers

You can define a Combination policy to trigger based on the states of other policies.

- Other trigger policies to include
- Remote trigger policies ([pfsMesh-enabled triggers](#) that are visible to all nodes in pfsMesh)
- Whether to include Any or All in the combination

**Note:** If a selected remote trigger is no longer reachable, it displays in red towards end of the Remote Profiles list.

- State (active/inactive) to be monitored on the selected profiles.
- [Trigger Timer Settings](#)
- [Trigger Actions](#)

The screenshot shows the configuration for a 'Combo' trigger. At the top, there are five radio buttons: Linkstate, Healthcheck, Overflow, BandwidthUtilization, and Combo (which is selected). Below this, there are two dropdown menus: 'Other Profiles' and 'Remote Profiles', both with a 'Clear All' button. The 'Condition' is set to 'Any', and the 'State' is set to 'Active'. The 'Active Set Time' and 'Active Clear Time' both have a value of 5. Detailed descriptions for each field are provided below the input fields.

Setting	Description
Condition	Any
State	Active
Active Set Time	5
Active Clear Time	5



## PPS Threshold Triggers

**Note:** The PPS Threshold triggers are only supported on the PFS 5000/7000 series.

You can define a Packets per Second (PPS) Threshold policy to trigger when packets per second of one or more specified ports exceeds user-defined limits.

- The direction to be monitored - receive (RX) or transmit (TX)
- The minimum level threshold, below which the trigger is activated. Enter 0 Packets per Second to disable the minimum level of PPS threshold.
- The maximum level threshold, above which the trigger is activated. Enter 0 Packets per Second to disable the maximum level of PPS threshold.

**Note:** Threshold values can include one decimal point (for example, 123.1 is valid, but 123.12 is not valid).

- Threshold unit of measure:
  - PPS – Packets Per Second
  - KPPS – Kilo/Thousand Packets Per Second
  - MPPS – Million Packets Per Second
- [Trigger Timer Settings](#)
- [Port Selection](#)
- [Trigger Actions](#)

The screenshot shows a configuration interface for a PPS Threshold trigger. At the top, there are tabs for Linkstate, Healthcheck, Overflow, BandwidthUtilization, Combo, and PPS Threshold. The PPS Threshold tab is selected, indicated by a blue circle. Below the tabs, there is a dropdown for 'Direction' set to 'Rx'. A note says 'Default: tx' and 'Direction to monitor PPS threshold - either rx or tx'. There are two sections for thresholds: 'Minimum PPS' (checkbox checked, value 0.0, default 0.0, note 'Lower threshold for port PPS') and 'Maximum PPS' (checkbox checked, value 8500.0, default 0.0, note 'Upper threshold for port PPS'). A dropdown for 'Maximum Unit' is set to 'KPPS' (default PPS). Below these are 'Active Set Time' (value 0, default 5, note 'Valid values: 0-30') and 'Active Clear Time' (value 0, default 5, note 'Valid values: 0-30').



## Trigger Timer Settings

Each trigger policy provides timer settings to help prevent flapping of the condition. Flapping occurs when a condition changes state too frequently, resulting in an excess of notifications.

- **Active set time:** set the amount of time in seconds the trigger condition must be true before it is set to Active state.
- **Active Clear time:** set the amount of time in seconds the trigger condition must be false before it is set to Inactive state.

Active Set Time	<input type="text" value="5"/>
Default: 5	
Valid values: 0-30	
Time to monitor whether the selected conditions are met persistently before setting active	
Active Clear Time	<input type="text" value="5"/>
Default: 5	
Valid values: 0-30	
Time to monitor whether the conditions are not met persistantly before setting inactive	

## Port Selection

Most trigger policies allow you to select specific ports or port groups to monitor for the trigger condition.

### Port Selection

Select the individual ports you want to monitor for the condition.

Select ports to use (drag-n-drop):

List of ports to be monitored

Slot:  1  All

Available Ports					Selected Ports		
1-1	1-2	1-3	1-4	1-6	1-5	1-7	1-8
1-9	1-10	1-11	1-12	1-13			
1-14	1-15	1-16	1-17	1-18			
1-19	1-20	1-21	1-22	1-23			
1-24	1-25	1-26	1-27	1-28			
1-29	1-30	1-31	1-32	1-33			
1-34	1-35	1-36	1-37	1-38			
1-39	1-40	1-41	1-42	1-43			
1-44	1-45	1-46	1-47	1-48			
1-49	1-50	1-51	1-52	1-53			
1-54							

OK Cancel Clear All

A red arrow points from the "Available Ports" section to the "Selected Ports" section, indicating the direction of selection.



## Port Group Selection

You can define multiple port groups of each type (network, monitor, inline-network, and inline-monitor) that you want to monitor for the condition. Note that PFOS processes each port in each group individually, as if each port were added individually to the list of ports.

The screenshot shows a 'Port Groups' configuration window with four main sections:

- Network:** Contains two entries: NPG1 and NPG2. Below it is the text "List of network port groups to be monitored".
- Monitor:** Contains two entries: MPG1 and MPG2. Below it is the text "List of monitor port groups to be monitored".
- Inline Network:** Contains two entries: INPG1 and INPG2. Below it is the text "List of inline-network port groups to be monit...".
- Inline Monitor:** Contains one entry: IMPG1. Below it is the text "List of inline-monitor port groups to be monit...".

## Trigger Actions

For each defined trigger, one or more of these actions can be taken when the trigger becomes active:

- Modify the traffic mapping (as defined and configured in [Traffic Maps](#))
- Send a notification (see [Configuring Trigger Policies](#) and [Configuring Notifications](#) for details):
  - 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 (see [Port Selection](#) for how to select ports).

When one or more triggers have been defined with certain conditions, you can enable/disable Traffic Maps based on the outcome of the applied trigger policies.



^ Action

Notifications   
Enable notifications  
(false)

Force Link Down List of ports to be forced down when trigger becomes active

Ports [configure](#) Selected Ports:

Status inactive  
**Default:** inactive  
Current status of this trigger

## pfsMesh Option

You can configure whether the trigger is visible to all nodes in pfsMesh (remote node).

pfsMesh  Disable  Enable  
**Default:** Disable  
pfsMesh Visibility enable/disable

- **Disable:** trigger is only visible to the node on which it was created.
- **Enable:** 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.
- You can view a list of currently available remote triggers by accessing the [Remote Triggers](#) tab on the pfsMesh page.



## Trigger Status and Nodes with Conflict

You can view the following status information for a trigger.

Status	inactive
<b>Default:</b> init Current status of this trigger	
Pfs Mesh Status	TriggerNameConflicts
<b>Default:</b> TriggerNameResolved Trigger profile pfsMesh status	
<b>Nodes with Conflict</b> List of nodes with which the trigger profile name conflicts	
Conflicting Node ID	Conflicting Node Name
FFB99E00	PFS-5010-119

Status	Displays the current status of this trigger: <b>Active:</b> indicates the condition defined in the trigger <b>has</b> occurred. <b>Inactive:</b> indicates the condition defined in the trigger has <b>not yet</b> occurred.
pfsMesh Status	Trigger name resolution status as updated by pStack protocol. <ul style="list-style-type: none"><li>• <b>TriggerNameConflicts:</b> a conflict occurred with current trigger name and another trigger within pfsMesh.</li><li>• <b>TriggerNameResolved:</b> no conflict exists with current trigger name and another trigger within pfsMesh.</li></ul>
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.

## Configuring Trigger Policies

Use the following process to configure trigger policies.

1. From the **Trigger Policies** page, click the **Add** button.
2. In the **Name** field, enter a descriptive name for the new trigger profile and click **Add**.

**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.



# Add new Profile

## ^ Add new Profile

Name \*

User friendly name for trigger profile

Add

Cancel

3. Select a trigger type and configure the relevant settings for the trigger. Settings vary per type, refer to the following sections for details:
  - [Link State Triggers](#)
  - [Health Check Triggers](#)
  - [Overflow Drop Triggers](#)
  - [Bandwidth Utilization Triggers](#)
  - [Combination \("Combo"\) Triggers](#)
  - [PPS Threshold Triggers](#)
4. If you enabled notifications in the trigger policy, configure the type of notification you want to send using the following [Configuring Notifications](#) settings (All, None, Syslog, SNMP, NETCONF):
  - Use the **Notifications > Events > Config Notification > Applications** *trigger-policy* setting to define the type of notification sent when a trigger configuration change is detected.
  - Use the **Notifications > Events > Chassis Notification > Mgmt** *trigger-policy* setting to define the type of notification sent when any state change to a trigger policy is detected.
  - Use the **Notifications > SNMP > Traps > System** *trigger-policy* setting to send only SNMP traps when any state change to a trigger policy is detected. Note this setting is the same as enabling the SNMP option for **Notifications > Events > Chassis Notification > Mgmt** *trigger-policy*.
5. To enable or disable traffic maps based on the outcome of the trigger, assign the trigger to one or more traffic maps (refer to [Traffic Maps](#) for more information):
  - a. On the **Traffic Maps** page, select the traffic map you want to assign a trigger policy.
  - b. In the **State** area, select **Trigger Profile**.
  - c. In the **Name** field, select the trigger policy you want to assign to the traffic map.
  - d. In the **State** field, select the trigger state you want to enable the map (Active/Inactive).



State

Enable    Disable    Trigger Profile

Name: tg1   Name of the trigger to be monitored

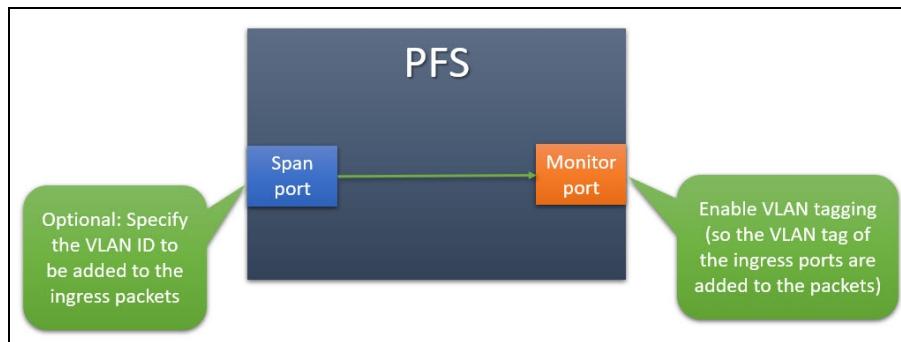
State: Active   Default: active

Enable map when trigger state is active/inactive

## Source Port VLAN Tagging

When a packet enters the system through a Span, Service, or Span-Monitor port, PFOS adds a VLAN tag to the packet. This VLAN tag identifies the PFOS port through which traffic entered the system. The VLAN tag contains the VLAN identifier (VID) of the port ingressing the traffic. By default, PFOS removes this VLAN tag when the packet exits the system through a Monitor port. You can configure PFOS to retain the VLAN tag for egress packets; refer to [Configure a Port to Add VLAN Tags to Egress Packets](#).

The following diagram describes how and where to configure source port VLAN tagging.



## Ingress Port VLAN IDs

The default VID value of each port is determined by the starting VID and the ingress port identifier value (Port ID) based on its physical location. You can customize the default VID; refer to [Change the Default TPID or Starting VLAN ID](#) for details.

You can also configure a user-defined VID; refer to [Override the System Default Ingress VLAN ID on an Ingress Port](#).

You can view the VLAN ID assigned to each port in the "VID" column on the Port Settings page or by using the CLI command `show interface <x> eth <y> vid` (see the [PFOS CLI Reference Guide](#)).

**Note:** If pStack is enabled (that is, PFS has a port with Class=pStack OR has learned a pStack port in pfsMesh):

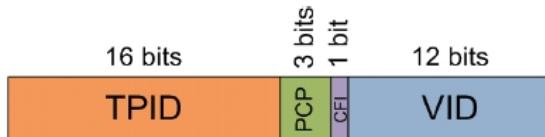
- The pStack protocol overrides the default VLAN ID and assigns a unique pStack VLAN ID (1 to 4000) to each port; incoming packets are tagged with the pStack VLAN ID, and the "VID" column in the Port settings page or CLI will display the pStack-assigned VLAN ID.



- If a user-defined VLAN ID is configured, the pStack VLAN ID is replaced with the user-defined VLAN ID at the egress port. Refer to [pfsMesh](#) in this guide and the CLI command `show vlan-translation` in the **PFOS CLI Reference Guide** for details.

## VLAN Tag Format

The following figure shows the general format of a VLAN tag:



The VLAN tag contains the following fields:

**Table 4.5 - VLAN Tag Fields**

Bits	Field	Description
1-16	TPID	Tag Protocol Identifier
17-19	PCP	Priority Code Point: IEEE 802.1p priority level
20	CFI	Canonical Format Identifier: 0 = canonical MAC; 1 = non-canonical MAC
21-32	VID	VLAN Identifier: combination of the ingress system ID and port ID, or user-specified value

The Tagged Protocol Identifier (TPID) is often referred to as the EtherType (EType), since the TPID for the outermost VLAN tag appears in the normal EType position of the packet header. By default, the TPID value is 0x88A8, which is in accordance with the IEEE 802.1ad standard from 2005. You can choose an alternate TPID value of 0x8100 (IEEE 802.1q) or 0x9100 (old IEEE 802.1q-in-q draft). 0x88A8 is the better of these TPID values because this is the standard for supporting arbitrary numbers of VLAN tags on a packet, but not all monitoring tools support or recognize this TPID value.

## Override the System Default Ingress VLAN ID on an Ingress Port

You can optionally assign a specific VID to any port, overriding the default VID (or pStack VLAN ID) for that port. This allows you to assign the same VID to multiple ports. If a VID is specified for a specific port, then that VID is used instead of the default value.

1. On the Port Settings page, select the ingress port for which you want to configure a specific VLAN ID. This option is available for port classes Span, Span-Monitor, and Service.
2. In the VLAN ID section, select **User Defined** and enter a VLAN ID (1-4094) in the field that displays.



The screenshot shows a 'Basic' configuration page for a port. It includes fields for Name (string), Class (Span selected), Link State (Auto), VLAN ID (User Defined set to 101), and Link status (down). The 'User Defined' radio button for VLAN ID is highlighted with a red oval.

3. Repeat Steps 1 and 2 for each port that you want to use a user-specified VLAN ID.
4. Click **Apply**.

## Configure a Port to Add VLAN Tags to Egress Packets

**Note:** Source Port VLAN tagging is not supported on Span-Monitor ports with External Device Tagging enabled. This option is used in PFS/PFX inner filtering and inner load balancing configurations; refer to [PFS+PFX Inner Filtering and Inner Load Balancing](#) for details.

Source port VLAN tagging is enabled/disabled on a per-port basis on the Port Settings page for each Monitor port.

- Enabled: Source port VLAN tag is retained when packets egress out of device
- Disabled: Source port VLAN tag is removed when packets egress out of device

Perform the following:

1. On the Port Settings page, select the egress port for which you want PFOS to add VLAN tags to egress packets. This option is available for port classes Span, Span-Monitor, and Service.
2. Select **Enable** from the VLAN Tagging pull-down list for that egress port.
3. Repeat Steps 1 and 2 for each port that you want PFOS to add VLAN tags to egress packets.
4. Click **Apply**.



Basic Advanced

Name: string  
A user friendly port name. Max length is 31.

Class: Span Monitor Span-Monitor Service pStack

Link State: Auto Default: auto Port Link state

Vlan Tagging: Enable Default: disable VLAN Tagging enable/disable

VLAN ID: Default User Defined string

Link: down Default: down Port Link status

## Change the Default TPID or Starting VLAN ID

1. Open the **Global Settings > System** page.
2. On the Source Port VLAN Tagging tab, select the desired **TPID EtherType**. This EtherType will be used for all VLAN tags added by the PFS.
3. On the same page, select a **Starting VLAN ID** (1-3464, default is 1). The starting VLAN ID affects the default VLAN ID that PFOS automatically assigns to all ports (which may be [overridden by a user-defined VLAN ID](#)).
4. Click **Apply**.

Basic Information Network Source Port VLAN Tagging Features Syslog Trace Log LCD

TPID Ether Type: 88A8 -- Provider Bridging (IEE...) Default: 88A8 -- Provider Bridging (IEE...)

Starting VLAN ID: 1 Default: 1 Valid values: 1—3464

## IP Tunnel Termination

**Note:** The [Features Tunnel option](#) in Global Settings must be enabled before you can use this feature.

IP Tunnel Termination allows PFOS to perform encapsulated forwarding of mirrored traffic. This allows, for example, PFOS to act as a remote mirroring destination, using IP tunneling protocols. PFOS works with most types of tunnels such as Encapsulated Remote Port Analyzer (ERSPAN [all types]), Generic Routing Encapsulation (GRE), Network Virtualization GRE (NVGRE), or VXLAN.

As a destination endpoint, designated ports on a system running PFOS will receive traffic from one or more remote mirroring source ports. A remote mirroring source port mirrors, encapsulates, and transmits the traffic to a destination port over a local area network. The traffic



is typically encapsulated in some form of GRE (using IP as its transport) and is, therefore, routable across a Layer 3 network between the source node and the destination node. Common GRE, NVGRE, and ERSPAN sources include L2/L3 switches or virtual environments.

Acting as an IP endpoint, each defined PFOS port responds to ARP and ICMP (ping) messages so that upstream switches and routers can forward the tunneled traffic to the PFOS port. You must configure at least one IP address for each port that will act as a tunnel destination.

**Note:** Generic IP Tunnel Termination does not include header stripping or de-encapsulation, though this feature can be combined with the stripping capabilities of the PFS or PFX when necessary. Refer to [Enhanced Port Features](#) for PFS details and PFX documentation for PFX details.

IP Tunnel Termination is available on Span and Span-Monitor class ports on all models of line cards supported by PFOS. However, advanced ports of class Span, Span-Monitor, Service, or Monitor on a 40SadvR line card are required to de-encapsulate tunneled traffic before forwarding the frames to the monitoring tools. Refer to [Protocol De-encapsulation and Stripping](#) for details on how to set this up. Conducting the de-encapsulation on a Service or Monitor class port might be desirable, depending on the monitoring tools being used.

Two steps are required to use Tunnel Termination:

- Create a Tunnel Termination group containing a list of IP addresses, or use a Tunnel Termination group that you created earlier.
- Enable Tunnel Termination on the desired port(s), and associate a Tunnel Termination group with each port on which the feature is enabled.

## Create Tunnel Termination Group

**Note:** The [Features Tunnel option](#) in Global Settings must be enabled before you can use this feature.

1. On the Applications page, click the **Tunnel Termination** tab. This page shows the currently defined Tunnel Termination groups and the port(s) that are using each group.

Name	IP	Port List
ep1	10.10.10.1, 10.10.10.2, 10.10.10.3, 10.10.10.4	
ep2	1.1.1.1, 2.2.2.2	

2. Click **Add** to create a new Tunnel Termination group.
3. In the Name field, enter a descriptive name for the Tunnel Termination group that you are going to create.



4. Click **Add** to begin adding IPv4 addresses to the group.

**Add new Tunnel Termination** tunnel-termination Groups

Name \*  User friendly name for tunnel-termination Grou...

**Add** **Cancel**

5. In the IP field, click **Add an entry**.
6. In the field that then displays, enter an IPv4 address.
7. To add that address, click **Add**.
8. To add another address, click in the IP list and repeat steps 6-7.

**ep1** x [New Tunnel Termination...](#)

IP     **Update** **Add** **Cancel**

List of IP addresses

**Port List** List of Port using this tunnel-termination group

Port Name

Table is empty

## Assign a Tunnel Termination Group to a Port

**Note:** The [Features Tunnel option](#) in Global Settings must be enabled before you can use this feature.

1. Go to the Port Settings page for the port on which you want to use Tunnel Termination.
2. Enable the **Tunnel Termination** checkbox.
3. In the Tunnel Termination Library drop-down list that displays, select the Tunnel



Termination group to associate with Tunnel Termination on this port.

## Port 5-6 Settings

Reset Port ▾

Basic Advanced References

Name	string	Class	<input checked="" type="radio"/> Span <input type="radio"/> Monitor <input type="radio"/> Service
Link State	Auto	Link	down
VLAN ID	<input checked="" type="radio"/> Default <input type="radio"/> User Defined	Tunnel Termination Library	ep1
Tunnel Termination	<b>Default: disable</b> Selectable Tunnel Termination in this port	Tunnel Termination Library	Select an Tunnel Termination name

## Delete a Tunnel Termination Group

1. From the Tunnel Termination page, in the Tunnel Termination groups list, click the line containing the entry that you want to move. The line is highlighted with a gray background.
2. Click **Delete**. Click **Yes** in the confirmation pop-up window.

## Tunnel Termination Considerations and Limitations

The following considerations apply to the current release of Tunnel Termination:

- After an IP address has been added to a Tunnel Termination group, any ARP request packet with that IP address as the target will be consumed by the packet flow switch running PFOS. These packets will not be forwarded, but will be analyzed and counted as ARP packets on that port displayed under Control Packets Statistics. Such ARP requests will be responded to.
- After an IP address has been added to a Tunnel Termination group, any ICMP packet with that destination MAC address and that destination IP address will be consumed by the packet flow switch running PFOS. Those packets will not be forwarded, but will be analyzed and counted as ICMP packets on that port displayed under Control Packets Statistics. Such ICMP requests will be responded to.
- Each Tunnel Termination group supports a maximum of 16 IP addresses.
- Tunnel Termination is rate-limited to 200 ARP control packets and 300 ICMP control packets per second on all channels. Extra packets are dropped and are counted as dropped packets on that port, displayed under Control Packets Statistics.
- The Tunnel Termination destination does not respond to fragmented control (ARP, ICMP) packets.
- Jumbo control packet MTU larger than 9000 bytes is not supported.



## pfsMesh

**Note:** Packet flow switches that run PFOS 3.x, such as the NETSCOUT nGenius® PFS 2204 and PFS 4204, support a different stack protocol and mesh architecture and are not compatible with pStack and pfsMesh. You cannot combine PFOS 3.x and PFOS 4.x/5.x/6.x systems into the same mesh.

pfsMesh helps you interconnect PFOS devices and create maps spanning across the pfsMesh to build redundant mesh systems for complete traffic access and visibility. Each traffic access model functions as a node in the system architecture. Supporting LANs and cloud-based network infrastructure, pfsMesh technology is available on all devices that use PFOS.

With a pfsMesh, monitor output can be directed to monitor ports on the local system (the same system as the network port input), to a group of monitor ports on a remote system (any system in the stacking topology), or any combination of these ports. You can tap into your network on a system in one location and have the filtered and monitored output directed to a different system in a different location. For example, a system in one building of a campus can have its monitor output directed to a system in a different building in the campus, or a system on one floor of a building can be monitored on a different floor.

pfsMesh provides an administrator an integrated management Interface. All nodes within a pfsMesh can be viewed and managed from any of the nodes. Each system is then accessible from that same Web UI instance (see [Using the pfsMesh Page \(pStack\)](#)). This leverages your investment in network analysis equipment, as stacking can be used to direct monitored traffic to centrally-located analyzers for wider stacking ability. Benefits include:

- A distributed management architecture that has no single point of failure; if one node fails, then all other nodes continue to be fully manageable.
- The physical management interface to each node remains the management Ethernet ports on each node; management occurs only through that interface. This means that each node must have a management Ethernet connection to your network (the same network on which the web browser is connected), and each node must be configured with a proper and unique IP address.

A pfsMesh can be established by devices having:

1. Only pStack ports
2. Only pStack+ ports
3. A combination of pStack and Stack+ ports

In a pfsMesh having devices with **only pStack ports OR a combination of pStack and pStack+ ports** the following is true:

- VLAN allocation is performed dynamically via the pStack protocol. This VLAN ID helps the pStack protocol segregate traffic streams received from different Ingress ports. A unique VLAN ID is assigned to each ingress port from which you have created a traffic map (due to VLAN ID limitation, it can support a maximum of 4000 Ingress ports).



- If a user-defined VLAN ID is configured at ingress ports, PFOS then performs VLAN translation on egress ports using a translation table; 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. See the `show vlan-translation-table` command in the **PFOS CLI Reference Guide**.

In a pfsMesh having devices with **only pStack+ ports** the following is true:

- PFOS does **not** use VLAN IDs to segregate flows if a pfsMesh is based on pStack+ only
- The incoming packets are tagged with the port's user-defined VLAN. If A user-defined VLAN is not set, then PFOS will use the port's default VLAN (VLAN ID assignment and translation are not required and the 4000 Ingress port maximum does not apply). Refer to [pStack and pStack+ Compatibility](#) for details.

## pStack Technology

**Note: pStack+ requires the PFS 7000 functionality license. Refer to [pfsMesh Using pStack+](#) for details.**

pStack and pStack+ are the proprietary technologies that allow the interconnection of multiple systems into a pfsMesh. pStack+ leverages existing pStack protocol features and supports additional enhancements that are not supported on pStack; pStack+ is supported on PFS 7000 devices and requires the PFS 7000 functionality license (refer to [pfsMesh Using pStack+](#) for details). Once a node is configured with pStack or pStack+ ports, each node automatically discovers all other interconnected nodes and each node has knowledge of all other nodes in the pfsMesh. pfsMesh also supports auto healing. When pStack or pStack+ ports fail, PFOS automatically re-routes traffic to other configured pStack/pStack+ ports (of the same type) within the pfsMesh.

## pfsMesh pStack Protocol Requirements

**Note: pStack+ requires the PFS 7000 functionality license. Refer to [pfsMesh Using pStack+](#) for details.**

Prior to PFOS 6.1.2, pStack versions contain only a major version number (such as versions 27 and 28). For 6.1.2 and later, pStack versions contain a *major.minor* version syntax, such as version 30.1.

The following sections summarize pStack protocol requirements within a pfsMesh. See also [pStack and pStack+ Compatibility](#)

### **PFS 5000, 7000, and 6000 Series Devices (EXCEPT PFS 5120/7120 and PFS 6010 Devices)**

All PFS 5000 and PFS 7000 devices in a pfsMesh must run the same major and minor version of the pStack/pStack+ protocol. See [PFS 5120/7120 exception](#) and [PFS 6010 exception](#).

**Note:** 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 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.**



- **PFS 5120/7120 Devices Exception**

PFS 5120/7120 devices running PFOS 6.5.0 and pStack version 30.6 are supported within a pfsMesh based on pStack with PFS 5000/7000 devices running pStack version 30.5 (PFOS 6.4.1/PFOS 6.4.2). This exception only applies to pfsMesh based on pStack; if the pfsMesh has any pStack+ configuration then all PFS 5000 and PFS 7000 systems in a pfsMesh must run the same major and minor versions of the pStack/pStack+ protocol. This exception only applies to PFS 5120/7120 devices; all PFS 5000 and PFS 7000 systems in a pfsMesh must run the same major and minor versions of the pStack/pStack+ protocol.

- **PFS 6010 Devices Exception**

As of PFOS 6.1.3 (pStack version 30.1), PFS 6010 devices within a pfsMesh running at least version 30.1 will be supported within a pfsMesh with PFS 5000/7000 devices running the same *major* version but also later minor versions of pStack/pStack+ protocol (such as 30.2). This exception only applies to PFS 6010 devices; all PFS 5000 and PFS 7000 systems in a pfsMesh must run the same major and minor versions of the pStack/pStack+ protocol.

### **Viewing Current pStack/pStack+ Version**

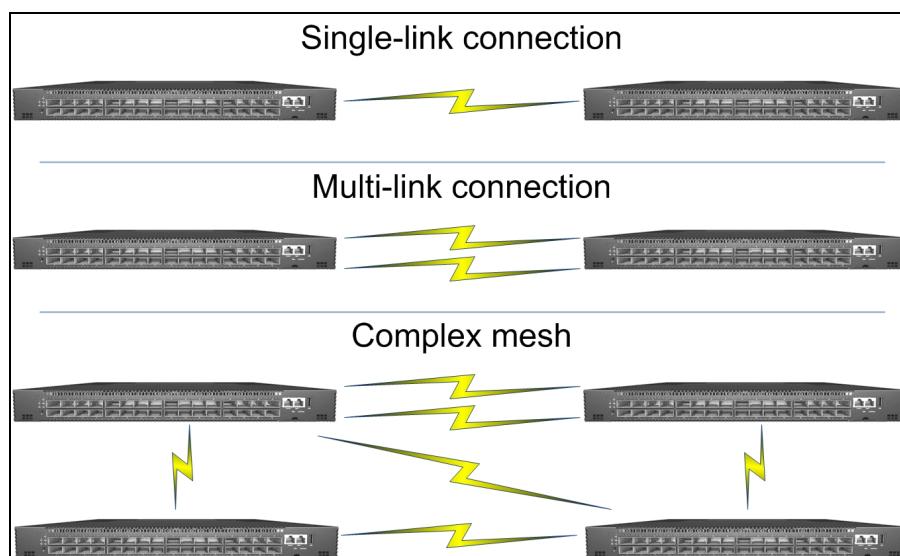
You can view the currently installed version of the pStack protocol:

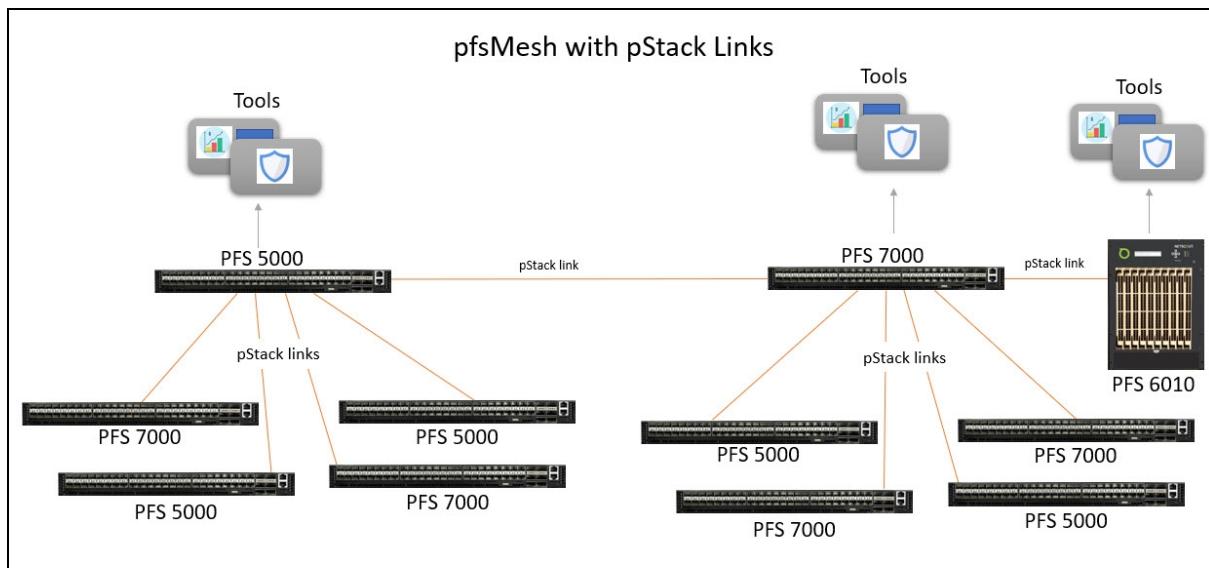
- On the System Status > [Software Tab](#) page
- By using the `show system pstack-version` CLI command, as described in the *PFOS 6.x CLI Reference Guide*.

## **pfsMesh Topology**

As shown below, pfsMesh stacking topology can range from a very simple single stack link between two systems to complex meshes with up to 256 nodes. Complex pfsMesh topologies have advantages over simple single links in providing aggregation of stacking bandwidth and redundant paths.

Systems in a pfsMesh automatically aggregate bandwidth across parallel paths and redundant paths, and automatically reconfigure monitor output to alternate paths in the event of link failure.





You can interconnect pStack or pStack+ ports to form a pfsMesh by using a direct, dedicated cable connection, physically from port to port; the ports do not have any Layer 2, 3, or 4 entity on the network. As part of PFS 7000 functionality, pfsMesh can also be built over IP networks using a VxLAN tunnel; refer to [pfsMesh Using pStack+](#) for details.

Technical considerations include:

- Stack links can be any port speed, using fiber or copper, as determined by the system model and port selected.
- Stack links use standard Ethernet cabling, as appropriate for the port type and speed. No proprietary or unusual cables are required.
- For pStack, there should not be any Ethernet switches or routers in any stack path; pStack links must be an unimpeded direct connection between two nodes. Standard Ethernet cabling distances apply: for example, 100 meters at 1Gbps (1000BaseT) to 80 kilometers at 10Gbps (10GBase-ZR).
- With pStack+ over IP (see [pfsMesh Using pStack+](#)), Ethernet switches and routers may be used between the two nodes.

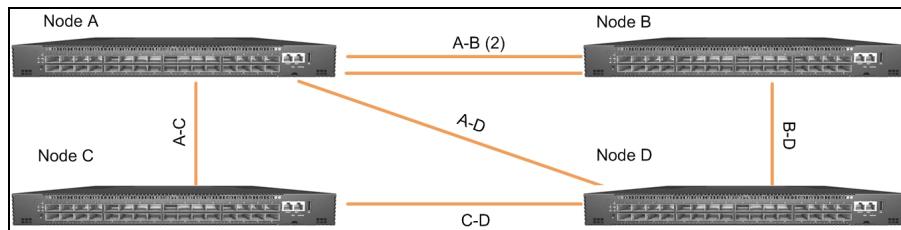
## pStack Optimal Path Forwarding

When you select one or more remote ports for monitor output, the system automatically chooses one or more stack links on which to transmit the monitor data. The system software always chooses the optimal path (or paths). The optimal path is determined using:

- **Link speed:** Higher-speed links are given great preference over slower-speed links.
- **Hops:** The most direct links are given slight preference over links that involve one or more intervening nodes, where monitor traffic must “hop” over another transit node. Hops do not necessarily reduce the available bandwidth, but they can introduce a small latency.



- **Available filtering resources:** If one or more filter maps are being applied to the traffic that is routed over the pfsMesh, then each node on the route must have sufficient filtering resources available to apply the filter map. If any node on the preferred route does not have sufficient filtering resources available, then the next lowest-cost route is selected and checked for filter resource availability until a viable route is found. For information about the Filter Resource Log, which displays available filtering resources on a node, and about the maximum number of filter elements allowed on each type of hardware, refer to [Traffic Filtering](#).



Therefore, in the above example:

- If all of the above stacking links are the same speed, and if Node A is configured to output monitored traffic to a monitor port on Node C, and if sufficient filtering resources are available on each node, then Node A chooses the A – C link for that traffic because it is the most direct path (no hops).
- If the A – C link failed, then Node A automatically reconfigures and chooses a new optimal path, A – D C – D. This path involves a single “hop” (through Node D), but it is then the optimal path from Node A to Node C.
- If the A – C link is linked at a slower speed, such as 1G when the other links are 10G, then Node A also chooses the path A – D C – D. This path is optimal because it is entirely 10G – which, although there is a single hop through Node D, is still faster than the A – C link at 1G.

Optimal path selection is automatically done on a per-map, per-output-port basis (and per-hop).

If the stacking topology has more than one possible optimal path for any given map/port, then the multiple optimal paths together are referred to as a parallel path. A parallel path can be used to achieve greater net bandwidth between nodes, using load spreading.

PFOS may determine the pStack optimal forwarding path before all pStack links are available. In addition, pStack link state change may offer a new optimal forwarding path. To avoid unnecessary traffic interruptions, pStack will not automatically move traffic to a new forwarding path even if it is a better path. However, you can manually force pStack to recalculate, determine, and use a new optimal forwarding path for traffic by using the `reroute-maps` CLI command.

**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.

## pStack Load Spreading in a pfsMesh

To prevent wasted bandwidth on the stack links, the node spreads the monitor traffic across the parallel path links using load spreading. This involves a static assignment of one of the parallel path links, on a map by map basis, alternating link assignments to each successive map. This divides the total traffic across the parallel path links, although in a manner which is most likely to be less “even” than with load balancing.



For example, using the topology shown in the previous section, if Node A is configured with two non-load-balanced maps specifying monitor output to local ports 2-1 and 2-2, and also remote ports Node B:3-3 and Node B:3-4, with one map filtering for HTTP traffic and another map filtering for Telnet traffic, then load spreading is done as follows:

- 100% of the traffic is output on 2-1.
- 100% of the traffic is output on 2-2.
- All HTTP traffic is forwarded across the A-B-1 stacking link.
- All Telnet traffic is forwarded across the A-B-2 stacking link
- 100% of the traffic is then output on Node B:3-3.
- 100% of the traffic is then output on Node B:3-4.

## Technical Considerations for Load Spreading

All filtering – and all load spreading – is performed on every node in the path, beginning with the network port input node, then every node/hop in the path, and ending with the destination output node. Each packet is individually refiltered and again load balanced at each hop. As a result, stacking load spreading will adapt and vary from hop to hop, even within a single mapping.

## Configuring a pfsMesh Using pStack

Refer to the following sections to set up a pStack pfsMesh.

1. [Configure pStack Port Settings](#)
2. [Configure Monitor Output with a pfsMesh](#)
  - Destination Nodes: [Configure Remote Monitor Port Group](#)
  - Head Node: [Configure Monitor Output to One or More Ports on Remote Nodes \(Traffic Maps\)](#)
  - [View Status of Remote Monitor Groups That are Used in a Traffic Map](#)

### Configure pStack Port Settings

**Note:** pStack+ requires the PFS 7000 functionality license. Refer to [Configure pStack plus Port Settings for details](#).

In general, most ports that can be configured as a monitor port can be configured as a pStack port.

**Note:** All nodes in a pfsMesh must be configured to use the default TPID of 88A8. For more information, refer to [Source Port VLAN Tagging](#).



1. On each node that will be part of the pfsMesh, go to the Port Settings page, and set **pStack** class for each port that will be used to establish a pfsMesh connection between two systems.

**Note: If the port class is currently set to pStack plus, you must first configure the port class to Span, then configure the port class to pStack. You cannot change the port class directly from pStack plus to pStack (or vice-versa), you must configure the port to Span first.**

The screenshot shows the 'Port 1-17 Settings' dialog box. At the top, there are tabs for 'Basic', 'Advanced', and 'References'. Below the tabs, there are several configuration fields:

- Name:** 113-1-17::connected\_to::115-1-1. A note below says: 'A user friendly port name. Max length is 64.'
- Link State:** Auto. A note below says: 'Default: auto Port Link state'
- Speed:** 10000. A note below says: 'Default: none Port Speed (Mbits/sec)'
- VLAN ID:** Default (radio button selected).
- Link:** up. A note below says: 'Default: down Port Link status'

In the 'Class' section, there are four radio buttons: Span, Monitor, Service, and pStack. The 'pStack' radio button is selected and highlighted with a red circle.

2. Physically connect the pStack ports, using appropriate network cables, into the desired topography.
3. Each node automatically discovers all other interconnected nodes; each node has knowledge of all other nodes in the pfsMesh. Auto-discovery takes only a few seconds.
4. Go to the pfsMesh page, and verify the connection status of each node in the pfsMesh.

## Configure Monitor Output with a pfsMesh

In a pfsMesh, monitor output can be directed to:

- One or more Monitor ports on the **local** node (the same node as the network port input). See [Configuring Ports](#).
- A group of one or more Monitor ports on a **remote** node (any other node in the pfsMesh)
- A combination of the above.

[Configuring remote monitor output groups](#) is different than configuring individual local output Monitor ports.

## Configure Remote Monitor Port Group

Configure remote monitor port groups on the appropriate destination nodes. Up to 64 remote monitor groups can be created on a single system. A port can belong to more than one remote monitor group. Optionally, a remote monitor group also can contain a load balance group.

1. Log in to the destination system on which you want to create a monitor port group.
2. Go to the **Configuration > Port Groups** page, click the **Monitor** tab, and then click **Add**.
3. Enter a descriptive name for the monitor port group, and click **Add**.



**Note:** A Monitor port group used in pfsMesh as a remote monitor group must have a unique monitor group name to avoid conflict with other monitor group names and so it is easily identifiable within pfsMesh.

Add new Group Monitoring group type

Name \* group1  
A user friendly port group name. Max length is...

Add Cancel

4. In the Ports section, click **configure**.
5. Select the slot number to show the available ports for that slot. Drag one or more ports to the Selected Ports box. You can select multiple line card slots and their associated ports as output ports for your port group.
6. Click **OK**.

group1

Ports configure Selected Output Ports: 1-1, 1-22 Lb Criteria: Load-balance criteria  
Load Balance Groups: Add an entry ...  
pfsmesh:  Enable  Disable  
Default: enable  
pfsmesh Visibility: enable/disable

Status: PortGroupNameResolved  
Default: PortGroupNameResolved  
Port group status

Nodes with Conflict: List of nodes with which the port group name conflicts  
Ref Map: List of traffic maps using the port-group  
Pstack Ref Map: List of pStack maps using the port-group  
Ref Toolgroup: Name



7. Optionally, to add a load balance group:
  - a. In the Lb Criteria section, select pre-defined or user-defined load balancing criteria.
  - b. Click **Add an entry** in the Load Balance Groups section.
  - c. In the empty field that displays, enter the name of a previously defined load balance group, or select a load balance group from the drop-down list.
  - d. Click **Update**.

8. In the pfsMesh section, click **Enable** so that this port group is visible across the pfsMesh. (The **Disable** option causes this port group to only be visible to the node on which it was created.)
9. Click **Apply**. Refer to the [Remote Monitor Groups](#) tab on the pfsMesh page to view a list of currently available remote monitor port groups.
10. View the following status information for a monitor group.

Nodes with Conflict	
List of nodes with which the port group name conflicts	
Conflicting Node ID	Conflicting Node Name
FFBB5A00	PFS5010_116

Status	Monitor group name resolution status as updated by pStack protocol. <ul style="list-style-type: none"><li>• PortGroupNameConflicts: a conflict occurred with the current monitor group name and another monitor group name within pfsMesh</li><li>• PortGroupNameResolved: no conflict exists with the current monitor group name and another monitor group within pfsMesh</li></ul>
Conflicting Node ID	If pfsMesh status is PortGroupNameConflicts, then this field reflects the node ID with which the conflict exists.
Conflicting Node Name	If pfsMesh status is PortGroupNameConflicts, then this field reflects the node name with which the conflict exists.

## Configure Monitor Output to One or More Ports on Remote Nodes (Traffic Maps)

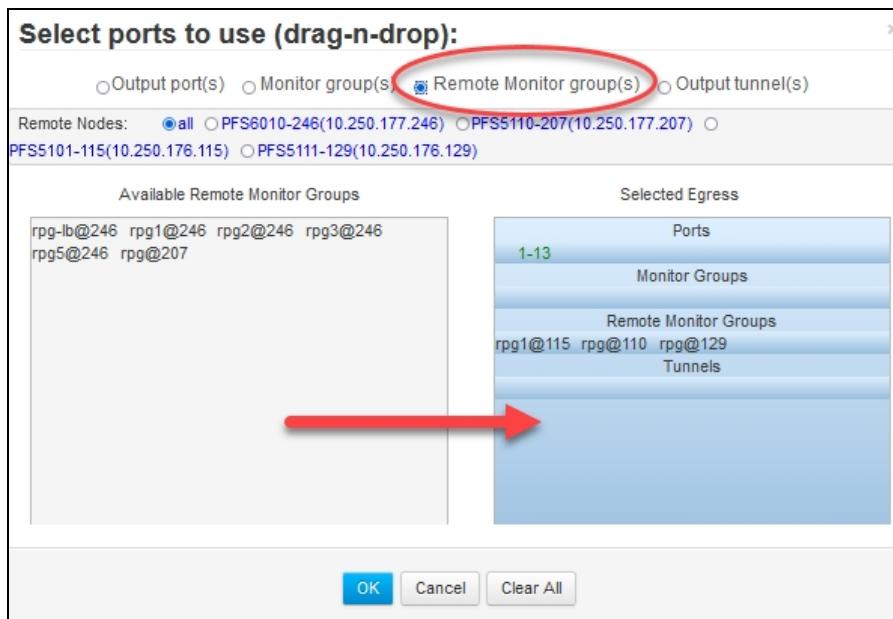
All traffic maps for pfsMesh are configured only on the head (input) node, the one on which traffic originally arrives in the pfsMesh.



1. Go to the Traffic Maps page.
2. In the Traffic Map section, click **Add**.
3. Enter a descriptive name for the traffic map, and click **Add**.
4. Specify the parameters of your traffic map as desired. For more information, refer to [Traffic Maps](#).
5. In the Ingress section, click **configure** and select the desired input port(s) and/or port group(s).
6. In the Egress section, click **configure**.

The screenshot shows the 'map-local' configuration dialog box. At the top, there are fields for 'Description' (string), 'Type' (Monitor), 'Mode' (Basic), and a 'Filter' dropdown set to 'unfiltered'. Below these are sections for 'Ingress' and 'Egress'. The 'Ingress' section has a 'configure' button and a note 'Selected Ingress: 1-54.1'. The 'Egress' section also has a 'configure' button, which is circled in red. It includes a note 'Selected Egress: rpg1@115, rpg@110, rpg@129, 1-13'. Further down are sections for 'Load Balance Criteria', 'Output Load Balance Groups', and 'Action' (Forward selected). On the right side, there are links for 'Map Status' and 'Remote Monitor Group Status'. At the bottom, there is a link for 'Output pStack Ports'.

7. The list of available output ports, monitor groups, and remote monitor groups on connected pfsMesh nodes displays. In the Remote Monitor Group(s), to list groups on all nodes, select **all**; to list groups on just one node, select the name of the node.
8. Drag and drop remote monitor groups as desired. When you are done, click **OK**.



- When you are done entering other parameters for your traffic map, click **Apply**. The system will try to find the remote monitor group(s) that you selected.

#### View Status of Remote Monitor Groups That are Used in a Traffic Map

- Go to the Traffic Maps page, and select the desired traffic map.
- Click **Remote Monitor Group Status** at the bottom of the page.

Remote Monitor Group Status			
Remote monitor group status			
<a href="#">Status Per Remote Monitor Group</a> <small>Remote monitor group status</small>			
Remote Port Group	Status	Destination Node ID	Destination Node
rpg1@115	RemotePortGroupResolved	E8EC4100	PFS5101-115
rpg@110	RemotePortGroupNotFound	0	
rpg@129	RemotePortGroupResolved	F316C100	PFS5111-129

Status	<ul style="list-style-type: none"><li>Remote monitor group resolution status as updated by pStack protocol.</li><li>RemotePortGroupNotFound: Unable to find any remote monitor group by this name in pfsMesh.</li><li>RemotePortGroupResolved: Remote monitor group name is unique in pfsMesh and successfully resolved to the Destination Node.</li><li>RemotePortGroupNotFound: More than one remote monitor group exists in pfsMesh by this name; to avoid ambiguity please use unique names. Protocol has resolved it to one of the nodes as depicted in the Destination Node.</li><li>HWEErrorOnTransitOrDestination: Map could not be created in pfsMesh as there was some HW error on a downstream node.</li></ul>
Destination Node ID	Node ID to which remote monitor group was resolved.



Destination Node	Node name to which remote monitor group was resolved.
------------------	---

## Using the pfsMesh Page (pStack)

The pfsMesh page displays the status of the pfsMesh as viewed from that system. It includes tabs to view topology, remote monitor groups, remote triggers, the pStack map, and VLAN IDs in use.

### Topology

The Topology tab displays information about each node currently in the pfsMesh. For remote nodes, you can click the IP address to access the Web UI for that node.

The screenshot shows the pfsMesh topology page with the 'Topology' tab selected. It displays five nodes:

- PFS6010-246 (10.250.177.246)**: Type: remote. Local Node's Port 1-35 connects to PF55110-207's Port (10.250.177.207) at 1-44. Local Node's Port 1-34 connects to PF55111-129's Port (10.250.176.129) at 1-44. Local Node's Port 1-4 connects to PF55010-137's Port (10.250.177.137) at 1-4. Local Node's Port 1-36 connects to PF55010-246's Port (10.250.177.246) at 1-36. Local Node's Port 1-39 connects to PF55010-246's Port (10.250.177.246) at 1-49.
- PFS5110-207 (10.250.177.207)**: Type: remote. Local Node's Port 1-44 connects to PFS6010-246's Port (10.250.177.246) at 1-35.
- PFS5101-115 (10.250.176.115)**: Type: local. Local Node's Port 1-4 connects to PFS5111-129's Port (10.250.176.129) at 1-4. Local Node's Port 1-36 connects to PFS5111-129's Port (10.250.176.129) at 1-36. Local Node's Port 1-49 connects to PFS5111-129's Port (10.250.176.129) at 1-39.
- PFS5111-129 (10.250.176.129)**: Type: local. Local Node's Port 1-54,4 connects to PFS5101-115's Port (10.250.176.115) at 1-32,4.
- PFS5010-137 (10.250.177.137)**: Type: local. Local Node's Port 1-4 connects to PFS5101-115's Port (10.250.176.115) at 1-32,4.

### Remote Monitor Groups

The Remote Monitor Groups tab displays the remote monitor port groups that are currently available on connected nodes in this mesh.



### pfsMesh

Topology    Remote Monitor Group    **Remote Trigger**    pStack Map    Vlan

▲ Partner Node Stacking partner node

ID	Name	Port Group(Name :: Status)
1F7A800	PFS6010-246	rpg-lb@246 :: PortGroupNameResolved rpg1@246 :: PortGroupNameResolved rpg2@246 :: PortGroupNameResolved rpg3@246 :: PortGroupNameResolved rpg5@246 :: PortGroupNameResolved
E0924600	PFS5110-207	rpg@207 :: PortGroupNameResolved
E8EC4100	PFS5101-115	rpg1@115 :: PortGroupNameResolved
F316C100	PFS5111-129	rpg@129 :: PortGroupNameResolved

Showing 1 to 4 of 4

## Remote Trigger

The Remote Trigger tab displays a list of remote triggers that are currently available on connected nodes in this mesh.

### pfsMesh

Topology    Remote Monitor Group    **Remote Trigger**    pStack Map    Vlan

▲ Trigger List of remote triggers

Name	Status	pfsMesh Status	Node ID	Node
ATG-1	inactive	TriggerNameResolved	4FD5F00	PFS5110-207
ATG-2	active	TriggerNameResolved	4FD5F00	PFS5110-207
TG2	inactive	TriggerNameResolved	4FD5F00	PFS5110-207
TG4	inactive	TriggerNameResolved	4FD5F00	PFS5110-207
TG5	inactive	TriggerNameResolved	4FD5F00	PFS5110-207
TG6	inactive	TriggerNameResolved	4FD5F00	PFS5110-207
TG7	inactive	TriggerNameResolved	4FD5F00	PFS5110-207
TG8	active	TriggerNameResolved	4FD5F00	PFS5110-207
Tg1	inactive	TriggerNameResolved	4FD5F00	PFS5110-207

## pStack Map

**Note:**pStack+ requires the PFS 7000 functionality license. Refer to [pfsMesh Using pStack+](#) for details.

The pStack Map tab displays all traffic maps created on this node via the pStack protocol. The pStack map is present on a node if it is either a transit hop, a destination node, or both for this map. PFOS lists the following information:



- **Name:** Name of pStack map 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.
- **Filter Expression:** Filter expression provided by pStack.
- **Input pStack Ports:** List of local pStack ports used as input.
- **Input pStack Plus Tunnel:** (only applicable to [pStack+](#)) Local pStack plus tunnel used as input.
- **Output pStack Ports:** List of local pStack ports used as output.
- **Output pStack Plus Tunnel:** (only applicable to [pStack+](#)) List of local pStack plus tunnels used as output to reach remote destination.
- **Output Monitor Groups:** Local output monitor port groups.
- **Priority:** Priority of this map.
- **Status:** Not displayed by default (for internal use only).

Name	Filter Expression	Input pStack Port	Input pStack Plus Tunnel	Output pStack Ports	Output pStack Plus Tunnels	Output Monitor Groups	Priority
E8EC4100-map-to-246-non-match-1696	VLAN 1696	1-54.4		1-36			2147483646
E8EC4100-map-to-246-non-match-1697	VLAN 1697	1-54.4		1-36			2147483646
E8EC4100-map-to-246-non-match-1698	VLAN 1698	1-54.4		1-36			2147483646
E8EC4100-map-to-246-non-match-1699	VLAN 1699	1-54.4		1-36			2147483646
E8EC4100-map-to-246-non-match-1700	VLAN 1700	1-54.4		1-36			2147483646
E8EC4100-map-to-246-non-match-1701	VLAN 1701	1-54.4		1-36			2147483646
E8EC4100-map-to-246-non-match-1702	VLAN 1702	1-54.4		1-36			2147483646
E8EC4100-map-to-246-non-match-1703	VLAN 1703	1-54.4		1-36			2147483646
E8EC4100-map-to-246-non-match-1704	VLAN 1704	1-54.4		1-36			2147483646
E8EC4100-map-to-246-non-match-1705	VLAN 1705	1-54.4		1-36			2147483646

## VLAN

The VLAN tab displays the VLAN IDs in use. Click on any item in the list to see the physical port associated with that ID.

ID
4
36
49
65
70
71
72
256
258



#### ▲ Line Card Port Settings

Port ID	Name	Class	Link	Speed	VID	XCVR Model	XCVR
1-1		Span	down	10000	257		
1-2		Span	down	10000	258	FINISAR CORP. FTLX1471D3BCV	1G/10
1-3		Span	up	10000	259	AVAGO AFBR-709DMZ	1G/10
1-4	pStack		up	10000	4	FINISAR CORP. FTLX8571D3BCV	1G/10

# 5 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](#).

- [Standard Stripping](#) (PFS 5000 and PFS 7000 Series)
- [Inline Monitor Egress VLAN Stripping](#)
- [Timestamping](#) (PFS 7000 Series)
- [L2GRE Tunnel Origination/Termination Support](#) (PFS 7000 Series)
- [VXLAN Tunnel Origination/Termination Support](#) (PFS 7000 Series)
- [Neighbor Discovery Using LLDP](#) (PFS 7000 Series)
- [pfsMesh Using pStack+](#) (PFS 7000 Series)
- [Mirroring and Slicing](#) (PFS 7000 Series)

### Standard Stripping

**Note: Standard stripping is available only on PFS 5000/7000 Series systems. For generic stripping on PFS 6000 Series systems, refer to [Protocol De-encapsulation and Stripping](#).**

Network monitoring, analysis, and security tools are typically either unable to handle or have limitations handling traffic that has certain tunneling or encapsulation protocols present in the packets. Furthermore, the presence of such protocols in the packets can restrict or limit the ability to apply filtering and flow-based load balancing to the traffic as it is forwarded to specific tools. To address each of these challenges, Standard Stripping options provide the ability to deencapsulate or strip protocols from traffic. Removing these labeling or tagging protocols allows the packets to be more easily filtered and load-balanced. PFOS provides the following stripping options:



Feature	Description	Support
<b>VLAN Tag (Ingress)</b>	You can enable or disable ingress VLAN tag stripping on a per-port basis. When this capability is enabled and a VLAN tag is present, it will be stripped from the traffic associated with the ingress port. Refer to <a href="#">Configure Standard VLAN Tag Stripping (Ingress)</a> for configuration details.	PFS 5000 Series  PFS 7000 Series
<b>Egress VLAN Tag</b>	You can enable or disable Egress VLAN tag stripping on a per-port basis. When this capability is enabled and a VLAN tag is present, it will be stripped from the traffic associated with the egress port. Refer to <a href="#">Configure Standard Egress VLAN Tag Stripping</a> for configuration details.  <b>Notes:</b> <ul style="list-style-type: none"><li>• Egress VLAN stripping is not supported for tunnel (VxLAN/L2GRE) terminated packets because tunnel termination only deletes the outer VLAN tag (PVID) and not the inner VLAN.</li><li>• To remove a specific set of VLAN IDs from an inline monitor egress port, refer to <a href="#">Inline Monitor Egress VLAN Stripping</a>.</li></ul>	PFS 5000 Series (except PFS 503x and PFS 504x)  PFS 7000 Series (except PFS 703x and PFS 704x)
<b>Vn Tag</b>	You can enable or disable Vn tag stripping on a per-port basis. When this capability is enabled and a Vn tag is present, it will be stripped from the traffic associated with the port. Refer to <a href="#">Configure Standard Vn Tag Stripping</a> for configuration details.	PFS 5000 Series (except PFS 503x and PFS 504x)  PFS 7000 Series (except PFS 703x and PFS 704x)
<b>VXLAN</b>	You can enable or disable VXLAN stripping (which performs de-encapsulation of the original packet from VXLAN tunnel encapsulation) on a per-port basis. Refer to <a href="#">Configure Standard VXLAN Stripping</a> for configuration details.  <b>Note:</b> PFOS does not support both VXLAN and MPLS stripping on the same port; you must configure VXLAN and MPLS stripping on separate ports.	PFS 5000 Series  PFS 7000 Series



Feature	Description	Support
MPLS	<p><i>This feature requires the PFS 7000 functionality license. You must enable the <a href="#">Features MPLS option in Global Settings</a> before you can use this feature.</i></p> <p>You can enable or disable MPLS stripping on a per-port basis. MPLS transports L3 packets (IP over MPLS) or L2 packets (Ethernet over MPLS). Once enabled, PFOS automatically defines MPLS labels based on incoming traffic. Users can also define custom MPLS labels. Refer to <a href="#">Configure Standard MPLS Stripping</a> for configuration details.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"><li>PFOS does not support both MPLS and VxLAN stripping on the same port; you must configure MPLS and VxLAN stripping on separate ports.</li><li>PFOS does not support both MPLS and L2GRE stripping on the same port; you must configure MPLS and L2GRE stripping on separate ports.</li></ul>	PFS 7000 Series (except PFS 704x)
L2GRE	<p><i>This feature requires the PFS 7000 functionality license.</i></p> <p>You can enable or disable L2GRE stripping (which performs de-encapsulation of the original packet from L2GRE tunnel encapsulation) on a per-port basis. Refer to <a href="#">Configure Standard L2GRE Stripping</a> for configuration details.</p> <p><b>Note:</b> PFOS does not support both L2GRE and MPLS stripping on the same port; you must configure L2GRE and MPLS stripping on separate ports.</p>	PFS 7000 Series (except PFS 704x)

## Standard Stripping Port Class Compatibility

The following table shows the availability of each stripping option on various port classes:

	Span	Monitor	Service	pStack	Span-Monitor	Inline Network	Inline Monitor
VLAN tag stripping (Ingress)	Yes	No	Yes	No	Yes	No	No
Egress VLAN tag stripping	No	Yes	Yes	No	Yes	No	Yes <sup>[3]</sup>
Vn tag stripping	Yes	Yes	Yes	No	Yes	No	No
VXLAN stripping	Yes	No	Yes	No	Yes	No	No
MPLS	Yes <sup>[1]</sup>	No	Yes <sup>[2]</sup>	No	Yes <sup>[1]</sup>	No	No
L2GRE	Yes	No	Yes	No	Yes	No	No

[1] Due to hardware limitations, Span and Span-Monitor ports can strip either 1 or 2 MPLS labels on PFS 7000 platforms except the PFS 7120 which can strip up to 3 MPLS labels when MPLS label values are not manually configured (or 1 or 2 labels when the label values are manually configured).



[2] Stripping more than 2 MPLS labels on packets is supported on Service ports. PFOS processes the packet through the service port several times until the last known MPLS label is removed. This additional processing requires additional bandwidth for service ports. For example, a packet with 8 labels will be processed through the service port 8+1 times; so for 1G of 8 MPLS label packets, 9G of bandwidth is required.

[3] Inline Monitor ports support a different type of Egress VLAN stripping that removes a specific set of VLAN IDs from egress traffic; refer to [Inline Monitor Egress VLAN Stripping](#).

### Configure Standard VLAN Tag Stripping (Ingress)

When you enable VLAN stripping on a PFS 5000/7000 Series port, the first one or two (the default) VLAN tags are stripped from the packets when the outer TPID matches 0x88A8, 0x8100, or 0x9100. (The inner TPID is fixed at 0x8100.)

Perform the following steps to configure ingress VLAN tag stripping.

1. Go to the Port Settings page for the ingress port on which you want to configure VLAN tag stripping.
2. Scroll down to the **Stripping** section.
3. Select or deselect **VLAN Tag** as desired.
4. In the Count field, enter either **1** or **2** (the default) for the number of VLAN tags to strip.

The screenshot shows the 'Stripping' configuration section. It includes a 'Vlan Tag' checkbox (which is checked by default) and a 'Count' input field set to '2'. Both the checkbox and the input field are circled in red.

5. Click **Apply** in the toolbar to save the settings to the running configuration.

### Configure Standard Egress VLAN Tag 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 [Inline Monitor Egress VLAN Stripping](#).

Perform the following steps to configure egress VLAN tag stripping.

1. Go to the Port Settings page for the egress port on which you want to configure Egress VLAN tag stripping.
2. Scroll down to the **Stripping** section.
3. Select or deselect **Egress VLAN Tag** as desired.



#### ▲ Stripping

Vlan Tag	<input type="checkbox"/>	<b>Default: disable</b> Select to enable ingress VLAN tag stripping
Egress Vlan Tag	<input checked="" type="checkbox"/>	<b>Default: disable</b> Select to enable egress VLAN tag stripping
Vn Tag	<input type="checkbox"/>	<b>Default: disable</b> Select to enable VN tag stripping
VxLAN	<input type="checkbox"/>	<b>Default: disable</b> Select to enable VxLAN tag stripping
L2GRE	<input type="checkbox"/>	<b>Default: disable</b> Select to enable L2GRE stripping

- Click **Apply** in the toolbar to save the settings to the running configuration.

### Configure Standard Vn Tag Stripping

**Note:** The PFS 503x/703x and PFS 504x/704x devices do not support Vn Tag stripping.

Perform the following steps to configure Vn tag stripping.

- Go to the Port Settings page for the port on which you want to configure Vn tag stripping.
- Scroll down to the Stripping section.
- Select or deselect **Vn Tag** as desired.
- Click **Apply** in the toolbar to save the settings to the running configuration.

#### ▲ Stripping

Vlan Tag	<input type="checkbox"/>	<b>Default: disable</b> Select to enable VLAN tag stripping
Vn Tag	<input type="checkbox"/>	<b>Default: disable</b> Select to enable VN tag stripping
VxLAN	<input type="checkbox"/>	<b>Default: disable</b> Select to enable VxLAN tag stripping
L2GRE	<input type="checkbox"/>	<b>Default: disable</b> Select to enable L2GRE stripping
MPLS	<input type="checkbox"/>	<b>Default: disable</b> Select to enable MPLS stripping



## Configure Standard VXLAN Stripping

**Note:** PFOS does not support both VxLAN and MPLS stripping on the same port; you must configure VxLAN and MPLS stripping on separate ports.

VXLAN stripping is a two-part configuration:

- Configure a set of VTEP addresses, UDP ports, and VNIDs.
- Configure the desired port(s) to enable or disable VXLAN stripping.

Perform the following steps to configure VXLAN stripping.

1. On the Applications page, click the **Standard Stripping** tab.
2. Configure parameters as desired for VxLAN stripping:
  - **Vtep address:** One or more VTEP addresses in CIDR format: IP/prefix. Up to 1024 VTEP addresses (input either as an individual address or one or more ranges of addresses). This field is for **outer IP Destination** address.
  - **UDP Port:** UDP port number to use, usually either 4789 or 8472. This field is for **outer UDP destination** port.
  - **Vnid:** A list of VNID ranges or individual VNIDs. 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.

The screenshot shows the PFOS Applications page with the Standard Stripping tab selected. The VxLAN stripping section is active, displaying the following configuration:

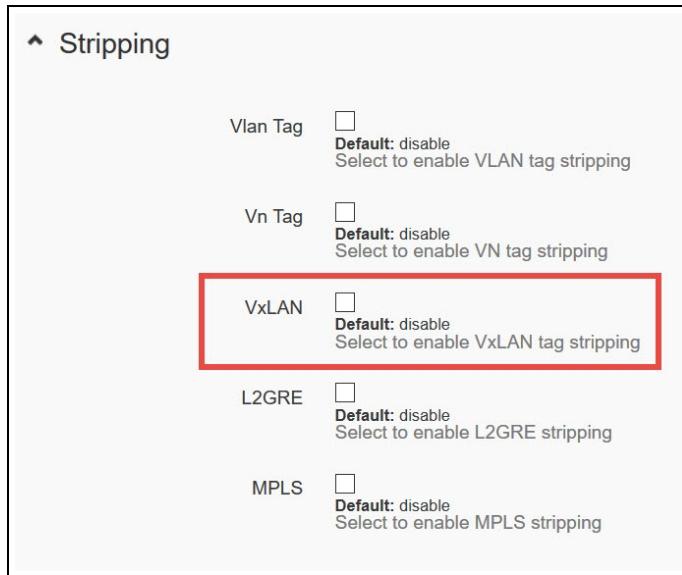
- Vtep Address: 10.20.30.0/24 (VTEP address)
- UDP Port: 4789 (Default: 4789, Valid values: 1024—65535, UDP destination port)
- Vnid: 400-500 (VNID or range of VNIDs (allowed range:1 ... 16...))
- Vteps Configured Count: 256 (Default: 0, Number of VTEPs currently configured)
- Vnids Configured Count: 101 (Default: 0, Number of VNIDs currently configured)

**Note:** You can view counts of VTEP configured IP addresses and VNIDs. CIDR enables a single IP address to be used to designate many unique IP addresses. For example, an IP address using "/24" designates 256 IP addresses while an IP address using "/32" designates only 1 IP address.

3. Go to the Port Settings page for the port on which you want to configure VXLAN stripping.
4. Scroll down to the Stripping section.



5. Select or deselect **VxLAN** as desired.
6. Click **Apply** in the toolbar to save the settings to the running configuration.



### Standard VXLAN Stripping Limitations and Considerations

- For VXLAN-stripped packets, filtering and/or load-balancing cannot be applied on the same port. The unfiltered traffic must be redirected to a service port, where it can be filtered and/or load-balanced.
- IPv6 addresses are not supported in VXLAN stripping.
- VLAN stripping will be enabled internally when VXLAN stripping is enabled.
- Source port VLAN tagging for the inner packet (payload of a VXLAN packet) cannot be done. Instead, the de-encapsulated packet must be sent to a Service port, where source port VLAN tagging can be performed.
- Packets which have been stripped of VXLAN headers cannot be sent directly to remote (pfsMesh) destinations. In order to forward stripped traffic to a remote port group via pfsMesh, a Service port and 2 traffic maps are necessary:
  - Map #1 – from a Span port where the stripping is performed to a Service port;
  - Map #2 – from the Service port to a remote monitor port group.
- PFOS does not support both VXLAN and MPLS stripping on the same port; you must configure VXLAN and MPLS stripping on separate ports.
- Up to 1024 VNID values (input either as individual values or in a range) can be configured per PFS
- 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.
- VXLAN stripping function does not work on VXLAN packets with More Fragments (MF) flag bit set to 1 or the outer source IP is a multicast address.



## Configure Standard MPLS Stripping

### Notes:

- This feature requires the PFS 7000 functionality license. You must enable the [Features MPLS option in Global Settings](#) before you can use this feature.
- The PFS 704x devices do not support MPLS stripping.
- PFOS does not support both MPLS and VxLAN stripping on the same port; you must configure MPLS and VxLAN stripping on separate ports.
- PFOS does not support both MPLS and L2GRE stripping on the same port; you must configure MPLS and L2GRE stripping on separate ports.

MPLS stripping supports both L3 (IP over MPLS) and L2 (Ethernet over MPLS) and is enabled/disabled on a per-port basis.

Once enabled, PFOS automatically defines MPLS labels based on incoming traffic. Users can also define additional custom MPLS labels. Refer to the following sections for details:

- [Enable MPLS Stripping](#)
- [Configure Additional User-Defined MPLS Labels](#)
- [Clear Programmed MPLS Labels Manually](#)
- [Standard MPLS Stripping Limitations and Considerations](#)

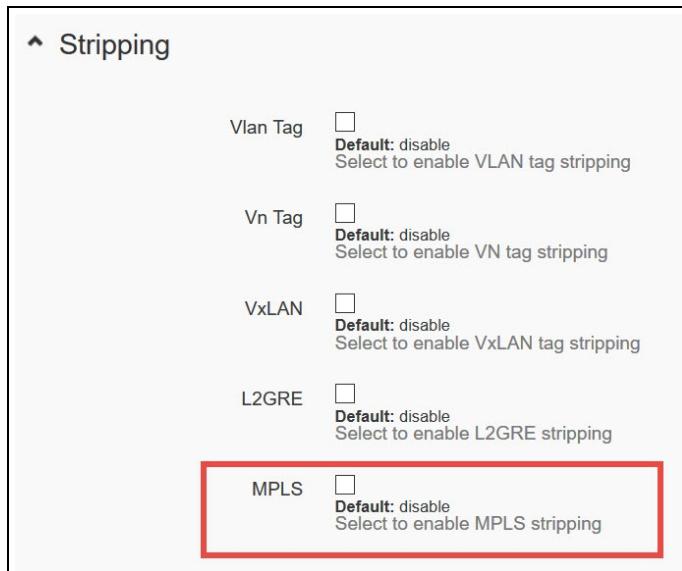
### Enable MPLS Stripping

You enable MPLS Stripping on a per-port basis. Once enabled, PFOS automatically defines MPLS labels based on incoming traffic. By default, PFOS can define up to 1024 entries. You can modify this value; refer to [MPLS Max Labels](#).

1. Go to the Port Settings page for the port on which you want to configure MPLS stripping.
2. Scroll down to the Stripping section.



3. Select **MPLS** to enable L3 MPLS stripping. Two additional fields appear:
  - Select **L2 MPLS** to enable L2 MPLS stripping.
  - **Unstrippable MPLS Destination** - On Span/Span-Monitor ports, 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. This option is not available on Service ports. If not configured, the unstrippable packets will be dropped.



4. Click **Apply** in the toolbar to save the settings to the running configuration.

### Configure Additional User-Defined MPLS Labels

Once MPLS Standard Stripping is [enabled](#), PFOS automatically defines MPLS labels based on incoming traffic. Users can also define custom MPLS labels. Perform the following to define additional MPLS labels.

1. On the Applications page, click the **Standard Stripping** tab.
2. Scroll down and select the MPLS option to display the MPLS page.



## Applications

Tunnel Termination   Healthcheck   Standard Stripping

**Vxlan** VXLAN stripping application library

Vtep Address	<input type="button" value="Add an entry ..."/>	UDP Port	4789
VTEP address		Default: 4789 Valid values: 1024—65535 UDP destination port	
Vteps Configured Count	0	Vnids Configured Count	0
Default: 0 Number of VTEPs currently configured		Default: 0 Number of VNIDs currently configured	

**L2GRE** L2GRE stripping application library

Destination Address	<input type="button" value="Add an entry ..."/>	L 2gre ID	<input type="button" value="Add an entry ..."/>
destination address		L2GRE ID or range of L2GRE ID (allowed range 1...)	
L 2gre Configured ID	0	L 2gre Configured Address	0
Default: 0 Number of L2GRE ID currently configured		Default: 0 Number of L2GRE address currently configured	

**MPLS** MPLS stripping application library

MPLS	MPLS stripping application library
------	------------------------------------

3. If configuring L3 (IP over MPLS) stripping, configure tunnel labels:
  - a. Click **Add an entry...**
  - b. Enter a valid tunnel value (between 16 and 1048575; 0 to 15 are reserved), a range of values (for example, 16-200), or a combination of both. **CAUTION: If label value ranges overlap between Tunnel/L3 and L2 label list, packets will be sent to the Unstripable MPLS Destination.**
  - c. Click **Add**.

## MPLS

Tunnel Label	<input type="button" value="Add an entry ..."/>	<input type="text"/>
Tunnel label(0 .. 1048575)		
<input type="button" value="Update"/> <input type="button" value="Add"/> <input type="button" value="Cancel"/>		



4. If configuring L2 (Ethernet over MPLS) stripping, configure L2 MPLS labels:
  - a. Click the **Add** button.

The screenshot shows the 'MPLS' configuration interface. At the top, there's a 'Tunnel Label' field with a 'Tunnel label(0 ... 1048575)' placeholder. Below it are 'Update', 'Add', and 'Cancel' buttons. Underneath is a table header 'L 2 Mpls Labels VPWS/VPLS label list'. The table has columns 'Label' and 'Pwc'. A single row is present with a 'Label' value of '1200' and a 'Pwc' value of 'Pvc'. At the bottom of the table area, there are 'Add' and 'Delete' buttons, with the 'Add' button being circled in red.

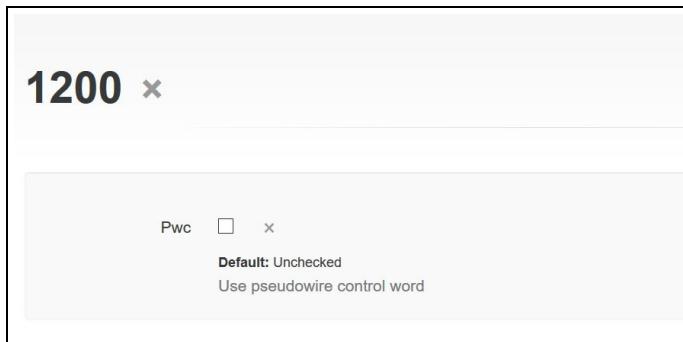
- b. On the **Add new L2 MPLS Labels** page, enter a valid L2 label value (between 16 and 1048575; 0 to 15 are reserved), a range of values (for example, 201-400), or a combination of both. **CAUTION: If label value ranges overlap between the Tunnel/L3 and the L2 label list, packets will be sent to the Unstripable MPLS Destination.**

The screenshot shows the 'Add new L2 Mpls Labels' configuration interface. It has a header 'Add new L 2 Mpls Labels VPWS/VPLS label list'. Below is a table with a single row. The first column is 'Label \*' with a value of '1200' and a note 'L2 label(0 ... 1048575)'. At the bottom are 'Add' and 'Cancel' buttons.

**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](#) setting in the next step).



- c. Select or deselect **Pwc** to indicate whether or not incoming packets will have a pseudowire control word. **CAUTION: If the Pwc configuration on the L2 label does not match the packets then the packets will be corrupted before being delivered to the destination port.**



**Note:** The bottom of the MPLS page enables you to view counts of L2 MPLS labels and Tunnel labels. The following graphic shows example counts when ranges of labels have been configured.

The screenshot shows the PFOS MPLS configuration page. At the top, there are two input fields for Tunnel Labels: one containing "100-200" and another containing "1-10". Below these is a note: "Tunnel label(0 .. 1048575)". Under the heading "L 2 Mpls Labels" is a table with one entry: "Label: 300-500, Pwc: true". To the right of the table is a note: "Showing 1 to 1 of 1". At the bottom of the page, there are two summary sections: "L 2mpls Label Configured Count" (201, Default: 0) and "Tunnel Label Configured Count" (101, Default: 0). A red box highlights the "L 2mpls Label Configured Count" section.

### Clear Programmed MPLS Labels Manually

PFOS automatically defines MPLS labels based on incoming traffic. By default, PFOS can define up to 1024 entries (you can modify this value; refer to [MPLS Max Labels](#)).

If the number of programmed MPLS labels reaches the maximum allocated MPLS entries, they can be cleared manually by accessing the **Stripping** option under the Status side menu (see graphic below). Clicking the **Clear** button clears the MPLS labels. You can also use the CLI command `stripping clear mpls` to perform the same function; refer to the [PFOS CLI Reference Guide](#) for details. Once cleared, PFOS relearns MPLS labels from incoming traffic.

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



The screenshot shows the NETSCOUT Stripping configuration interface. On the left, there's a navigation sidebar with sections like Status, Configuration, and Stripping. The 'Stripping' section is currently selected and highlighted with a red box. The main area is titled 'Stripping Dynamic stripping information' and contains a 'MPLS' tab. Below the tabs, there's a table header for 'MPLS dynamic stripping MPLS label info' with columns for 'Port', 'Label', and 'Type'. A note at the bottom right of the table says 'Table is empty'.

PFOS can be configured to automatically clear the programmed MPLS labels when they reach their maximum allocated limit; see [Configuring the System and Ports](#) for cleanup mode details.

### Standard MPLS Stripping Limitations and Considerations

- On a Service port, MPLS labels will be removed until either it reaches the Bottom-of-Stack (BOS) bit or non-matched MPLS labels.
- PFOS cannot remove an MPLS label if the MPLS Label=0. When a packet has multiple MPLS labels, including a 0 label, PFOS MPLS stripping will only remove the labels *prior* to the 0 label. The 0 label and other labels after the 0 label are not removed.
- The [Unstrippable MPLS destination](#) is always a port and not a Load-balancing Group (LBG).
- PFOS does not support both MPLS and VxLAN stripping on the same port; you must configure MPLS and VxLAN stripping on separate ports.
- PFOS does not support both MPLS and L2GRE stripping on the same port; you must configure MPLS and L2GRE stripping on separate ports.
- Router Alert Label has a specific purpose and the receiving router is required to perform specific operations. Since PFS is not part of LSPs (Label Switched Path) PFS does not support stripping of Router Alert Labels.
- Enabling L2 MPLS stripping and VN tag stripping on a same port results in packet corruption.
- MPLS stripping will not work for double VLAN tagged packets.
- IP over MPLS Maximum Entries: By default, PFOS supports 1024 MPLS entries (you can modify this value; refer to [MPLS Max Labels](#)). The number of ports MPLS can be enabled on depends upon how many tunnel labels are created and vice versa. For example, if the user configures 1000 tunnel labels, then MPLS stripping can be enabled on 1 port. If the user configures 500 tunnel labels, then MPLS stripping can be enabled on 2 ports and so on.
- Ethernet over MPLS Maximum Entries: The number of L2 labels that can be created depends on the number of ports on which L2 MPLS is enabled and vice versa. You can configure the maximum number of MPLS labels that PFOS supports; refer to [MPLS Max Labels](#) for details.
- 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 [Step 4](#)).
- To apply IP address filters on L2/L3 MPLS packets, the system [Map Profile](#) must be configured as Legacy mode.



- Filter expressions can normally work at a SPAN port with MPLS stripping enabled to filter packets after they are stripped. However, the following limitations are applied:
  - EType filter will be always applied to packets before stripping.
  - Source IP filter will be applied to packets before stripping when Map Profile is set to SIP mode.
  - Destination IP filter will be applied to packets before stripping when Map Profile is set to DIP mode.

For example, to apply IPv6 source or destination IP filter on a SPAN port with MPLS stripping enabled:

- Set Map Profile as Legacy mode.
- Configure source or destination IPv6 address filter without using EType (0x86DD).

```
feature map-profile legacy
filter IPv6
expression "( IP Dest 2001:0568:FFFF:2025:0000:0000:0000:0000
mask FFFF:FFFF:FFFF:FFFF:0000:0000:0000:0000 or IP Source
2001:0568:FFFF:2025:0000:0000:0000:0000 mask
FFFF:FFFF:FFFF:FFFF:0000:0000:0000:0000 )"
!
```

## Configure Standard L2GRE Stripping

### Notes:

- This feature requires the PFS 7000 functionality license.
- 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.

L2GRE stripping is a two-part configuration:

- Configure a set of destination IP addresses and L2GRE IDs.
- Configure the desired port(s) to enable or disable L2GRE stripping.

Perform the following steps to configure L2GRE stripping.

1. On the Applications page, click the **Standard Stripping** tab. Scroll down to the L2GRE section.
2. Configure parameters for L2GRE stripping:
  - **Destination address:** One or more IP addresses in CIDR format: IP/prefix.
  - **L2GRE ID:** A list of L2GRE ID ranges or individual L2GRE IDs. 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. **Note:** PFS 7030s and PFS 7031s support



an L2GRE ID value of 0.

Destination Address	L 2gre ID
10.20.10.0/24	100
10.10.30.0/24	200
10.10.10.10/32	300

destination address

L 2gre Configured Address	L 2gre Configured ID
513	4

Default: 0  
Number of L2GRE Destination address currently ...

Default: 0  
Number of L2GRE ID currently configured

**Note:** You can view counts of L2GRE configured IP addresses and IDs. CIDR enables a single IP address to be used to designate many unique IP addresses. For example, an IP address using "/24" designates 256 IP addresses while an IP address using "/32" designates only 1 IP address.

3. Go to the Port Settings page for the port on which you want to configure L2GRE stripping.
4. Scroll down to the Stripping section, and select **L2GRE**.
5. Click **Apply** in the toolbar to save the settings to the running configuration.

Stripping Type	Enabled	Description
Vlan Tag	<input type="checkbox"/>	Default: disable Select to enable VLAN tag stripping
Vn Tag	<input type="checkbox"/>	Default: disable Select to enable VN tag stripping
VxLAN	<input type="checkbox"/>	Default: disable Select to enable VxLAN tag stripping
L2GRE	<input type="checkbox"/>	Default: disable Select to enable L2GRE stripping
MPLS	<input type="checkbox"/>	Default: disable Select to enable MPLS stripping

### Standard L2GRE Stripping Limitations and Considerations

- For L2GRE-stripped packets, filtering and/or load-balancing cannot be applied on the same port. The unfiltered traffic must be redirected to a service port, where it can be filtered and/or load-balanced.
- IPv6 addresses are not supported in L2GRE stripping.
- VLAN stripping will be enabled internally when L2GRE stripping is enabled.
- Source port VLAN tagging for the inner packet (payload of an L2GRE packet) cannot be done. Instead, the de-encapsulated packet must be sent to a Service port, where source port VLAN tagging can be performed.



- Packets which have been stripped of L2GRE headers cannot be sent directly to remote (pfsMesh) destinations. In order to forward stripped traffic to a remote port group via pfsMesh, a Service port and two traffic maps are necessary:
  - Map #1 – from a Span port where the stripping is performed to a Service port;
  - Map #2 – from the Service port to a remote monitor port group.
- Up to 1024 L2GRE ID values (input either as individual values or in a range) can be configured per PFS.
- PFOS does not support both L2GRE and MPLS stripping on the same port; you must configure L2GRE and MPLS stripping on separate ports.
- L2GRE stripping function does not work on L2GRE packets with More Fragments (MF) flag bit set to 1 or the outer source IP is a multicast address.

## Inline Monitor Egress VLAN Stripping

**Note: This feature requires the PFS 7000 functionality license. The PFS 704x-32D devices do not support Inline Monitor Egress VLAN Stripping.**

PFOS supports an option for Inline Monitor ports to strip specific VLANs from PFS egress traffic. The Applications>Egress VLAN Action page enables you to create a profile 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
- Each PFS Device supports a total of 8 Egress VLAN Action groups.

Inline Monitor Egress VLAN Stripping is a three-part configuration:

- Create an Egress VLAN Action Group.
- Assign the Egress VLAN Action Group to an Inline Monitor port.
- Create a notification for the Egress VLAN Action group.

### Configure an Egress VLAN Action Group

Perform the following steps to configure an Egress VLAN Action Group:

1. Create the Egress VLAN Action Group:
  - a. Open the **Applications>Egress VLAN Action** page and click **Add**.
  - b. On the Add New Group page, enter a name to identify the Egress VLAN Action group and click **Add**. A new VLAN page opens for you to add VLAN IDs to the group.
  - c. Click **Add**, enter a VLAN ID (1-4094), and click **Add** to add to the group. If adding multiple VLAN IDs to the group, repeat this step until all VLAN IDs are added (maximum 16).
  - d. Click **Apply**.



2. Assign the Egress VLAN Action Group to an Inline Monitor port:
  - a. Open the **Port Settings** page and click the Inline Monitor port link you want.
  - b. In the **Egress VLAN Action Library** field, select the name of the Egress VLAN Action group you want to assign to this port.

**Note:** You can also [configure a notification](#) for the Egress VLAN Action on the Notifications>Events>Config Notification page. An egress-vlan-action option is available for you to select the Notifications you want.

## PFS 7000 Timestamping

**Note:** This feature is only available on PFS 7120, PFS 7121-64X, PFS 703x-32X, PFS 7030-54X, PFS 7031-56X, and the PFS 704x-32D devices.

The timestamping feature appends packet arrival and departure information in a 48-bit time stamp at the end of the data payload of each packet. Packet timestamping information allows users to:

- Monitor real-time application/flow performance
- Measure latency of flow
- Detect network congestion
- Validate sequence of arrival at a service point (such as a switch ingress port)

Timestamping can be enabled on a per port basis either in Ingress (RX), Egress (TX), or both directions for the following port-class types:

**Note:** Time stamping and [IP Tunnel Termination](#) cannot be enabled on the same port.

**Table 5.1 - Supported Time Stamp Directions**

Class-type	Direction	
	RX	TX
Span	Yes	No
Monitor	No	Yes
Span-Monitor	Yes	Yes
Service	Yes	Yes

### Time Stamp Details

- Timestamps are added to the end of a frame; the timestamp consists of a count of seconds and nanoseconds (see below for details). The timestamp is relative to some arbitrary time in the past; the time is not related to the time of day.
- A maximum of two timestamp values can be inserted per packet:
  - Ingress time
  - Egress time

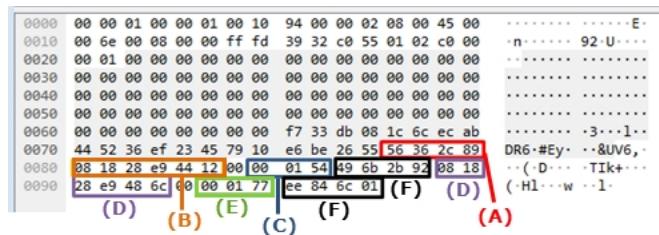


The meta-data record (14 bytes) that is included at the end of frame is called TS\_SHIM. The existing Ethernet CRC is skipped and new CRC is appended at the end. To keep all timestamp insertions uniform, every timestamp record will have four bytes of overhead. The last TS\_SHIM record gets a new Frame Check Sequence (FCS) placed over these 4 bytes. The following table describes the TS\_SHIM format:

Field	1 Bit Pos	Width	Position
time_0_47	0	48b	48-bit timestamp (18b sec + 30b nanosecond)
reserved_0	48	8b	Unused byte
origin_id	56	23b	Origin ID (configured by user on port - see Step 3 in <a href="#">Enable Time Stamping</a> )
rx_tx	79	1b	Direction (0=Rx, 1=Tx)
reserved_1	80	32b	Place holder for FCS if last SHIM else unused

## Time Stamp Example

The following diagram shows a time stamp example:



- The **(A) RED BOX** is the original 4 Bytes of FCS.
- The **(B) ORANGE BOX** is the 6 Bytes of RX Timestamp.
- The **(C) BLUE BOX** is the 3 Bytes of RX Origin ID and Direction
- The **(D) PURPLE BOXES** is the 6 Bytes of TX Timestamp.
- The **(E) GREEN BOX** is the 3 Bytes of TX Origin ID and Direction
- The **(F) BLACK BOXES** are the 4 Bytes of RX and TX FCS.

## Enable Time Stamping

1. Go to the Port Settings page and select the port on which you want to configure time stamping.
2. Scroll until you find the Timestamp option(s) and click the **Rx** and/or **Tx** checkboxes to enable them ([supported Time Stamp Direction options](#) vary depending on the port type). When enabled, an ID field appears.

**Note:** Time stamping and [IP Tunnel Termination](#) cannot be enabled on the same port.

3. Enter a unique ID to be included in the timestamp; valid values are 0-8388607.
4. Click **Apply** in the toolbar to save the settings to the running configuration.



## L2GRE Tunnel Origination/Termination Support

**Note:** This feature requires the PFS 7000 functionality license.

PFOS supports Layer-2 Generic Routing Encapsulation (L2GRE) protocol. L2GRE provides a private, secure path for transporting packets through an otherwise public network by encapsulating (or tunneling) the packets.

PFS devices encapsulate packet payload for transport through the tunnel to a destination network. The Layer-2 packets are first encapsulated in a GRE header, and then the GRE packet is encapsulated in an IP header. The remote tunnel destination extracts the tunneled packet and forwards the packet to its destination. This allows the tunnel origination and destination points to operate as if they have a virtual point-to-point connection with each other.

Because GRE headers are added to frames sent over the GRE tunnel, the tunnel's transport network MTU should be large enough to hold the largest monitored frame plus the tunnel headers.

**Note:** PFS 7000 will not fragment nor reassemble oversized frames.

PFOS supports the following L2GRE use cases:

- [L2GRE Tunnel between Two PFS 7000 Devices](#)
- [L2GRE Tunnel from PFS to vSTREAMs](#)

Refer to [Configuring L2GRE Tunnel Origination/Termination](#) for workflow details. **Review the L2GRE Origination/Termination Limitations prior to configuring L2GRE Tunnel Origination/Termination.**

**Note:** There is a maximum of 1024 GRE tunnels per chassis.

### Configuring L2GRE Tunnel Origination/Termination

**Note:** The [Features Tunnel option](#) in Global Settings must be enabled before you can use this feature.

Use the following procedure to configure L2GRE Tunnel Origination/Termination. Refer to the [PFOS CLI Reference Guide](#) for CLI command details. **Review the L2GRE Origination/Termination Limitations prior to configuring L2GRE Tunnel Origination/Termination.**

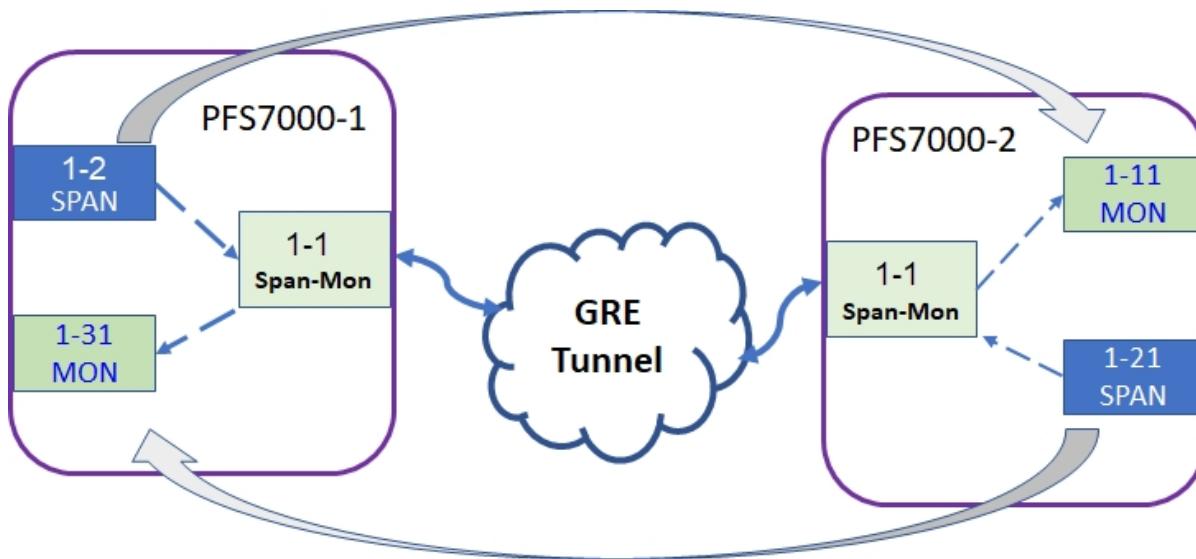
Step	Web UI	CLI
<b>1 Configure Ports</b> Configure a port that is connected to the IP network as Span-Monitor.	Port Settings Page	interface command
<b>2 Configure IP Interface</b> Configure the Source IP address for the tunnel and select the Span-Monitor port configured in Step 1 to connect to the public/private IP network.	Tunnel Settings>IP Interface Page	interface ip command



Step	Web UI	CLI
<b>3 Configure GRE Interface</b> Configure the Destination IP address for the tunnel, the IP Interface configured in Step 2, GRE Tunnel Key, and Gateway.	Tunnel Settings>GRE Interface Page	interface gre command
<b>4 Configure Traffic Map for the Tunnel</b> <b>Note:</b> PFOS does not support both input tunnels and output tunnels in the same map.	Traffic Maps	Refer to Map Commands for GRE Tunnel Origination/Termination

### Use Case 1 - L2GRE Tunnel between Two PFS 7000 Devices

In this scenario, two PFS 7000 devices are connected via a public/private IP network. The first PFS applies filtering, encapsulates the traffic with an L2GRE header, and sends the filtered traffic to the second PFS 7000. The second PFS 7000 receives the tunneled traffic, de-encapsulates it (removing the L2GRE header) and forwards the traffic to the monitor port. In this example the tunnel is bidirectional so traffic can also flow in the opposite direction.



Perform the following procedures to configure GRE Tunnel Origination/Termination for this scenario:

- [Configure Ports](#)
- [Configure IP Interface](#)
- [Configure GRE Interface](#)
- [Configure Traffic Map for the Tunnel](#)

**Note:** The configuration in this example is based on PFS 7120.

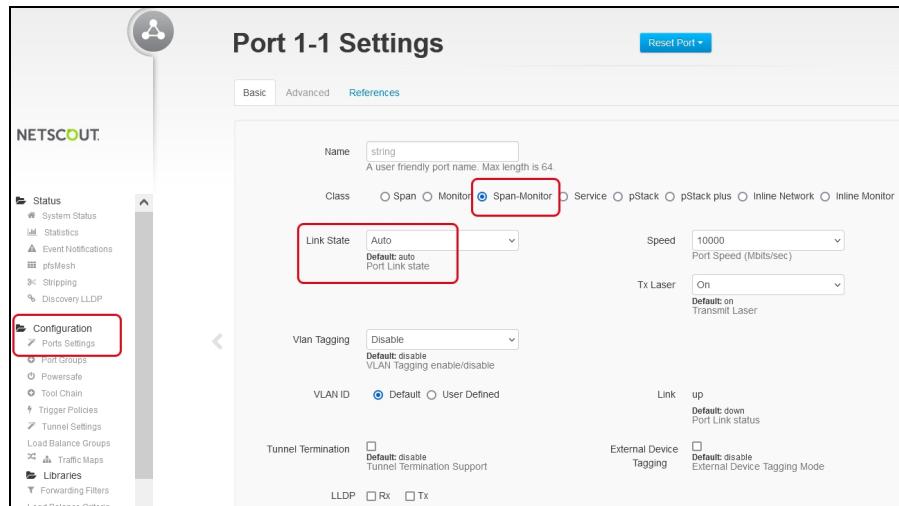
Once configured, see [L2GRE Tunnel Statistics and Status](#) for status details.



## Configure Ports

Configure port 1-1 on each PFS 7000 that will be used to connect to the IP network.

1. On the Configuration > Port Settings page, click a port ID link to display the settings for the port.
2. Configure Basic settings.
  - a. Select **Span-Monitor** as the Port Class.
  - b. Select **Auto** as the Link State.
3. Click **Apply** in the Toolbar to save the changes to the running configuration.



## Configure IP Interface

Configure the Source IP address for the tunnel and select the Span-Monitor port configured in previous section to connect to the public/private IP network.

1. On the Configuration > Tunnel Settings page, select the **IP Interface** tab.
2. Click the **Add** button to add a new IP interface. Enter a name for the interface (example uses IP\_interface\_1112) and click the **Add** button. The interface settings page for the new IP interface appears.
3. In the **Address** field, enter the Source IP address for the tunnel (example uses 1.1.1.2).
4. In the **Interface** area, click the **Select Port** drop down menu and select the previously configured Span-Monitor port (Port 1-1 in [Configure Ports](#)) to connect to the public/private IP network.
5. Click **Apply** in the Toolbar to save the changes to the running configuration.



IP\_interface\_1112 ×

Address *	1.1.1.2	IP Address	State up
		Default: down	
IP Interface Link State			
Interface			
Select Port			
Port	1-1	Configure IP Interface on port	

### CLI Configuration

```
PFS7120(config)# interface ip IP_interface_1112 address 1.1.1.2
port 1-1
```

### Show IP Interface on Chosen L2GRE Tunnel Ports

View IP Interface Settings on the Configuration > Tunnel Settings > IP Interface page.

NETSCOUT.

Tunnel Settings

IP Interface GRE VLAN

Add ... Delete

Name	Address	State	Port
IP_interface_1112	1.1.1.2	up	1-1
IP_interface_1-9	1.1.1.9	up	1-9
IP_interface_1-49	1.1.1.49	up	1-49

Showing 1 to 3 of 3

**Note:** The State column shows the link status (Up or Down) of the port associated with the IP interface used for the tunnel.

### CLI show command:

```
PFS7120# show running-config interface ip IP_interface_1112
interface ip IP_interface_1112
address 1.1.1.2
port 1-1
```

### Configure GRE Interface

Configure the Destination IP address for the tunnel, using the IP Interface configured in the previous section, a GRE Tunnel Key, and Gateway IP address.



1. On the Configuration > Tunnel Settings page, select the **GRE Interface** tab.
2. Click the **Add** button to add a new GRE interface. Enter a name for the interface (example uses `gre_tunnel_1113`) and click the **Add** button. The interface settings page for the new GRE interface appears.
3. In the **Source** field, select the previously configured IP interface (`IP_interface_1112` in [Configure IP Interface](#)).
4. In the **Address** field, enter the Destination IP address for the tunnel (example shows `1.1.1.3`).
5. In the **Key** field, define an L2GRE key to be used to identify packets on the tunnel. Valid values are 1 to 268435455 (example shows 1233). **Note:** PFS 7030s and PFS 7031s also support an L2GRE key value of 0.
6. Configure Gateway, if applicable:
  - When the destination is **local**, do not configure a **Gateway** to avoid possible network problems.

**gre\_tunnel\_1113** ×

**Local Destination**

Source * <input style="width: 20px; height: 20px; vertical-align: middle;" type="button" value="..."/> IP_interface_1112	Destination * <input type="text" value="1.1.1.3"/> Destination IP
Key * <input type="text" value="1233"/> <small>Valid values: 0—268435455 L2GRE key</small>	Gateway <input type="text" value="ipv4-address"/> Gateway IP Address
Vlan Tagging <input type="button" value="No Tag"/>	<small>Default: no-tag Service Tag options for Encapsulated traffic</small>
State up	Resolved Mac 00:10:94:00:00:03
Default: down	<small>Default: 00:00:00:00:00:00 MAC Learned on this tunnel</small>
Tunnel State	

- When the destination is on a **remote** network, in the **Gateway** field, enter the local gateway IPv4 IP address for the GRE interface.

**GRE\_4444\_gateway\_1111** ×

**Remote Destination**

Source * <input style="width: 20px; height: 20px; vertical-align: middle;" type="button" value="..."/> IP_interface_1112	Destination * <input type="text" value="4.4.4.4"/> Destination IP
Key * <input type="text" value="1232"/> <small>Valid values: 0—268435455 L2GRE key</small>	Gateway <input type="text" value="1.1.1.1"/> Gateway IP Address
Vlan Tagging <input type="button" value="Ingress Tag"/>	<small>Default: no-tag Service Tag options for Encapsulated traffic</small>
State up	Resolved Mac 00:10:94:00:00:11
Default: down	<small>Default: 00:00:00:00:00:00 MAC Learned on this tunnel</small>
Tunnel State	

**Local Gateway**



7. Click **Apply** in the Toolbar to save the changes to the running configuration.

8. Confirm the tunnel State and Resolved MAC:

If the port associated with the IP Interface used for the GRE Tunnel has an "Up" link state, once the IP Interface and the GRE tunnel settings are applied, PFOS will send an ARP request to the Gateway (if configured) or to the Destination (if Gateway is not configured). PFOS GRE tunnel settings do not include a subnet mask; therefore, PFOS relies on the Gateway setting to decide if the Destination is at a remote or local subnet:

- If a Gateway **is not** configured, PFOS assumes tunnel destination at a local subnet, and sends the ARP request directly to the Destination IP address.
- If a Gateway **is** configured, PFOS assumes tunnel destination at a remote subnet, and sends the ARP request to the Gateway IP address.

Once the ARP response is received, the tunnel State at the WebUI will display "up" with a proper "Resolved Mac" address for the tunnel Gateway or Destination.

Otherwise, the tunnel State will display "mac-unresolved" or "down" with "Resolved Mac" as all "00s".

### CLI Configuration (Local)

```
PFS7120(config)# interface gre gre_tunnel_1113 source IP_interface_1112 destination 1.1.1.3 key 1233
```

### CLI Configuration (Remote)

```
PFS7120(config)# interface gre GRE_4444 gateway_1111 source IP_interface_1112 destination 4.4.4.4 key 1232 gateway 1.1.1.1
```

## Show GRE Interface on IP Interfaces

View GRE Interface Settings on the Configuration > Tunnel Settings > GRE page.

Name	Source	Destination	Key	State
GRE_tunnel-mac-unresolved	IP_interface_149	10.10.10.10	123410	mac-unresolved
GRE_3353_gateway_1111	IP_interface_1112	3.3.3.3	1231	up
GRE_4444_gateway_1111	IP_interface_1112	4.4.4.4	1232	up
GRE_9099_port49_gateway1111	IP_interface_149	9.9.9.9	12349	mac-unresolved
gre_tunnel_1113	IP_interface_1112	1.1.1.3	1233	up

**Note:** The State column shows the ARP response status, if the port associated with the IP Interface receives an ARP response from the local gateway or tunnel destination. Possible state values are:

- **down:** the default status
- **up:** the ARP response is received, and the MAC address is resolved for the local gateway IP or the local destination IP.
- **mac-unresolved:** No ARP response is received.

### CLI show command:



```
PFS7120# show running-config interface gre gre_tunnel_1113
interface gre gre_tunnel_1113
source IP_interface_1112
destination 1.1.1.3
key 1233
```

## Configure Traffic Map for the Tunnel

Configure a traffic map for the tunnel.

1. On the Configuration > Traffic Maps page, click the **Add** button to add a new traffic map.
2. Enter a name for the traffic map and click the **Add** button. The map settings page for the new map appears.
3. Add a map **Description**.
4. Select **Monitor** for map **Type**.
5. Select **Basic** for map **Mode**.
6. In the **Filter** field, select a filter or select Unfiltered for tunnel traffic. Ingress tunnels support only unfiltered traffic.

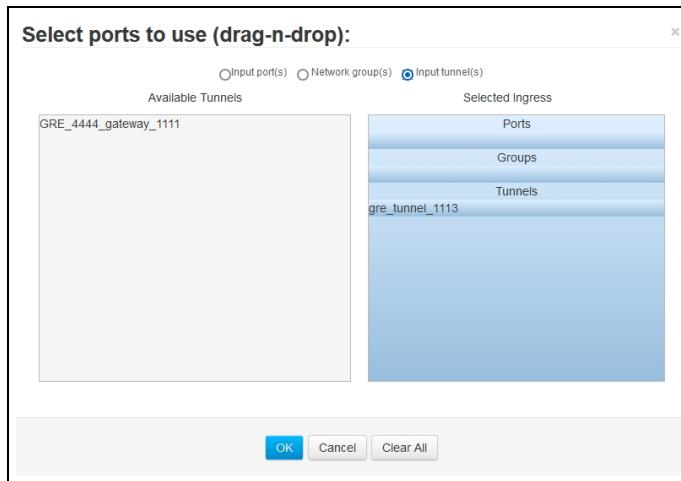
**Note:** PFOS does not support both input tunnels and output tunnels in the same map. If you configure an Input tunnel in Ingress, you must configure a port for Egress; if you configure an Output tunnel in Egress, you must configure a port for Ingress. Refer to the following sections for details:

- [Using Tunnel as Ingress](#)
- [Using Tunnel as Egress](#)

### Using Tunnel as Ingress

L2GRE packets coming to tunnels with matching Source/Destination MACs, Source/Destination IPs and GRE keys are decapsulated and forwarded to the traffic map's output ports, non-matching packets are dropped.

1. From the traffic map configuration page, click the **Ingress Configure** button. The Select Ports to Use dialog box appears.
2. Select the **Input tunnels** radio button to display the available tunnels. Drag and drop the tunnel name to the Ingress tunnel section on the right and click **OK**.



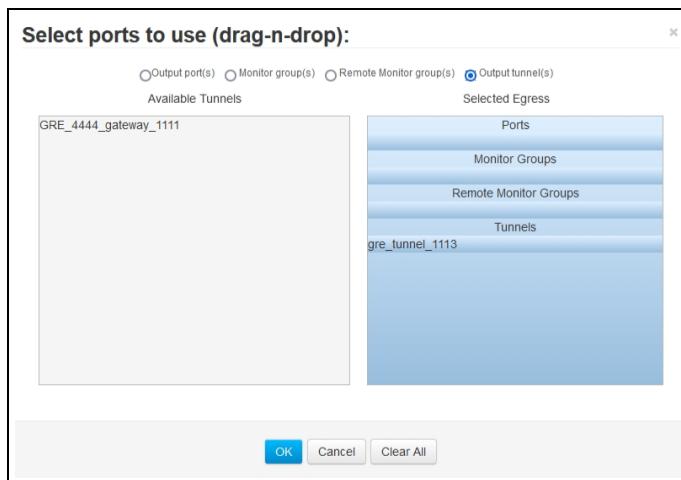
3. Click **Apply** in the Toolbar to save the changes to the running configuration.
4. Assign a filter to the map to forward matching packets to GRE tunnel interfaces.

### CLI Configuration

```
PFS7120(config)# map map_tunnels_to_port input-tunnels gre_tunnel_1113  
filter unfiltered output_ports 1-1
```

### Using Tunnel as Egress

1. From the traffic map configuration page, click the **Egress Configure** button. The Select Ports to Use dialog box appears.
2. Select the **Output tunnels** radio button to display the available tunnels. Drag and drop the tunnel name to the Egress tunnel section on the right and click **OK**.



3. Click **Apply** in the Toolbar to save the changes to the running configuration.
4. Assign a filter to the map to forward matching packets to GRE tunnel interfaces.



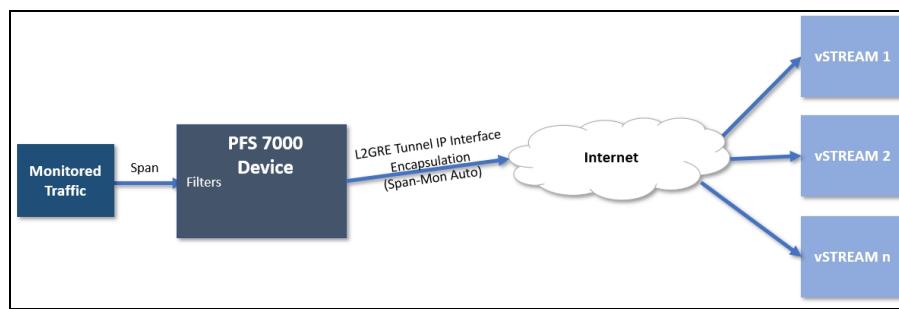
### CLI configuration

```
PFS7120(config)# map map_port_to_tunnel_1113 input_ports 1-1 filter  
IP333 output-tunnels gre_tunnel_1113
```

### Use Case 2 - L2GRE Tunnel from PFS to vSTREAMs

In this scenario:

- Monitored traffic is sent to PFS 7000 device
- Data packets are filtered and encapsulated with L2GRE headers to designated destinations, one physical port with multiple GRE interfaces to multiple vSTREAMs
- Data packets arrive at destinations for analysis



Perform the following procedures to configure GRE Tunnel Origination/Termination for this scenario:

- [Configure Ports](#)
- [Configure IP Interface](#)
- [Configure GRE Interface](#)
- [Configure Traffic Map for the Tunnel](#)

Once configured, see [L2GRE Tunnel Statistics and Status](#) for status details.

**Note:** The configuration in this example is based on PFS 7120.

### Configure Ports

Configure a port that will be used to connect to the IP network.

1. On the Configuration > Port Settings page, click a port ID link (example uses Port 1-1) to display the settings for the port.
2. Configure [Basic](#) settings.
  - a. Select **Span-Monitor** as the Port Class.
  - b. Select **Auto** as the Link State.
3. Click **Apply** in the Toolbar to save the changes to the running configuration.



The screenshot shows the NETSCOUT interface with the title "Port 1-1 Settings". On the left, there's a navigation tree under "NETSCOUT" with "Status", "Configuration" (which has "Ports Settings" selected), and "Tunnel Settings". The main panel shows port configuration details: Name (string, max length 64), Class (Span-Monitor selected), Link State (Auto), Speed (10000), Tx Laser (On), VLAN Tagging (Disable), VLAN ID (Default), Tunnel Termination (Disable), LLDP (Rx, Tx), and External Device Tagging (Disable). Buttons for "Reset Port" and "Apply" are at the top right.

## Configure IP Interface

Configure the following IP Interface settings.

1. On the Configuration > Tunnel Settings page, select the **IP Interface** tab.
2. Click the **Add** button to add a new IP interface. Enter a name for the interface (example uses IP\_interface\_1112) and click the **Add** button. The interface settings page for the new IP interface appears.
3. In the **Address** field, enter the Source IP address for the tunnel (example uses 1.1.1.2).
4. In the **Interface** area, click the **Select Port** drop down menu and select the previously configured Span-Monitor port (Port 1-1 in [Configure Ports](#)) to connect to the public/private IP network.
5. Click **Apply** in the Toolbar to save the changes to the running configuration.

The screenshot shows the "IP\_interface\_1112" configuration page. It has fields for "Address" (1.1.1.2) and "State" (up). Under the "Interface" section, there's a "Select Port" dropdown set to "1-1". A note below says "Configure IP Interface on port".

## CLI Configuration

```
PFS7120(config)# interface ip IP_interface_1112 address 1.1.1.2
port 1-1
```



## Show IP Interface on Chosen L2GRE Tunnel Ports

View IP Interface Settings on the Configuration > Tunnel Settings > IP Interface page.

Name	Address	State	Port
IP_interface_1112	1.1.1.2	up	1-1
IP_interface_1-9	1.1.1.9	up	1-9
IP_interface_1-49	1.1.1.49	up	1-49

**Note:** The State column shows the link status (Up or Down) of the port associated with the IP interface used for the tunnel.

### CLI show command:

```
PFS7120# show running-config interface ip IP_interface_1112
interface ip IP_interface_1112
address 1.1.1.2
port 1-1
```

## Configure GRE Interface

Configure the GRE Interface settings.

1. On the Configuration > Tunnel Settings page, select the **GRE Interface** tab.
2. Click the **Add** button to add a new GRE interface. Enter a name for the interface (example uses gre\_tunnel\_1113) and click the **Add** button. The interface settings page for the new GRE interface appears.
3. In the Source field, select the previously configured IP interface (IP\_interface\_1112 in [Configure IP Interface](#)).
4. In the **Address** field, enter the Destination IP address for the tunnel (example shows 1.1.1.3).
5. In the **Key** field, define an L2GRE key to be used to identify packets on the tunnel. Valid values are 1 to 268435455 (example shows 1233). **Note:** PFS 7030s and PFS 7031s also support an L2GRE key value of 0.
6. Configure Gateway, if applicable:
  - When the destination is **local**, do not configure a **Gateway** to avoid possible network problems.



gre\_tunnel\_1113 ×

Source * <input type="button" value="IP_interface_1112"/> IP Interface name	Destination * <input type="text" value="1.1.1.3"/> Destination IP
Key * <input type="text" value="1233"/> Valid values: 0—268435455 L2GRE key	Gateway <input type="text" value=""/> ipv4-address Gateway IP Address
Vlan Tagging <input type="text" value="No Tag"/> Default: no-tag Service Tag options for Encapsulated traffic	Resolved Mac <input type="text" value="00:10:94:00:00:03"/> Default: 00:00:00:00:00:00 MAC Learned on this tunnel
State up Default: down Tunnel State	

- When the destination is on a **remote** network, in the **Gateway** field, enter the local gateway IPv4 IP address for the GRE interface.

GRE\_4444\_gateway\_1111 ×

Source * <input type="button" value="IP_interface_1112"/> IP Interface name	Destination * <input type="text" value="4.4.4.4"/> Destination IP
Key * <input type="text" value="1232"/> Valid values: 0—268435455 L2GRE key	Gateway <input type="text" value="1.1.1.1"/> × Local Gateway
Vlan Tagging <input type="text" value="Ingress Tag"/> Default: no-tag Service Tag options for Encapsulated traffic	Resolved Mac <input type="text" value="00:10:94:00:00:11"/> Default: 00:00:00:00:00:00 MAC Learned on this tunnel
State up Default: down Tunnel State	

7. Click **Apply** in the Toolbar to save the changes to the running configuration.

8. Confirm the tunnel State and Resolved MAC:

If the port associated with the IP Interface used for the GRE Tunnel has an "Up" link state, once the IP Interface and the GRE tunnel settings are applied, PFOS will send an ARP request to the Gateway (if configured) or to the Destination (if Gateway is not configured). PFOS GRE tunnel settings do not include a subnet mask; therefore, PFOS relies on the Gateway setting to decide if the Destination is at a remote or local subnet:

- If a Gateway **is not** configured, PFOS assumes tunnel destination at a local subnet, and sends the ARP request directly to the Destination IP address.
- If a Gateway **is** configured, PFOS assumes tunnel destination at a remote subnet, and sends the ARP request to the Gateway IP address.

Once the ARP response is received, the tunnel State at the WebUI will display "up" with a proper "Resolved Mac" address for the tunnel Gateway or Destination.

Otherwise, the tunnel State will display "mac-unresolved" or "down" with "Resolved Mac" as all "00s".

### CLI Configuration (Local)



```
PFS7120 (config)# interface gre gre_tunnel_1113 source IP_interface_1112 destination 1.1.1.3 key 1233
```

### CLI Configuration (Remote)

```
PFS7120 (config)# interface gre GRE_4444_gateway_1111 source IP_interface_1112 destination 4.4.4.4 key 1232 gateway 1.1.1.1
```

## Show GRE Interface on IP Interfaces

View GRE Interface Settings on the Configuration > Tunnel Settings > GRE page.

Name	Source	Destination	Key	State
GRE-tunnel-mac-unresolved	IP_interface_1-49	10.10.10.10	123410	mac-unresolved
GRE_3333_gateway_1111	IP_interface_1112	3.3.3.3	1231	up
GRE_4444_gateway_1111	IP_interface_1112	4.4.4.4	1232	up
GRE_9999_port49_gateway1111	IP_interface_1-49	9.9.9.9	12349	mac-unresolved
gre_tunnel_1113	IP_interface_1112	1.1.1.3	1233	up

**Note:** The State column shows the ARP response status, if the port associated with the IP Interface receives an ARP response from the local gateway or tunnel destination. Possible state values are:

- **down:** the default status
- **up:** the ARP response is received, and the MAC address is resolved for the local gateway IP or the local destination IP.
- **mac-unresolved:** No ARP response is received.

### CLI show command:

```
PFS7120# show running-config interface gre gre_tunnel_1113
interface gre gre_tunnel_1113
source IP_interface_1112
destination 1.1.1.3
key 1233
```

## Configure Traffic Map for the Tunnel

Refer to steps in Use Case 1 [Using Tunnel as Egress](#) to create traffic maps with L2GRE tunnel as egress traffic.

## L2GRE Tunnel Statistics and Status

Refer to the following sections for details about viewing tunnels statistics and status:

- [Display Statistics Counters for each Tunnel](#)
- [Display Tunnel Status at Event Notifications](#)



- [Display Tunnel Status at IP Interface](#)
- [Display GRE Tunnel State](#)

## Display Statistics Counters for each Tunnel

To view packet counters on GRE tunnel interfaces.

**CLI:** use the `show statistics tunnel gre` command.

```
PFOS# statistics reset 12gre-stats
PFOS# show statistics tunnel gre gre-tunnel-name gre_tunnel_1113
      ARP      ARP
GRE TUNNEL      REQ     RES    PACKET   PACKET   TX     RX
NAME          SENT    RECV    TX       RX      PPS    PPS
-----
gre_tunnel_1113  1       1      0        0       0      0
```

**WebUI:** Access the Status>Statistics>Tunnel GUI.

The screenshot shows the 'Statistics' page with the 'Tunnel' tab selected. Under 'Tunnel Views', 'GRE' is selected. The 'GRE View' section displays statistics for several GRE tunnels, including their names, ARP request sent, ARP response received, packet transmitted, packet received, and transmission/reception rates per second. The table has columns: GRE Tunnel Name, Arp Req Sent, Arp Res Recv, Packet Tx, Packet Rx, Tx Pkt/Sec (PPS), and Rx Pkt/Sec (PPS). The table data is as follows:

GRE Tunnel Name	Arp Req Sent	Arp Res Recv	Packet Tx	Packet Rx	Tx Pkt/Sec (PPS)	Rx Pkt/Sec (PPS)
gre_tunnel_1113	1	1	0	0	0	0
GRE_9999_port49_gateway1111	34107	0	0	0	0	0
GRE_4444_gateway_1111	1	1	0	0	0	0
GRE_3333_gateway_1111	1	1	0	0	0	0
GRE-tunnel-mac-unresolved	34107	0	0	0	0	0

PFOS lists the following statistics:

- **Arp Req Sent:** ARP request packets sent from PFS IP interface to local gateway or local tunnel destination.
- **Arp Res Recv:** ARP response packets received by PFS IP interface from local gateway or local tunnel destination.
- **Packet TX, Packet Rx:** packets transmitted and received at PFS IP interface after ARP response is received and local gateway or local tunnel destination MAC is resolved.



- **Packet TX PPS, Packet Rx PPS:** packets transmitted and received per second at PFS IP interface after ARP response is received and local gateway or local tunnel destination MAC is resolved.

### Display Tunnel Status at Event Notifications

At the WebUI, you can access the SysLog History to view GRE tunnel interface events for state changes (Status>Event Notifications>SysLog History).

### Event Notifications

Syslog History    Alarm

^ Syslog History

ID	Facility	Severity	Timestamp	Message
514	system	notice	2024-02-29T04:36:03.634Z	SysAccCtl Logged in User:admin,Role:admin,IP:10.252.2.34, Context:cli,AccessType:HTTP
513	system	notice	2024-02-29T04:21:06.055Z	SysAccCtl Logged out User:admin,IP:10.252.2.34, Context:webui,AccessType:HTTPS
512	system	notice	2024-02-29T03:52:28.770Z	SysAccCtl Logged in User:admin,Role:admin,IP:10.252.2.34, Context:webui,AccessType:HTTPS
511	system	notice	2024-02-29T00:56:34.622Z	SysAccCtl Logged out User:admin,IP:10.200.130.120, Context:webui,AccessType:HTTPS
510	system	notice	2024-02-28T23:34:35.331Z	SysAccCtl Logged in User:admin,Role:admin,IP:10.252.2.34, Context:webui,AccessType:HTTPS
509	system	notice	2024-02-28T23:02:03.841Z	SysCfgChg, Interface IP IP_interface_1-49 state changed to UP
508	system	warning	2024-02-28T23:02:03.819Z	SysPort ports 1-49 is now online (link up)
507	system	warning	2024-02-28T23:02:02.968Z	SysPort ports 1-48 is now online (link up)
506	system	warning	2024-02-28T23:01:53.448Z	SysPort ports 1-26 is now online (link up)
505	system	notice	2024-02-28T22:59:35.422Z	SysCfgChg, Interface IP IP_interface_1-49 state changed to Down
504	system	alert	2024-02-28T22:59:35.406Z	SysPort ports 1-49 is offline (link down)
503	system	notice	2024-02-28T22:59:35.393Z	SysCfgChg, Tunnel vxlan_1-49_gateway1111 state changed to mac Unresolved
502	system	notice	2024-02-28T22:59:35.390Z	SysCfgChg, Tunnel GRE_9999_port49_gateway1111 state changed to mac Unresolved
501	system	notice	2024-02-28T22:59:35.387Z	SysCfgChg, Tunnel GRE-tunnel-mac-unresolved state changed to mac Unresolved
500	system	alert	2024-02-28T22:59:35.362Z	SysPort ports 1-48 is offline (link down)
499	system	alert	2024-02-28T22:59:35.324Z	SysPort ports 1-26 is offline (link down)

### Display Tunnel Status at IP Interface

To view IP interface tunnel status.

**CLI:** Use the show interface ip command.

```
PFOS# show interface ip IP_interface_1112 ref-gre
GRE NAME
-----
GRE_3333_gateway_1111
GRE_4444_gateway_1111
gre_tunnel_1113

PFOS# show interface ip IP_interface_1112 state
state up
```



**WebUI:** Access the Configuration>Tunnel Settings>IP Interface GUI.

Name	Address	State	Port
IP_interface_1-49	1.1.1.49	up	1-49
IP_interface_1-9	1.1.1.9	up	1-9
IP_interface_1112	1.1.1.2	up	1-1

**Note:** The State column shows the link status (Up or Down) of the port associated with the IP interface used for the tunnel.

### Display GRE Tunnel State

GRE tunnel interface state depends on the reachability to local destinations or local gateways when destinations are on remote networks (up or mac-unresolved).

**CLI:** Use the `show interface gre` command.

```
PFOS# show interface gre
interface gre GRE_4444_gateway_1111
    state      up
    resolved mac 00:10:94:00:00:11
    ref-lbg additional_tunnel_LBG
interface gre gre_tunnel_1113
    state      up
    resolved mac 00:10:94:00:00:03
```

**WebUI:** Access the Configuration>Tunnel Settings>GRE GUI.

Name	Source	Destination	Key	State
gre_tunnel_1113	IP_interface_1112	1.1.1.3	1233	up
GRE_9999_port49_gateway1111	IP_interface_1-49	9.9.9.9	12349	mac-unresolved
GRE_4444_gateway_1111	IP_interface_1112	4.4.4.4	1232	up
GRE_3333_gateway_1111	IP_interface_1112	3.3.3.3	1231	up
GRE-tunnel-mac-unresolved	IP_interface_1-49	10.10.10.10	123410	mac-unresolved

**Note:** The State column shows the ARP response status, if the IP Interface receives an ARP response from the local gateway or tunnel destination. Possible state values are:



- **down:** the default status
- **up:** the ARP response is received, and the MAC address is resolved for the local gateway IP or the local destination IP.
- **mac-unresolved:** No ARP response is received.

## L2GRE Origination/Termination Limitations

- The PFS 704x-32D devices do not support L2GRE Origination/Termination.
- Up to 1024 different L2GRE interfaces are possible per chassis
- The L2GRE key parameter must be used/must be present on all received packets.
  - Supported L2GRE key values are 1 to  $2^{28}$  (1 to 268435455). **Note:** PFS 7030s and PFS 7031s also support an L2GRE key value of 0.
  - L2GRE keys must be unique per chassis (the same key cannot be used by more than one tunnel).
  - L2GRE key values cannot be the same as configured L2GRE IDs used in Standard L2GRE Stripping.
- Maximum one L2GRE tunnel per Destination IP address.
- Up to 256 IP Interfaces per chassis
  - No Restriction on L2GRE to IP interface mapping
  - One IP interface per physical port (or breakout port)

**Note:** PFOS supports configuring multiple tunnels over one physical port as long as each tunnel has a unique Destination IP address

- IP/GRE Tunnel currently supports only IPv4 for GRE encapsulation and decapsulation
- After terminating and decapsulating traffic, PFOS only supports “Unfiltered” filter for maps. Ingress tunnels only support unfiltered traffic.
- When you configure a traffic map with L2GRE tunnels as input-tunnels, flow map counters are not updated.
- IP/GRE Tunnel interface ports:

- **SHOULD NOT have any stripping function enabled.**

**Note: If ANY stripping function is inadvertently configured at an L2GRE tunnel interface, disabling the stripping function may not resolve the configuration conflict. It may be necessary to reboot the device after disabling the stripping function.**

- **SHOULD NOT have IP Tunnel Termination function enabled.**
  - **SHOULD NOT** be used as regular input or output ports in traffic maps/load balance groups.
  - **SHOULD NOT** enable monitor port VLAN tagging.
  - **SHOULD NOT** be used as a Port Mirroring session’s source or destination interface.

In addition, the ingress interface that is sending traffic to the tunnel interface **SHOULD NOT** have any stripping function enabled. A workaround is to create another map for stripped traffic to a service port; then use the service port as input to GRE tunnel.



- When adding a tunnel load balance group (LBG) as a map's output, the following limitations apply:
  - No other output ports are supported.
  - No port load balance groups are supported.
  - Only one tunnel load balance group is supported.
  - The input ports used in a filter traffic map that egress to tunnel load balance group(s) cannot be used at another unfiltered map.

## VXLAN Tunnel Origination/Termination Support

**Note:** This feature requires the PFS 7000 functionality license.

PFOS supports VXLAN tunnel origination and termination. Virtual Extensible LAN (VXLAN) is a VLAN extension technology that encapsulates the standard Layer 2 Ethernet frames within IP, specifically using UDP port 4789 assigned by the Internet Assigned Numbers Authority (IANA). The MAC Address in UDP encapsulation creates a tunnel that allows users to extend a Layer 2 segment across any Layer 3 network. A VXLAN header is added to the Layer 2 frame and placed inside a UDP packet prior to transmission.

Note that because VXLAN headers are added to frames sent over the VXLAN tunnel, the tunnel's transport network MTU should be large enough to hold the largest monitored frame plus the tunnel headers. PFS 7000 will not fragment nor reassemble oversized frames.

VXLAN networks include a 24-bit VNID or VXLAN Network Identifier to define VXLAN broadcast domains.

VXLAN uses the VXLAN tunnel endpoint (VTEP) to map end devices to VXLAN segments and to perform VXLAN encapsulation and decapsulation. Each VTEP function has two interfaces: one is a switch interface on the local LAN segment to support local endpoint communication, and the other is an IP interface to the transport IP network.

**Note:** VXLAN tunnels do not support packet fragmentation and reassembly.

Refer to [Configuring VXLAN Tunnel Origination/Termination](#) for workflow details. ***Review the VXLAN Tunnel Origination/Termination Limitations prior to configuring VXLAN Tunnel Origination/Termination.***

### Configuring VXLAN Tunnel Origination/Termination

**Note:** The [Features Tunnel option](#) in Global Settings must be enabled before you can use this feature.

Use the following procedure to configure VXLAN tunnel origination/termination. Refer to the **PFOS 6.x CLI Reference Guide** for CLI command details. ***Review the VXLAN Tunnel Origination/Termination Limitations prior to configuring VXLAN Tunnel Origination/Termination.***

**Note:** There is a maximum of 1024 VXLAN tunnels per chassis.

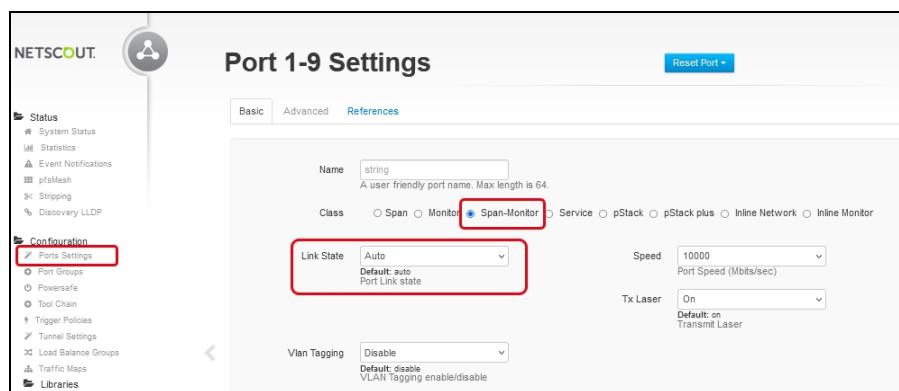


Step	Web UI	CLI
<b>1 Configure Ports</b> Configure a port that is connected to the IP network as Span-Monitor.	Port Settings Page	interface command
<b>2 Configure IP Interface</b> Configure the Source IP address for the tunnel and select the Span-Monitor port to connect to the public/private IP network.	Tunnel Settings>IP Interface Page	interface ip command
<b>3 Configure VXLAN Interface</b> Configure the Destination IP address for the tunnel, the IP Interface, VXLAN Tunnel Key, UDP Source Port, and Gateway.	Tunnel Settings>VXLAN Interface Page	interface vxlan command
<b>4 Configure Traffic Map for the Tunnel</b> <b>Note:</b> PFOS does not support both input tunnels and output tunnels in the same map.	Traffic Maps	Refer to Map Commands for VXLAN Tunnel Origination/Termination

## Configure Ports

Configure a port that will be used to connect to the IP network.

1. On the Configuration > Port Settings page, click a port ID link to display the settings for the port.
2. Configure Basic settings.
  - a. Select **Span-Monitor** as the Port Class.
  - b. Select **Auto** as the Link State.
3. Click **Apply** in the Toolbar to save the changes to the running configuration.



## Configure IP Interface

Configure the following IP Interface settings.

1. On the Configuration > Tunnel Settings page, select the **IP Interface** tab.
2. Click the **Add** button to add a new IP interface. Enter a name for the interface and click the **Add** button. The interface settings page for the new IP interface appears.



3. In the **Address** field, enter the Source IP address for the tunnel.
4. In the **Interface** area, click the **Select Port** drop down menu and select the previously configured Span-Monitor port to connect to the public/private IP network.
5. Click **Apply** in the Toolbar to save the changes to the running configuration.

The screenshot shows the configuration interface for an IP interface named 'IP\_interface\_1-9'. At the top, there's a 'Select Port' dropdown menu. Below it, a 'Port' dropdown is set to '1-9'. The main configuration area includes fields for 'Address' (set to '1.1.1.9') and 'State' (set to 'up'). There's also a note about the IP Interface Link State. The interface section is expanded, showing the 'Select Port' dropdown again.

## Configure VXLAN Interface

Configure the VXLAN Interface settings.

1. On the Configuration > Tunnel Settings page, select the **VXLAN Interface** tab.
2. Click the **Add** button to add a new VXLAN interface. Enter a name for the interface and click the **Add** button. The interface settings page for the new VXLAN interface appears.
3. In the Source field, select the previously configured IP interface.
4. In the **Address** field, enter the Destination IP address for the tunnel.
5. In the **Key** field, define a VXLAN key to be used to identify packets on the tunnel. Valid values are 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.
6. Enter the **UDP L4 Source Port** for encapsulated traffic; valid values range from 1 to 65535.
7. Configure a Gateway, if applicable:
  - When the destination is **local**, do not configure a **Gateway** to avoid possible network problems.
  - When the destination is on a **remote** network, in the **Gateway** field, enter the local gateway IPv4 IP address for the VXLAN interface.
8. To enable ingress port VLAN tags to be added to the packets being forwarded to the VXLAN tunnel, select **Ingress Tag**.
9. Click **Apply** in the Toolbar to save the changes to the running configuration.



#### 10. Confirm the tunnel State and Resolved MAC:

If the port associated with the IP Interface used for the VXLAN Tunnel has an "Up" link state, once the IP Interface and the VXLAN tunnel settings are applied, PFOS will send an ARP request to the Gateway (if configured) or to the Destination (if Gateway is not configured). PFOS VXLAN tunnel settings do not include a subnet mask; therefore, PFOS relies on the Gateway setting to decide if the Destination is at a remote or local subnet:

- If a Gateway **is not** configured, PFOS assumes tunnel destination at a local subnet, and sends the ARP request directly to the Destination IP address.
- If a Gateway **is** configured, PFOS assumes tunnel destination at a remote subnet, and sends the ARP request to the Gateway IP address.

Once the ARP response is received, the tunnel State at the WebUI will display "up" with a proper "Resolved Mac" address for the tunnel Gateway or Destination.

Otherwise, the tunnel State will display "mac-unresolved" or "down" with "Resolved Mac" as all "00s".

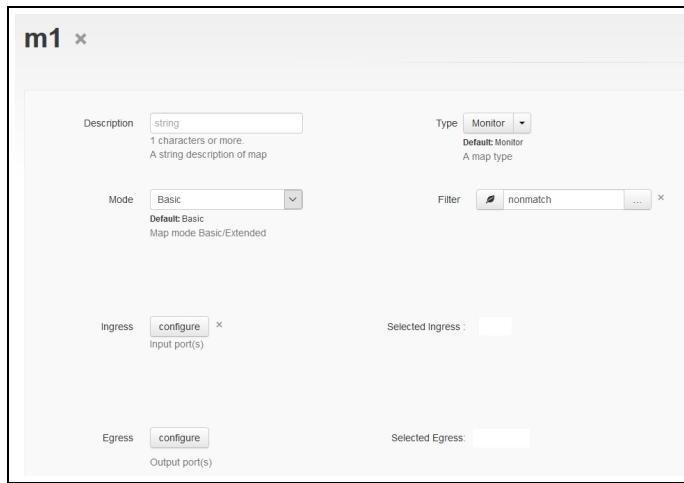
The screenshot displays the 'vxlan\_1-9\_tunnel1' VxLAN Tunnel Settings page. The configuration includes:

- Source: IP\_Interface\_1-9
- Destination: 3.3.3.5
- Key: 12391
- UDP Src Port: 12391
- Gateway: 1.1.1.1
- VLAN Tagging: No Tag
- State: mac-unresolved
- Resolved Mac: 00:00:00:00:00:00

#### Configure Traffic Map for the Tunnel

Configure a traffic map for the tunnel.

1. On the Configuration > Traffic Maps page, click the **Add** button to add a new traffic map. Enter a name for the traffic map and click the **Add** button. The map settings page for the new map appears.
2. Add a map **Description**.
3. Select **Monitor** for map **Type**.
4. Select **Basic** for map **Mode**.
5. In the **Filter** field, select a filter or select **Unfiltered** for tunnel traffic.



**Note:** PFOS does not support both input tunnels and output tunnels in the same map. If you configure an Input tunnel in Ingress, you must configure a port for Egress; if you configure an Output tunnel in Egress, you must configure a port for Ingress. The following sections are example configurations showing this.

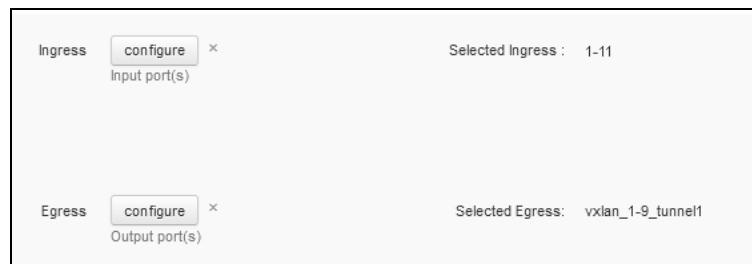
### Map Span Traffic to Tunnel (Encapsulation)

1. Click the **Egress Configure** button. The Select Ports to Use dialog box appears. Select the **Output tunnels** radio button to display the available tunnels. Drag and drop the tunnel name to the Egress tunnel section on the right and click **OK**.

**Note:** When using CLI to configure a traffic map with 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.



2. Since a tunnel was configured for Egress, click the **Ingress** button and select an Ingress Span port for the map.





3. Click **Apply** in the Toolbar to save the changes to the running configuration.

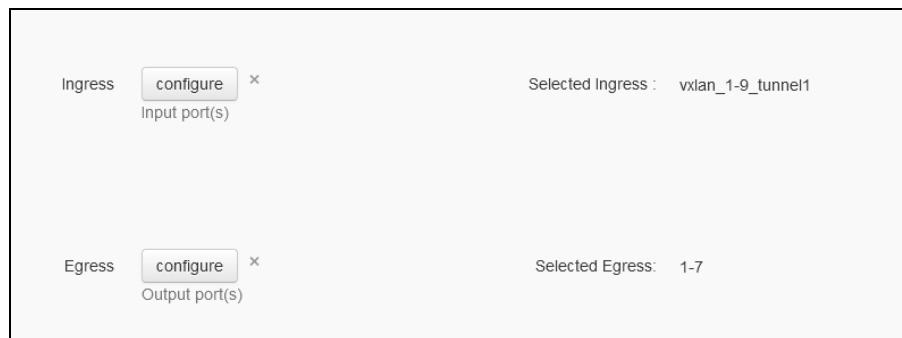
### Map Tunnel Traffic to the Monitor Port (Decapsulation)

1. Click the **Ingress Configure** button. The Select Ports to Use dialog box appears. Select the **Input tunnels** radio button to display the available tunnels. Drag and drop the tunnel name to the Ingress tunnel section on the right and click **OK**.

**Note:** When using CLI to configure a traffic map with 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.



2. Since a tunnel was configured for Ingress, click the **Egress** button and select an Egress port for the map, such as a monitor port.



3. Click **Apply** in the Toolbar to save the changes to the running configuration.

### Tunnel Statistics and Status

Refer to the following sections for details about viewing tunnels statistics and status:

- [Display Statistics Counters for each Tunnel](#)
- [Display Tunnel Status at Event Notifications](#)
- [Display Tunnel Status at IP Interface](#)
- [Display VXLAN Tunnel State](#)

#### *Display Statistics Counters for each Tunnel*

To view packet counters on VXLAN tunnel interfaces.

**CLI:** use the `show statistics tunnel vxlan` command.



```
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 37613  0       0       0       0       0
vxlan_1-9_tunnel1  37613  0       0       0       0       0
vxlan_tunnel_1111_gateway 1       1       4971   0       0       0
vxlan_tunnel_1113  1       2       5016   0       0       0
vxlan_tunnel_1114  1       1       4626   0       0       0
vxlan_tunnel_1115  1       1       4522   4836   0       0
vxlan_tunnel_2223_gateway 1       1       0       0       0       0
```

**WebUI:** Access the Status>Statistics>Tunnel GUI.

The screenshot shows the PFOS WebUI Statistics page with the 'Tunnel' tab selected. It displays statistics for VxLAN tunnels. The top section shows a summary table with columns: Vxlan Tunnel Name, Arp Req Sent, Arp Res Recv, Packet Tx, Packet Rx, Tx Pkt/Sec (PPS), and Rx Pkt/Sec (PPS). Below this is a detailed table for each tunnel, showing specific packet counts and rates. The interface includes a toolbar with various icons for filtering and searching.

Vxlan Tunnel Name	Arp Req Sent	Arp Res Recv	Packet Tx	Packet Rx	Tx Pkt/Sec (PPS)	Rx Pkt/Sec (PPS)
vxlan_1-49_gateway1111	37653	0	0	0	0	0
vxlan_1-9_tunnel1	37653	0	0	0	0	0
vxlan_tunnel_1111_gateway	1	1	4971	0	0	0
vxlan_tunnel_1113	1	2	5016	0	0	0
vxlan_tunnel_1114	1	1	4626	0	0	0
vxlan_tunnel_1115	1	1	4522	4836	0	0
vxlan_tunnel_2223_gateway	1	1	0	0	0	0

PFOS lists the following statistics:

- **Arp Req Sent:** ARP request packets sent from PFS IP interface to local gateway or local tunnel destination.
- **Arp Res Recv:** ARP response packets received by PFS IP interface from local gateway or local tunnel destination.
- **Packet TX, Packet RX:** packets transmitted and received at PFS IP interface after ARP response is received and local gateway or local tunnel destination MAC is resolved.
- **Packet TX PPS, Packet RX PPS:** packets transmitted and received per second at PFS IP interface after ARP response is received and local gateway or local tunnel destination MAC is resolved.



## Display Tunnel Status at Event Notifications

At the WebUI, you can access the SysLog History to view VXLAN tunnel interface events for state changes (Status>Event Notifications>SysLog History).

### Event Notifications

Syslog History    Alarm

▲ Syslog History

ID	Facility	Severity	Timestamp	Message
487	system	notice	2024-02-28T20:51:21.718Z	SysCfgChg, Interface IP IP_interface_1-49 state changed to UP
486	system	warning	2024-02-28T20:51:21.702Z	SysPort. ports 1-49 is now online (link up)
485	system	warning	2024-02-28T20:51:19.567Z	SysPort. ports 1-48 is now online (link up)
484	system	warning	2024-02-28T20:51:11.054Z	SysPort. ports 1-26 is now online (link up)
483	system	notice	2024-02-28T20:46:59.874Z	SysCfgChg, Tunnel vxlan_1-49_gateway1111 state changed to mac Unresolved
482	system	notice	2024-02-28T20:46:59.872Z	SysCfgChg, Tunnel GRE_9999_port49_gateway1111 state changed to mac Unresolved
481	system	notice	2024-02-28T20:46:59.871Z	SysCfgChg, Tunnel GRE-tunnel-mac-unresolved state changed to mac Unresolved
480	system	notice	2024-02-28T20:46:59.686Z	SysCfgChg, Interface IP IP_interface_1-49 state changed to Down
479	system	alert	2024-02-28T20:46:59.670Z	SysPort. ports 1-49 is offline (link down)
478	system	alert	2024-02-28T20:46:58.640Z	SysPort. ports 1-48 is offline (link down)
477	system	alert	2024-02-28T20:46:58.607Z	SysPort. ports 1-26 is offline (link down)

## Display Tunnel Status at IP Interface

To view IP interface tunnel status.

**CLI:** Use the `show interface ip` command.

```
PFOS# show interface ip IP_interface_1112
NAME          STATE   GRE NAME           VXLAN NAME
-----
IP_interface_1112  up     GRE_3333_gateway_1111
                  GRE_4444_gateway_1111
                  gre_tunnel_1113      vxlan_tunnel_1111_gateway
                                         vxlan_tunnel_1113
                                         vxlan_tunnel_1114
                                         vxlan_tunnel_1115
                                         vxlan_tunnel_2223_gateway
```



**WebUI:** Access the Configuration>Tunnel Settings>IP Interface GUI.

Name	Address	State	Port
IP_interface_1-49	1.1.1.49	up	1-49
IP_interface_1-9	1.1.1.9	up	1-9
IP_interface_1112	1.1.1.2	up	1-1

Showing 1 to 3 of 3

**Note:** The State column shows the link status (Up or Down) of the port associated with the IP interface used for the tunnel.

### Display VXLAN Tunnel State

VXLAN tunnel interface state depends on the reachability to local destinations or local gateways when destinations are on remote networks (up or mac-unresolved).

**CLI:** Use the show interface vxlan command.

```
PFOS# show interface vxlan vxlan_tunnel_1111_gateway
interface vxlan vxlan_tunnel_1111_gateway
    state      up
    resolved mac 00:10:94:00:00:11
    ref-network-map map_tunnels_to_port
    ref-monitor-map map_port_to_tunnel_1111
```

**WebUI:** Access the Configuration>Tunnel Settings>VXLAN GUI.

Name	Source	Destination	Key	State
vxlan_1-49_gateway1111	IP_interface_1-49	9.9.9.49	12491	mac-unresolved
vxlan_1-9_tunnel1	IP_interface_1-9	3.3.3.5	12391	mac-unresolved
vxlan_tunnel_1111_gateway	IP_interface_1112	2.2.2.2	1231	up
vxlan_tunnel_1113	IP_interface_1112	1.1.1.3	1233	up
vxlan_tunnel_1114	IP_interface_1112	1.1.1.4	1234	up
vxlan_tunnel_1115	IP_interface_1112	1.1.1.5	1235	up
vxlan_tunnel_2223_gateway	IP_interface_1112	2.2.2.3	12313	up

Showing 1 to 7 of 7

**Note:** The State column shows the ARP response status, if the IP Interface receives an ARP response from the local gateway or tunnel destination. Possible state values are:



- **down:** the default status
- **up:** the ARP response is received, and the MAC address is resolved for the local gateway IP or the local destination IP.
- **mac-unresolved:** No ARP response is received.

## VXLAN Tunnel Origination/Termination Limitations

- Up to 1024 different VXLAN interfaces are possible per chassis
- VxLAN VNIDs supported are 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.
  - VXLAN VNIDs must be unique per chassis (the same VNID cannot be used by more than one tunnel).
  - VXLAN key values cannot be the same as configured VXLAN IDs used in Standard VXLAN Stripping.
- Maximum one VxLAN tunnel per Destination IP address.
- Up to 256 IP Interfaces per chassis
  - No Restriction on VxLAN to IP interface mapping
  - One IP interface per physical port (or breakout port)
- Note: PFOS supports configuring multiple tunnels over one physical port as long as each tunnel has a unique Destination IP address
- When two VxLAN tunnels are configured on the same port (that is, using the same IP address tunnel to two destinations), the second tunnel's encapsulation will always use the UDP port number setting in the first tunnel configuration.
- IP/VXLAN Tunnel currently supports only IPv4 for VXLAN encapsulation and decapsulation
- After terminating and decapsulating traffic, PFOS only supports "Unfiltered" filter for maps. Ingress tunnels only support unfiltered traffic.
- When you configure a traffic map with VxLAN tunnels as input-tunnels, flow map counters are not updated.

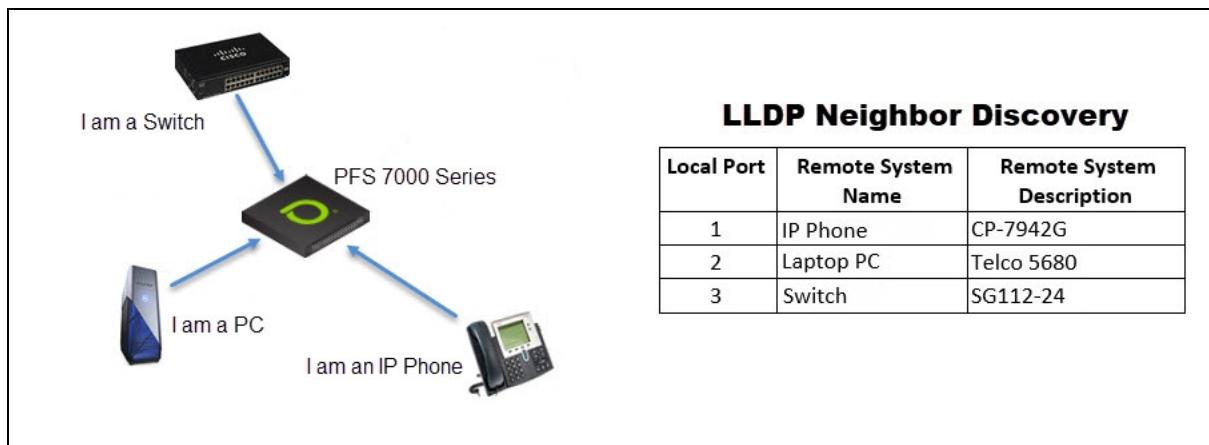


- IP/VXLAN Tunnel interface ports:
  - **Should NOT have any stripping function enabled.**  
**Note: If ANY stripping function is inadvertently configured at a VXLAN tunnel interface, disabling the stripping function may not resolve the configuration conflict. It may be necessary to reboot the device after disabling the stripping function.**
  - **Should NOT have the IP Tunnel Termination function enabled.**
  - **Should NOT** be used as regular input or output ports in traffic maps/load balance groups.
  - **Should NOT** enable monitor port VLAN tagging.
  - **SHOULD NOT** be used as a Port Mirroring session's source or destination interface.
- In addition, the ingress interface that is sending traffic to the tunnel interface **Should NOT** have any stripping function enabled. A workaround is to create another map for stripped traffic to a service port; then use the service port as input to VxLAN tunnel.
- When adding a tunnel load balance group (LBG) as a map's output, the following limitations apply:
  - No other output ports are supported.
  - No port load balance groups are supported.
  - Only one tunnel load balance group is supported.
  - The input ports used in a filter traffic map that egress to tunnel load balance group(s) cannot be used at another unfiltered map.

## Neighbor Discovery Using LLDP

**Note: This feature requires the PFS 7000 functionality license. If you apply configuration files that contain the LLDP feature, but do not have a PFS 7000 license installed, the configuration will be applied without error. However, the LLDP feature is not enabled until the PFS 7000 license is installed.**

Link Layer Discovery Protocol (LLDP) is a Layer 2 neighbor discovery protocol that allows devices to advertise device information to their directly connected peers/neighbors. Using LLDP, device information such as chassis identification, port ID, port description, system name and description, device capability (such as a router, switch, hub, etc.), and IP/MAC address, are transmitted to the neighboring devices on each port.



In an extended network of thousands of interconnected ports, LLDP can help PFS devices recognize the neighboring systems and provide users a better understanding of the interconnections between the Production Network and the monitoring system. Additionally, LLDP enhances the ability of network management tools in multi-vendor environments.

### LLDP Ethernet Frame Structure

The Ethernet frame contains one LLDP Data Unit (LLDPDU) which is a sequence of type-length-value (TLV) structures. LLDP Packet's Destination MAC address is a reserved multicast address that 802.1D compliant bridges do not forward. The EtherType field is set to 0x88cc.

Preamble	Destination MAC	Source MAC	Ethertype	Chassis ID TLV	Port ID TLV	Time to live TLV	Optional TLVs	End of LLDPDU TLV	Frame check sequence
	01:80:c2:00:00:0e 01:80:c2:00:00:03 01:80:c2:00:00:00 See <a href="#">LLDP Destination MAC Support</a> for details.	Station's address	0x88CC	Type=1	Type=2	Type=3	Zero or more complete TLVs	Type=0, Length=0	

### LLDP Destination MAC Support

LLDP supports following destination MACs:

- 0x0180-C200-000E for LLDP frames destined for nearest bridge agents.
- 0x0180-C200-0000 for LLDP frames destined for nearest customer bridge agents.
- 0x0180-C200-0003 for LLDP frames destined for nearest non-TPMR bridge agents.

### PFOS LLDP Destination MAC Support

PFOS provides the following LLDP Destination MAC support:



- **LLDP Rx**: Supports all MACs (Nearest Bridge, Nearest Customer Bridge and Nearest non-TPMR bridge)
- **LLDP Tx**: Supports only Nearest Bridge MAC; that is, only Tx with MAC 0x0180-C200-000E
- Supports learning only ONE neighbor per agent per port. That means a port can learn a maximum of three neighbors on a port, one per each Destination MAC agent.

## Mandatory TLVs

All LLDPDUs will contain the following four mandated TLVs.

Mandatory TLV	TLV Type	Description
Chassis ID	1	Identifies the device
Port ID	2	Identifies the port
Time To Live (TTL)	3	Lets the receiving device know how long the received information should remain valid.
End of LLDPDU	0	

## Optional TLVs

Optional TLVs are inserted between the TTL TLV and End of LLDPDU TLV. The basic set of optional TLVs include:

Optional TLV	TLV Type	Description
Port Description	4	Displays details about the port
System Name	5	Displays given name for the device
System Description	6	Displays version of the software
System Capabilities	7	Describes the primary function and capabilities of the device.
Management Address	8	Displays the IP or MAC address of the device

## Transmitted TLVs

The following table lists the TLVs that PFOS transmits. If any of the following values are empty, then PFOS transmits only the mandatory TLVs (Chassis ID, Port ID and TTL TLV).

TLV	Mandatory/Optional	Value sent
Chassis ID	Mandatory	System MAC address
Port ID	Mandatory	Port sys port ID as an integer
Time-to-Live	Mandatory	120s
System Name	Optional	System Name
Port Description	Optional	Port ID in slot-port format, like 1-1
System Description	Optional	PFOS Platform



TLV	Mandatory/Optional	Value sent
Management Address	Optional	IPv4 Address or IPv6 address if the IPv4 address is set to 0.0.0.0 <b>Note:</b> The IPv4 address is used for the LLDP Management Address TLV; the IPv6 address is only used if an IPv4 address is not available.

## Enabling LLDP Packet Transmit/Receive

You enable LLDP packet reception and transmission on a per-port level on the Configuration>Port Settings page by selecting the **Tx** (Transmit) and/or the **Rx** (Receive) checkboxes. Default value is Rx disable and Tx disable.

**Port 1-1 Settings**

[Reset Port](#)

[Basic](#) [Advanced](#) [References](#)

Name:  string  
A user friendly port name. Max length is 64.

Class:  Span  Monitor  Span-Monitor  Service  pStack  Inline Network  Inline Monitor

Link State:  Default: auto  
Port Link state

Speed:  Port Speed (Mbits/sec)

VLAN ID:  Default  User Defined

Link: up  
Default: down  
Port Link status

Tunnel Termination:   
Default: disable  
Tunnel Termination Support

LLDP:  Rx  Tx

## Viewing PFS LLDP Neighbors

If the PFS has been configured to receive LLDP Packets, you can view its neighbors on the Status>Discovery LLDP page.

**LLDP** LLDP information

[Refresh](#)

Neighbors LLDP Remote Information

Local Port	Chassis ID	Hold Time	System Name	System Desc	Management Address	Remote Port	Port Description
1-1	8c:ea:1b:ff:b9:9e	120	PFS-5010-Node119	PFS7010	10.250.177.119	27	1-27
1-39	8c:ea:1b:ff:b9:9e	120	PFS-5010-Node119	PFS7010	10.250.177.119	49	1-49.1
1-40	8c:ea:1b:ff:b9:9e	120	PFS-5010-Node119	PFS7010	10.250.177.119	50	1-49.2
1-7	8c:ea:1b:ff:b9:9e	120	PFS-5010-Node119	PFS7010	10.250.177.119	13	1-13

Note the following for received neighbor information:



- A maximum of 64 characters display for all Neighbor TLVs; PFOS truncates TLV characters greater than 64.
- Spaces in received LLDP Neighbor Chassis ID TLVs are converted to underscores.
- If PFOS receives more than three LLDP neighbor updates (add/delete/modify) on a port within a 30-second timeframe, PFOS stops processing on the port until the port is stable. Once the port becomes stable, neighbor information is updated within 120s of the last update received. Therefore, neighbor information updates may be delayed.
- 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".

## pfsMesh Using pStack+

**Note:** pStack+ requires the PFS 7000 functionality license. Refer to [pfsMesh](#) for details about pStack technology.

### pStack+ Technology

pStack+ is a proprietary technology that allows the interconnection of multiple systems into a pfsMesh. pStack+ is supported on PFS 7000 devices and leverages existing [pStack protocol features](#) and supports additional enhancements that are not supported on pStack:

- Support of pfsMesh over IP (See Note below)
- Load-balancing across multiple pStack+ links to same neighbor
- Reduced filter utilization on transit and end nodes

PFOS supports auto-learning and auto-healing over pStack+ ports for both directly connected ports and for ports connected over IP. If ports are connected over an IP interface, the user specifies the Source IP and Destination IP addresses while configuring port class as pStack+. For directly connected ports, PFOS determines the Source and Destination IP on pStack+ ports.

**Note:** pStack+ uses encapsulation which adds an additional 46-byte header on each packet. If the IP routing environment for pfsMesh has an MTU restriction, then the extra 46 bytes need to be considered.

Multiple directly connected (physically connected) pStack+ links to a neighbor behave as a trunk. PFOS load balances all traffic going to the same next hop across the available pStack+ links using the [Load Balance Criteria](#) used by other traffic map(s). If no Load Balance Criteria is in use, PFOS will use L3+L4 criteria for load-balancing traffic across the trunk. Multiple pStack+ ports connected over IP follow load spreading as done for pStack ports (see [pStack Load Spreading in a pfsMesh](#) for details).

When a map is created to a remote monitor group, PFOS assigns a unique tunnel ID to the map. This tunnel ID is unique across the pfsMesh and pStack+ protocol. If the next hop is a pStack+ port (or trunk), PFOS creates a VxLAN tunnel over the pStack+ port (or trunk). As PFOS sends traffic across the pfsMesh, packets matching the defined filter(s) are encapsulated with the tunnel ID and sent on the pStack+ ports (or trunk). PFOS decapsulates and encapsulates traffic at each step.



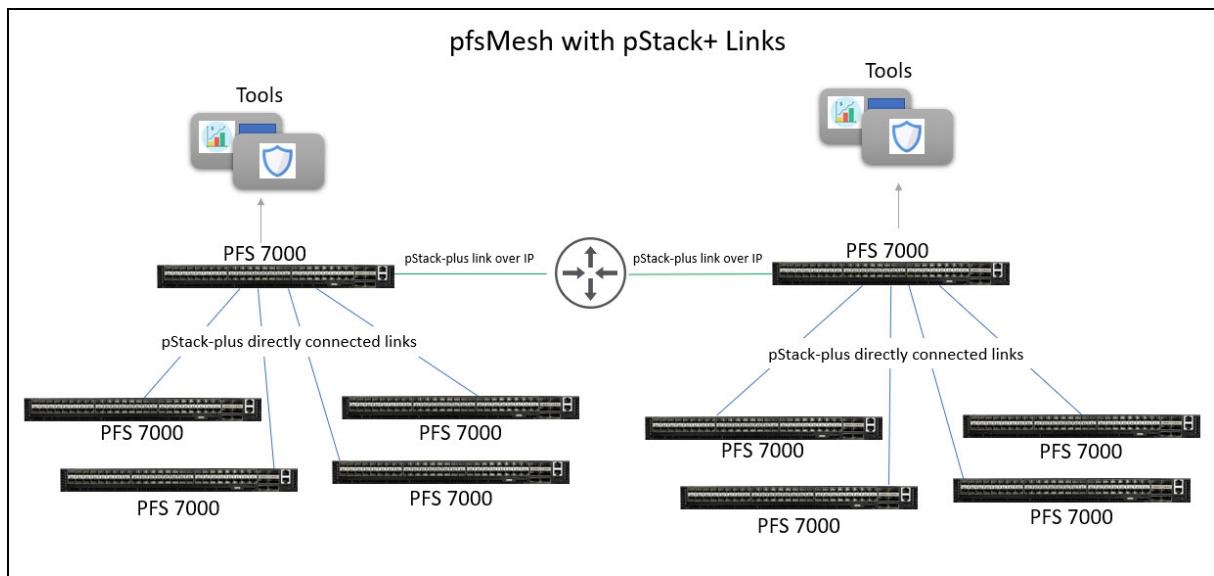
The following table summarizes pfsMesh feature support per pStack and pStack+ protocol.

pfsMesh Feature	pStack+ (PFS 7000 only)	pStack (PFS 5000/6000/7000)
pfsMesh over direct connections	Yes Maximum 16 directly connected pStack+ links supported between two neighbors (see <a href="#">pStack+ Topology</a> ) <b>Note:</b> Additional 46 bytes added to packets	Yes <b>Note:</b> Additional 4 bytes added to packets
pfsMesh over indirect connections (over IP)	Yes <b>Note:</b> Additional 46 bytes added to packets	No
Auto discovery (auto learning)	Direct Connection Indirect Connection (Over IP)	Direct Connection
Auto healing	Direct Connection Indirect Connection (Over IP)	Direct Connection
Support multiple pStack+ links between two devices as a trunk	Direct Connection	No
Load balancing across trunk	Direct Connection	No
Reduced filter resource usage	Yes	No
Configuration of a mix of pStack and pStack+ ports between PFS neighboring devices (see <a href="#">pStack and pStack+ Compatibility</a> )	No	No

## pStack+ Topology

The following graphic illustrates the supported pStack+ topology connections:

- pStack+ direct link connections (physical)
- pStack+ indirect link connections (over IP network)
- pStack and pStack+ links within same pfsMesh (see [pStack and pStack+ Compatibility](#))



For a configuration example, refer to [pfsMesh Configuration Example Using pStack+.](#)

## pStack and pStack+ Compatibility

### **pStack+ Ports**

- pStack+ ports are only supported on PFS 7000 devices, and pStack+ links can only be configured between two PFS 7000 devices. If a PFS 7000 is connecting to a PFS device other than another PFS 7000 over pfsMesh, then pStack links must be configured.
- pStack and pStack+ ports can be configured on the same PFS 7000 device. However, PFOS does not support a combination of different types of pStack links between neighbors. That is, links between two PFS devices must all be the same type of links: pStack links, OR directly connected pStack+ links, OR indirectly connected pStack+ links (see the [pfsMesh with Both pStack and pStack+ Links](#) diagram).

### **pfsMesh with PFS 7000 and PFS 6000 Devices:**

The **only** combination of PFS models with a combination of pStack+ and pStack ports supported in a pfsMesh is PFS 7000s interoperating with a PFS 6000; the following limitations apply (see [pfsMesh with Both pStack and pStack+ Links](#) diagram):

- All the PFS 7000 nodes MUST be connected via links with *pStack+* class.
- The link between the PFS 7000 and PFS 6000 MUST be *pStack* class.
- The PFS 7000 can only be a Head or Transit Node.
- The PFS 6000 can only be a Destination Node.

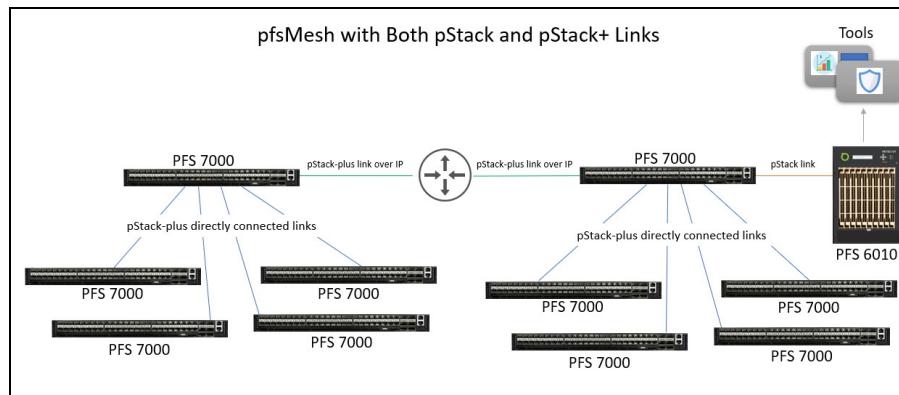
### **pfsMesh with PFS 7000 and PFS 5000 Devices:**

PFOS supports a pfsMesh configured with both PFS 5000 and PFS 7000 devices; however, *only pStack links are supported*. If a pfsMesh with both PFS 5000 and PFS 7000 devices requires pStack+ links between any two PFS 7000 devices, then every PFS 5000 device in the pfsMesh needs to install a PFS 7000 license.



## pStack+ pfsMesh and VLAN ID Assignment and Translation

If a pfsMesh is based on devices with only pStack+ links, VLAN ID assignment and translation are not required. This also removes 4000 Ingress port limitation. However, if the pfsMesh has a combination of both pStack and pStack+ links, then similar to a pfsMesh with only pStack links, VLAN ID assignment and VLAN translation are performed, and the ingress port limit of 4000 also applies. See [pfsMesh](#) for details.



## pStack+ Optimal Path Forwarding

When you select one or more remote ports for monitor output, PFOS automatically chooses one or more pStack+ links on which to transmit the monitor data. PFOS always chooses the optimal path (or paths). The optimal path for pStack+ is determined using:

- **Link speed:** Higher-speed links are given great preference over slower-speed links.
- **Hops:** The most direct links are given slight preference over links that involve one or more intervening nodes, where monitor traffic must “hop” over another transit node. Hops do not necessarily reduce the available bandwidth, but they can introduce a small latency.

PFOS may determine the pStack optimal forwarding path before all pStack links are available. In addition, pStack link state change may offer a new optimal forwarding path. To avoid unnecessary traffic interruptions, pStack will not automatically move traffic to a new forwarding path even if it is a better path. However, you can manually force pStack to recalculate, determine, and use a new optimal forwarding path for traffic by using the `reroute-maps` CLI command.

**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.

## pStack+ Limitations

- pStack+ load balancing uses the outer IPv4 header as input for the load balancing hash except when transporting IPv4 in IPv4. With IPv4-in-IPv4 traffic the head node will load balance on the inner IPv4 header while intermediate and end nodes will load balance on the outer IPv4 header.



- PFOS supports a maximum of 16 directly connected pStack+ links between two neighbors; however, if more than 16 links are configured, PFOS will not display an error message. The two chassis select their own sets of 16 ports. When one chassis selects a connection but the other chassis does not select the same connection, this link is shown as invalid in the pfsMesh. PFOS will not try to re-establish the invalid link's connectivity, even if other pStack+ links are removed and the total number of directly connected pStack+ links is 16 or less. Users must manually re-establish the links by one of two ways:
  - Manually change the port class to Span or any non-pStack+ mode then change back to pStack+. Wait for several minutes; the port firmware will reset then recover the link.
  - Manually change Port Link State from Auto, to Force Down, and back to Auto.
- Due to a hardware limitation, pStack+ [flow map statistics](#) and pStack+ [tunnel statistics](#) for PFS 704x devices are not incremented; they will display a 0 value.

## Configuring a pfsMesh Using pStack+

Refer to the following sections to set up a pStack+ pfsMesh. Most of the process is similar to configuring pfsMesh using pStack, so the links in Step 2 below refer you to the pStack section for details. For a configuration example, refer to [pfsMesh Configuration Example Using pStack+](#).

1. [Configure pStack plus Port Settings](#)
2. [Configure Monitor Output with a pfsMesh](#)
  - Destination Nodes: [Configure Remote Monitor Port Group](#)
  - Head Node: [Configure Monitor Output to One or More Ports on Remote Nodes \(Traffic Maps\)](#)
  - [View Status of Remote Monitor Groups That are Used in a Traffic Map](#)

### Configure pStack plus Port Settings

For each node that will be part of the pfsMesh, determine which ports will be used to establish a pStack+ connection between two systems. Perform the following steps.

#### 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.



1. On the Port Settings page, click the port number link to open the settings page.

## Port 1-14 Settings

[Reset Port ▾](#)

[Basic](#)   [Advanced](#)   [References](#)

Name	<input type="text" value="string"/> A user friendly port name. Max length is 64.		
Class	<input type="radio"/> Span <input type="radio"/> Monitor <input type="radio"/> Span-Monitor <input type="radio"/> Service <input type="radio"/> pStack <input checked="" type="radio"/> pStack plus <input type="radio"/> Inline Network <input type="radio"/> Inline Monitor		
Link State	<input type="radio"/> Auto <small>Default: auto Port Link state</small>	Speed	<input type="text" value="1000"/> Port Speed (Mbits/sec)
		Auto Negotiations	<input type="radio"/> On <small>Default: on Port autonegotiations</small>
VLAN ID	<input checked="" type="radio"/> Default <input type="radio"/> User Defined	Link	up <small>Default: down Port Link status</small>
Source IP Address	<input type="text" value="14.14.14.14"/> Tunnel Source IP Address	Destination IP Address	<input type="text" value="13.13.13.13"/> Tunnel Destination IP Address
Gateway IP Address	<input type="text" value="14.14.14.1"/> Tunnel Gateway IP Address		

2. Set the Class to **pStack plus** for the port. See [Notes](#).
3. Perform one of the following:
  - **Indirect connections over IP network:** Enter the Source IP Address, Destination IP Address, and Gateway Address (optional) for the point-to-point tunnel that PFOS creates.  
**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.
  - **Direct connections:** Physically connect the pStack plus ports into the desired topography, using appropriate network cables. PFOS automatically assigns the Source and Destination IP addresses.  
**Note:** PFOS supports a maximum of 16 directly connected pStack+ links between two neighbors; refer to [pStack+ Limitations](#) for details about this limitation.
4. Each node automatically discovers all other interconnected nodes; each node has knowledge of all other nodes in the pfsMesh. Auto-discovery takes only a few seconds.
5. Go to the pfsMesh page, and verify the connection status of each node in the pfsMesh.



## Using the pfsMesh Page (pStack+)

The pfsMesh page is very similar for both pStack and pStack+ ports. Refer to [Using the pfsMesh Page \(pStack\)](#) for a general overview of this page; refer to the following sections for examples that include pStack+ details.

### Topology

The Topology tab displays information about each node currently in the pfsMesh, including whether the port is pStack or pStack plus. For remote nodes, you can click the IP address to access the Web UI for that node.

The screenshot shows the pfsMesh Topology page with three nodes listed:

- PFS6010-233 (10.250.177.233)**

ID	Platform	Type
C6BB00	PFS6010	remote

Local Node's Port	PFS6010_117's Port	Speed	Class
3-10	10.250.177.117	10G	pStack
- PFS5010\_117 (10.250.177.117)**

ID	Platform	Type
7AD0DC00	PFS5010	remote

Local Node's Port	PFS6010-233's Port	Speed	Class
1-25	10.250.177.233	10G	pStack

Local Node's Port	PFS5010_118's Port	Speed	Class
1-32	10.250.177.118	10G	pStack-plus
1-35	10.250.177.115	10G	pStack-plus
1-41	10.250.177.116	10G	pStack-plus

Local Node's Port	PFS5010_116's Port	Speed	Class
1-14	10.250.177.114	1G	pStack-plus
- PFS5010\_118 (10.250.177.118)**

ID	Platform	Type
9703D400	PFS5010	local

Local Node's Port	PFS5010_117's Port	Speed	Class
1-21	10.250.177.117	10G	pStack-plus
1-27	10.250.177.115	10G	pStack-plus
1-41	10.250.177.116	10G	pStack-plus

Local Node's Port	PFS5010_116's Port	Speed	Class
1-15	10.250.177.114	10G	pStack-plus
1-28	10.250.177.113	10G	pStack-plus



## pStack Map

The pStack Map tab displays all traffic maps created on this node via pStack and pStack+. The pStack map is present on a node if it is either a transit hop, a destination node, or both for this map. PFOS lists the following information:

- **Name:** Name of pStack map shown in the format:  
*head-node~name~tunnel key* for pStack+ maps  
*head-node~name~VLAN ID* for pStack maps  
where *head-node* is the node where the map was created, *name* is the user-specified map name, *tunnel key* is the input tunnel key, and *VLAN ID* is the VLAN ID assigned to the ingress port.
- **Filter Expression:** Filter expression provided by pStack (only applicable for pstack; displays "n/a" for pStack+ maps).
- **Input pStack Ports:** List of local pStack ports used as input.
- **Input pStack Plus Tunnel:** Local pStack+ tunnel used as input.
- **Output pStack Ports:** List of local pStack ports used as output.
- **Output pStack Plus Tunnel:** List of local pStack+ tunnels used as output to reach remote destination.
- **Output Monitor Groups:** Local output monitor port groups.
- **Priority:** Priority of this map.
- **Status:** Not displayed by default (for internal use only).

Name	Filter Expression	Input pStack Port	Input pStack Plus Tunnel	Output pStack Ports	Output pStack Plus Tunnels	Output Monitor Groups	Priority
9703D400-map_118_to_116_and_117-2293694465	n/a		67108864			PG116	2147483647
FFBA7C00-map_119_to_116_and_117-2259091457	n/a		67108880			PG116	2147483647

### Understanding pStack Map Input

A pStack Map input stack port is either a pStack port or a pStack Plus port.

- If the input stack port for the node is a *pStack* port, it displays in the **Input pStack Port** column and its associated filter displays in the **Filter Expression** column for this pStack Map.
- If the input stack port for the node is a *pStack plus* port, PFOS internally creates a VxLAN tunnel and the tunnel ID displays in the **Input pStack Plus Tunnel** column. In this case, the Filter Expression is not applicable for these pstack maps.



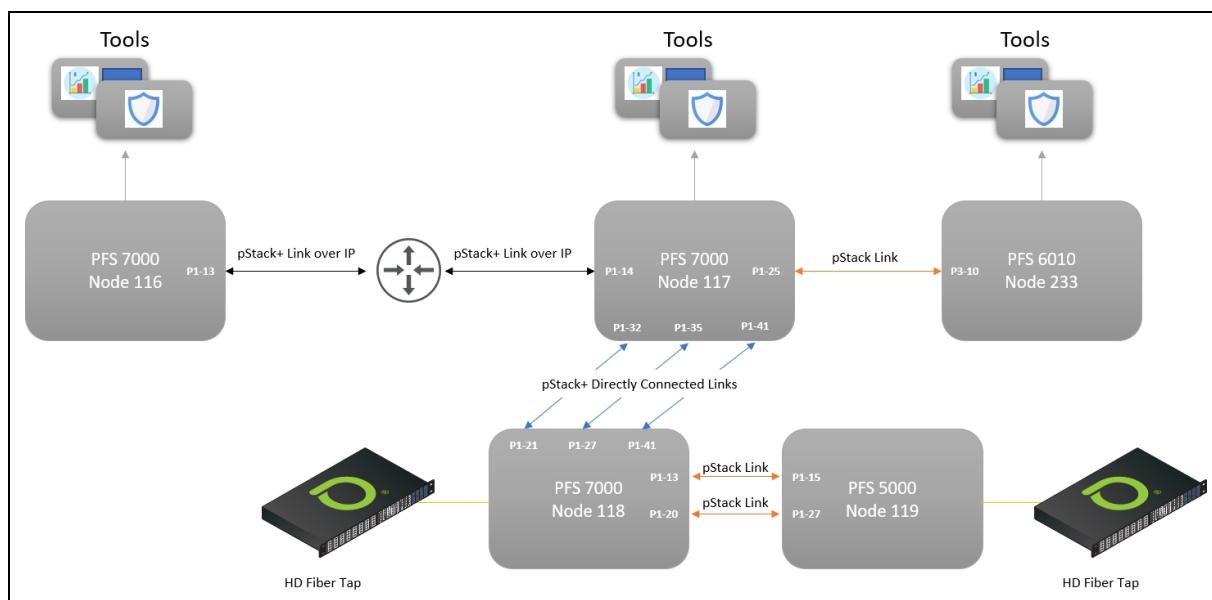
## Understanding pStack Map Output

pStack map output(s) can be a combination of any of the following: pStack port, pStack plus port, Local Output Monitor Group. If the pStack map needs to send traffic further downstream, output displays as either pStack ports or pStack plus tunnels. Output pStack port(s) are displayed in the **Output pStack Ports** column. If output is pStack plus ports, PFOS internally creates a VxLAN tunnel and the tunnel ID displays in the **Output pStack Plus Tunnels**.

If the pStack map has any local destinations, those display in the **Output Monitor Groups** column.

## pfsMesh Configuration Example Using pStack+

This section provides configuration details for the following pfsMesh example.



This example pfsMesh has:

- PFS 7000 Node 118 and PFS 5000 Node 119 as head (input) nodes on which traffic originally arrives in this pfsMesh
- pStack+ directly connected links between PFS 7000 Node 117 and PFS 7000 Node 118. These links function as a trunk and PFOS load balances traffic across them.
- pStack+ indirectly connected (over IP) links between PFS 7000 Node 116 and PFS 7000 Node 117
- pStack directly connected links between PFS 7000 Node 117 and PFS 6010 Node 233, and PFS 7000 Node 118 and PFS 5000 Node 119

Refer to the following sections for configuration details for the example topology.

- [Configure pStack+ Port Settings](#)
- [Configure pStack Port Settings](#)
- [Configure Remote Monitor Port Groups](#)



- [Configure Monitor Output to Ports on Remote Nodes \(Traffic Maps\)](#)
- [View pStack Map Data](#)

## Configure pStack+ Port Settings

For PFS 7000 devices Node 116, Node 117, and Node 118 in the [example topology](#), the following pStack+ port settings are configured on the Configuration>Port Settings page. Refer to [Configure pStack plus Port Settings](#) for configuration details.

PFS Device	Link	Port Details
PFS 7000 Node 116	pStack+ (Over IP)	<b>Port 1-13 to Port 1-14</b> on PFS 7000 Node 117 Users configure Source and Destination IPs for pStack+ ports over IP: Source IP: 13.13.13.13 Destination IP: 14.14.14.14 Gateway IP: 13.13.13.1 (optional)
PFS 7000 Node 117	pStack+ (Over IP)	<b>Port 1-14 to Port 1-13</b> PFS 7000 Node 116 Users configure Source and Destination IPs for pStack+ ports over IP: Source IP: 14.14.14.14 Destination IP: 13.13.13.13 Gateway IP: 14.14.14.1 (optional)
PFS 7000 Node 117	pStack+ (Directly Connected)	The following pStack+ ports physically connected using appropriate network cables. PFOS automatically assigns the Source and Destination IP addresses. <b>Port 1-32</b> (to Port 1-21 PFS 7000 Node 118) <b>Port 1-35</b> (to Port 1-27 PFS 7000 Node 118) <b>Port 1-41</b> (to Port 1-41 PFS 7000 Node 118)
PFS 7000 Node 118	pStack+ (Directly Connected)	The following pStack+ ports physically connected using appropriate network cables. PFOS automatically assigns the Source and Destination IP addresses. <b>Port 1-21</b> (to Port 1-32 PFS 7000 Node 117) <b>Port 1-27</b> (to Port 1-35 PFS 7000 Node 117) <b>Port 1-41</b> (to Port 1-41 PFS 7000 Node 117)



The following graphic shows the port settings for PFS 7000 Node 116 Port 1-13.

### Port 1-13 Settings

Reset Port ▾

Basic   Advanced   References

Name: string  
A user friendly port name. Max length is 64.

Class:  Span  Monitor  Span-Monitor  Service  pStack  pStack plus  Inline Network  Inline Monitor

Link State: Auto  
Default: auto  
Port Link state

Speed: 1000  
Port Speed (Mbits/sec)

Auto Negotiations: On  
Default: on  
Port autonegotiations

VLAN ID:  Default  User Defined

Link: up  
Default: down  
Port Link status

Source IP Address: 13.13.13.13  
Tunnel Source IP Address

Destination IP Address: 14.14.14.14  
Tunnel Destination IP Address

Gateway IP Address: 13.13.13.1  
Tunnel Gateway IP Address

The following graphic shows the port settings for PFS 7000 Node 117 Port 1-14.

### Port 1-14 Settings

Reset Port ▾

Basic   Advanced   References

Name: string  
A user friendly port name. Max length is 64.

Class:  Span  Monitor  Span-Monitor  Service  pStack  pStack plus  Inline Network  Inline Monitor

Link State: Auto  
Default: auto  
Port Link state

Speed: 1000  
Port Speed (Mbits/sec)

Auto Negotiations: On  
Default: on  
Port autonegotiations

VLAN ID:  Default  User Defined

Link: up  
Default: down  
Port Link status

Source IP Address: 14.14.14.14  
Tunnel Source IP Address

Destination IP Address: 13.13.13.13  
Tunnel Destination IP Address

Gateway IP Address: 14.14.14.1  
Tunnel Gateway IP Address



The following graphic shows the port settings for PFS 7000 Node 117 Port 1-32. These same settings are configured for the directly connected pStack+ ports between PFS 7000 Node 117 and PFS 7000 Node 118.

**Port 1-32 Settings** Reset Port ▾

**Basic** Advanced References

Name:  A user friendly port name. Max length is 64.

Class:  Span  Monitor  Span-Monitor  Service  pStack  pStack plus  Inline Network  Inline Monitor

Link State:  Default: auto Port Link state

Speed:  Port Speed (Mbps/sec)

VLAN ID:  Default  User Defined

Link: up Default: down Port Link status

Source IP Address:  Tunnel Source IP Address

Destination IP Address:  Tunnel Destination IP Address

Gateway IP Address:  Tunnel Gateway IP Address

Port ID:  Go Enter port id to navigate

### Configure pStack Port Settings

For PFS 7000 devices 117, 233, 118, and 119 in the [example topology](#), the following pStack port settings are configured on the Configuration>Port Settings page. Refer to [Configure pStack Port Settings](#) for configuration details. These pStack ports are physically connected using appropriate network cables.

PFS Device	Link	Port Details
PFS 7000 Node 117	pStack (Directly Connected)	<b>Port 1-25</b> (to Port 3-10 PFS 6010 Node 233)
PFS 6010 Node 233	pStack (Directly Connected)	<b>Port 3-10</b> (to Port 1-25 PFS 7000 Node 117)
PFS 7000 Node 118	pStack (Directly Connected)	<b>Port 1-13</b> (to Port 1-15 PFS 5000 Node 119) <b>Port 1-20</b> (to Port 1-27 PFS 5000 Node 119)
PFS 5000 Node 119	pStack (Directly Connected)	<b>Port 1-15</b> (to Port 1-13 PFS 5000 Node 119) <b>Port 1-27</b> (to Port 1-20 PFS 5000 Node 119)



The following graphic shows the port settings for PFS 7000 Node 117 Port 1-25. These same settings are configured for the directly connected pStack ports between PFS 7000 Node 118 and PFS 5000 Node 119.

The screenshot shows the 'Port 1-25 Settings' page with the 'Basic' tab selected. It includes fields for Name (string), Class (pStack selected), Link State (Auto), Speed (10000), VLAN ID (Default selected), and Link status (up).

## Configure Remote Monitor Port Groups

Remote monitor port groups are configured on the appropriate destination nodes. Up to 64 remote monitor groups can be created on a single system. A port can belong to more than one remote monitor group. Optionally, a remote monitor group also can contain a load balance group.

For PFS 7000 devices Node 116 and Node 117, and PFS 6010 device Node 233 in the [example topology](#), the following port groups are configured on the Configuration > Port Groups page. Setting the pfsMesh option to **Enable** allows this port group to be visible across the pfsMesh. Refer to [Configure Remote Monitor Port Group](#) for configuration details.

PFS Device	Port Group	Selected Monitor Output Ports	pfsMesh
PFS 7000 Node 116	PG116	1-32	Enable
PFS 7000 Node 117	PG117A	1-45, 1-52	Enable
	PG117B	1-1	Enable
PFS 6010 Node 233	PG6010	3-1	Enable

The following graphic shows the Monitor Port group configuration page for PG116 for PFS 7000 Node 116, Port 1-32.

The screenshot shows the 'PG116' configuration page. It includes fields for Ports (configure), Selected Ports (1-32), Lb Criteria (Load-balance criteria), Load Balance Groups (Add an entry...), and pfsMesh (Enable selected). Status information shows PortGroupNameResolved.



## Configure Monitor Output to Ports on Remote Nodes (Traffic Maps)

All traffic maps for pfsMesh are configured only on the head (input) nodes; that is, the nodes on which traffic originally arrives in the pfsMesh. In the [configuration example](#), both PFS 7000 Node 118 and PFS 5000 Node 119 are head (input) nodes, and have the following maps configured:

- Traffic Map for PFS 7000 Node 118 to PFS 7000 Node 117 (map\_118\_to\_117)
- Traffic Map for PFS 7000 Node 118 to PFS 7000 Node 117 and PFS 7000 Node 116 (map\_118\_to\_116\_and\_117)
- Traffic Map for PFS 7000 Node 118 to PFS 6010 Node 233 (map\_118\_to\_233)
- Traffic Map for PFS 5000 Node 119 to PFS 7000 Node 117 and PFS 7000 Node 116 (map\_119\_to\_116\_and\_117)

Node Map Created On	Name	Type	Description	Mode	Filter	Input Ports	Output Ports	Remote Monitor Groups	Action
PFS 7000 Node 118	map_118_to_117	Monitor	<ul style="list-style-type: none"><li>Raw unfiltered traffic from input port 1-17 is forwarded to Port 1-31 and Remote Monitor Group PG117_A.</li></ul>	Basic	unfiltered	1-17	1-31	PG117_A	Forward
PFS 7000 Node 118	map_118_to_116_and_117	Monitor	<ul style="list-style-type: none"><li>Raw unfiltered traffic from input ports 1-22, 1-33, 1-35, 1-42 is processed against mac_dest filter.</li><li>Packets matching mac_dest filter are forwarded to Remote Monitor Groups PG116 and PG117_B.</li></ul>	Basic	mac_dest	1-22, 1-33, 1-35, 1-42		PG116, PG117_B	Forward
PFS 7000 Node 118	map_118_to_233	Monitor	<ul style="list-style-type: none"><li>Raw unfiltered traffic from input ports 1-40, 1-43, 1-48, 1-49 is processed against IP_src filter.</li><li>Packets matching IP_src filter are forwarded to Remote Monitor Group PG6010.</li></ul>	Basic	IP_src	1-40, 1-43, 1-48, 1-49		PG6010	Forward



Node Map Created On	Name	Type	Description	Mode	Filter	Input Ports	Output Ports	Remote Monitor Groups	Action
PFS 5000 Node 119	map_ 119_to_ 116_and_ 117	Monitor	<ul style="list-style-type: none"><li>Raw unfiltered traffic from input ports 1-14, 1-22, 1-29 is processed against IP_dst filter.</li><li>Packets matching IP_dst filter are forwarded to Remote Monitor Groups PG116 and PG117_A.</li></ul>	Basic	IP_dst	1-14, 1-22, 1-29		PG116, PG117_A	Forward

The following graphics show the traffic map summary pages for PFS 7000 Node 118 and PFS 5000 Node 119.

### Traffic Maps

Filter Resources

Add ... Delete Move Merge

Showing 1 to 3 of 3

Name	Description	Type	Mode	Filter	Input Ports	Network Port Groups	Monitor Port Groups	Output Ports	Remote Monitor Groups	Output LBGs	Inline Network Group	Load Balance Criteria	Input Tunnels	Output Tunnels	Map Status - State
map_118_to_117		Monitor	Basic	unfiltered	1-17			1-31	PG117_A						enable
map_118_to_116_and_117		Monitor	Basic	mac_dest	1-22, 1-33, 1-35, 1-42				PG116, PG117_B						enable
map_118_to_233		Monitor	Basic	IP_src	1-40, 1-43, 1-48, 1-49				PG6010						enable

### Traffic Maps

Filter Resources

Add ... Delete Move Merge

Showing 1 to 1 of 1

Name	Description	Type	Mode	Filter	Input Ports	Network Port Groups	Monitor Port Groups	Output Ports	Remote Monitor Groups	Output LBGs	Inline Network Group	Load Balance Criteria	Input Tunnels	Output Tunnels	Map Status - State
map_119_to_116_and_117		Monitor	Basic	IP_dst	1-14, 1-22, 1-29				PG116, PG117_A						enable



## View pStack Map Data

pStack Map Data can be viewed for transit or destination nodes in a pfsMesh. Refer to [pStack Map](#) for details about this window.

### Understanding pStack Map Input

A pStack Map input stack port is either a pStack port or a pStack Plus port.

- If the input stack port for the node is a *pStack* port, it displays in the **Input pStack Port** column and its associated filter displays in the **Filter Expression** column for this pStack Map (refer to the pStack Maps for both [PFS 7000 Node 118](#) and [PFS 6010 Node 233](#) as examples).
- If the input stack port for the node is a *pStack plus* port, PFOS internally creates a VxLAN tunnel and the tunnel ID displays in the **Input pStack Plus Tunnel** column. In this case, the Filter Expression is not applicable for these pstack maps. Refer to the pStack Maps for both [PFS 7000 Node 117](#) and [PFS 7000 Node 116](#) as examples.

### Understanding pStack Map Output

pStack map output(s) can be a combination of any of the following: pStack port, pStack plus port, Local Output Monitor Group. If the pStack map needs to send traffic further downstream, output displays as either pStack ports or pStack plus tunnels. Output pStack port(s) are displayed in the **Output pStack Ports** column (see [PFS 7000 Node 117](#)). If output is pStack plus ports, PFOS internally creates a VxLAN tunnel and the tunnel ID displays in the **Output pStack Plus Tunnels**; see [PFS 7000 Node 117](#) and [PFS 7000 Node 118](#).

If the pStack map has any local destinations, those display in the **Output Monitor Groups** column (see [PFS 7000 Node 116](#) and [PFS 6010 Node 233](#)).

### PFS 7000 Node 117 pStack Map

The following graphic is the pStack Map page for PFS 7000 Node 117, a transit node in the [example configuration](#).

Name	Filter Expression	Input pStack Port	Input pStack Plus Tunnel	Output pStack Ports	Output pStack Plus Tunnels	Output Monitor Groups	Priority
9703D400-map_118_to_116_and_117-2293894465	n/a	67108864		67108880		PG117_B	2147483647
9703D400-map_118_to_117-2293894466	n/a	67108896				PG117_A	2147483647
9703D400-map_118_to_233-2293894467	n/a	67108944	1-25				2147483647
FFBAC7C00-map_119_to_116_and_117-2259091457	n/a	67108912		67108928		PG117_A	2147483647



## PFS 7000 Node 116 pStack Map

The following graphic is the pStack Map page for PFS 7000 Node 116, a destination node in the [example configuration](#).

Name	Filter Expression	Input pStack Port	Input pStack Plus Tunnel	Output pStack Ports	Output pStack Plus Tunnels	Output Monitor Groups	Priority
9703D400-map_118_to_116_and_117-2293694465	n/a	67108864				PG116	2147483647
FF8A7C00-map_119_to_116_and_117-2259901457	n/a	67108860				PG116	2147483647

## PFS 7000 Node 118 pStack Map

The following graphic is the pStack Map page for PFS 7000 Node 118, a head node and transit node in the [example configuration](#).

Name	Filter Expression	Input pStack Port	Input pStack Plus Tunnel	Output pStack Ports	Output pStack Plus Tunnels	Output Monitor Groups	Priority
FFBA7C00-map_119_to_116_and_117-2176	VLAN 2176 and (IP Dest 5.5.5.5)	1-13			67108896		0
FFBA7C00-map_119_to_116_and_117-2177	VLAN 2177 and (IP Dest 5.5.5.5)	1-13			67108912		0
FFBA7C00-map_119_to_116_and_117-2178	VLAN 2178 and (IP Dest 5.5.5.5)	1-13			67108928		0

## PFS 6010 Node 233 pStack Map

The following graphic is the pStack Map page for PFS 6010 Node 233, a destination node in the [example configuration](#).

Name	Filter Expression	Input pStack Port	Output pStack Ports	Output pStack Plus Tunnels	Output Monitor Groups	Priority
9703D400-map_118_to_233-165	VLAN 165 and (IP Source 5.5.5.5)	3-10			PG6010	2
9703D400-map_118_to_233-166	VLAN 166 and (IP Source 5.5.5.5)	3-10			PG6010	2
9703D400-map_118_to_233-167	VLAN 167 and (IP Source 5.5.5.5)	3-10			PG6010	2
9703D400-map_118_to_233-168	VLAN 168 and (IP Source 5.5.5.5)	3-10			PG6010	2



## Port Mirroring and Packet Slicing

**Note:** The Port Mirroring feature requires the PFS 7000 functionality license and is supported on all PFS 7000 devices. [Packet slicing](#) is only supported as part of the port mirroring feature on PFS 703x and PFS 704x devices.

Refer to the following sections for details:

- [Port Mirroring](#)
- [Packet Slicing](#)
- [Port Mirroring and Packet Slicing Limitations and Considerations](#)

### Port Mirroring

The Port mirroring feature duplicates traffic from one or more source ports and sends the duplicated traffic to a destination for analysis. Users configure port mirror sessions by defining source ports and an associated destination (port or Load Balance Group). Mirroring is an independent feature that does not affect the traffic configured using [Traffic Maps](#). PFOS supports the following mirroring functionality:

- Mirroring Ingress and/or Egress Packets
  - Users can create a mirroring session to duplicate ingress traffic only, egress traffic only, or both ingress and egress traffic for each source port to one destination. Note: When mirroring both traffic directions on Service ports, the destination will receive double of packets to the Service ports.
  - Mirroring can also help in troubleshooting and debugging scenarios.
- Mirroring Packets Through a Traffic Map
  - 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.

See also [Port Mirroring and Packet Slicing Limitations and Considerations](#) for details.

### Create a Port Mirroring Session

**Note:** PFS 704x devices support a maximum of four mirror sessions.

Perform the following steps to create a port mirroring session. If you will be configuring slicing for a mirror session refer to [Packet Slicing](#) for details prior to starting this procedure.

1. Open the **Applications>Mirror** page and click **Add**.
2. On the Add New Session page, enter a name to identify the mirror session and click **Add**. A new Mirror Session page opens for you to add a source interface and destination.
3. If applicable, [enable slicing](#).



**MirrorSession1** × Mirror Session

Slicing  Enable slicing on mirrored packets.

▲ Destination Configure the mirror destination

Interface  Load Balance Group

▲ Source Interface List of source interface

Add ... Delete

Interface	Direction
-----------	-----------

4. Configure a Destination (Port or Load Balance Group):
  - a. **Port:** Click **Interface** and select the port number you want for the destination. The destination port can only be MON or SPAN-MON port class.
  - b. **LBG:** Click **Load Balance Group** and select the name of an existing LBG 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).
5. Configure a source port:

**Note:** If [associating a mirror session with a traffic map](#), source interfaces are not required because PFOS uses the Ingress ports defined in the traffic map.

  - a. Click **Add**, select a port number and click **OK**, and then **Add**. The source port can be any port class.
  - b. Select the direction of the traffic that PFOS will mirror (**TX**, **RX**, or **Both**). **Note:** If mirroring both traffic directions on Service ports, the destination will receive double the number of packets due to loopback to the Service ports.
  - c. If adding multiple source ports, repeat these steps until all source ports are added.
6. Click **Apply**.

**Note:** You can also [configure a notification](#) for the mirror session on the Notifications>Events>Config Notification page. A mirror-session option is available for you to select the Notifications you want.



## Associating a Mirror Session with a Traffic Map

After creating a mirror session, you can [associate it with a traffic map](#). Packets matching the traffic map filters are duplicated to the destination defined in the mirroring session. Mirroring sessions associated with traffic maps do not require source interfaces because PFOS uses the Ingress ports defined in the traffic map.

## Packet Slicing

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. Enabling slicing reduces the volume of storing and transmitting unnecessary data, as well as improving traffic volume across PFOS systems, thereby enhancing efficiency and scalability of tools.

Packet slicing is only supported as part of the port mirroring feature on PFS 703x and PFS 704x devices. PFS 704x systems support an additional option to configure the slicing offset value; refer to [Enable Slicing](#) for details.

## Enable Slicing

**Note:** [Packet slicing](#) is only supported as part of the port mirroring feature on PFS 703x and PFS 704x devices.

Enabling the Slicing feature for port mirroring sessions requires you to configure two settings: Global Configuration and Mirror Session Configuration.

### Global Configuration

If you want the packet slicing option accessible for mirror session configuration, you must first enable it on the [Global Settings> System>Features](#) page. When slicing is enabled, 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)

PFS 704x systems provide an additional option enabling you to 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



The screenshot shows the 'System' tab in the PFOS interface. Under the 'Features' tab, the 'Slicing' checkbox is checked, and the 'Slicing Offset' field is set to 30. Both fields are highlighted with a red box.

## Mirror Session Configuration

Once Slicing is enabled in Global Settings, you can enable slicing for each mirroring session; refer to [Create a Port Mirroring Session](#) for details.

### Packet Slicing Examples

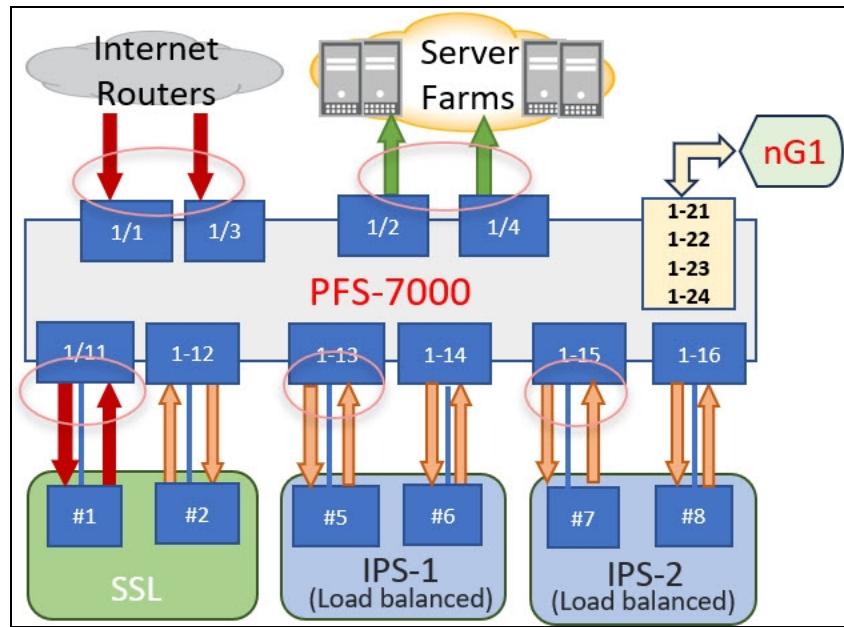
- PFS 703x supports **fixed** size slicing:
  - With Mirror Slicing configured, packets will be sliced to the default length (192 bytes) from the start of the L2 header of the packets.
- PFS 704x supports **fixed** and **variable** packet slicing:
  - With Mirror Slicing configured without a slicing-offset setting, packets will be sliced to the default length (190 bytes) from the start of the L2 header of the packets.
  - Variable slicing can be achieved with a *slicing offset*, a setting value between 30 to 60 bytes.

	IPv4 Pkts	IPv6 Pkts	UDP Pkts	IPv6 UDP	GRE Pkts	VxLAN Pkts	GPTv1 Pkts	L3 MPLS 5-Label	L2 MPLS 5-Label
<b>L2 Header Length (bytes)</b>	14	14	14	14	14	14	14	14	14
<b>L3 Header Length (bytes)</b>	20	40	20	40	20	20	20	0	0
<b>L4 Header Length (bytes)</b>	x	x	8	8	0	8	8	0	0
<b>Extra Header Bytes</b>	x	x	x	x	4	8	0	20	20
<b>Unknown Extra Bytes*</b>	x	4	8	8	x	x	8	x	4
<b>Header Bytes</b>	34	58	50	70	38	50	50	34	38
<b>PFS-704x Slicing Offset = 30</b>	64	88	80	100	68	80	80	64	68
<b>PFS-704x Slicing Offset = 63</b>	97	121	113	133	101	113	113	105	108
<b>PFS-703x default Slicing = 192</b>	192	192	192	192	192	192	192	192	192
<b>PFS-704x default Slicing = 190</b>	190	190	190	190	190	190	190	190	190

**Note:** The “Unknown Extra Bytes” are based on internal NETSCOUT testing results.

### Port Mirroring and Packet Slicing Use Case

Refer to the following diagram for the use case examples.



- Mirroring Inline Tool Chain Traffic**

Mirror sessions are not supported on inline traffic maps. However, PFOS supports mirroring inline interface traffic. The following table provides examples.

	<b>Source</b>	<b>Direction</b>	<b>Destination</b>	<b>Resource</b>
<b>Mirror_INT-Ingress</b>	1-1	RX	1-21	1
	1-3	RX		
<b>Mirror_Server-Egress</b>	1-2	TX	1-22	2
	1-4	TX		
<b>Mirror_SSL-ASide</b>	1-11	Both	1-23	2
<b>Mirror_IPS-ASide</b>	1-13	Both	1-24	2
	1-15	Both		

- Slicing Packets before Mirroring Traffic to ISNG**

Using the same LBG **ISNG** for traffic map and mirroring destination.

- Keep GTP control packets sizes but Reduce GTP User packets sizes :

```
load-balance-group ISNG ports [ 1-41 1-42 ]
mirror-session Mirror_GTP
slicing
destination load-balance-group ISNG
```

- No slicing on GTP Control Packets:

```
map GTPc filter gtp-c input_ports [ 1-31 1-32 1-33 1-34 ] output_
load_balancing_group ISNG
```

- Slicing GTP User Packets:

```
map GTPu filter gtp-u input_ports [ 1-31 1-32 1-33 1-34 ] mirror-
session Mirror_GTP
```



## Port Mirroring and Packet Slicing Limitations and Considerations

### Limitations for all PFS 7000 devices

- Mirror sessions are not supported on inline traffic maps.
- Ports (SPAN-MON ports) configured with tunnel cannot be used as mirror source or destination (interface or LBG).
- In Egress mirroring, replicated packets will only be copied (mirrored) once per mirror session. The following example illustrates if a packet from one Span port (port 1-1) is replicated to three Monitor ports (ports 1-11, 1-12, and 1-13 via a traffic map) and those three Monitor ports are used as source ports for a single mirror session (Mirror-Session-1), only a single copy of the packet will be sent to the mirror session destination. In this example port 1-21 will only receive one replicated copy from port 1-1.

	SPAN	MON	Mirror Session List
Traffic-Map	1-1	1-11 1-12 1-13	
	Source	Direction	Destination
Mirror-Session-1	#1-11	TX	1-21
	#1-12	TX	
	#1-13	TX	

### Limitations when Using Load Balance Groups as Mirror Session Destinations

- PFS 704x devices do not support load balance groups as a mirror session destination.
- A load balance group used on a mirror session should not be [PFX enabled](#).
- A load balance group used on a mirror session should not have any [tunnels configured](#).
- PFS can only support one [Load Balance Criteria \(LBC\)](#) per device. Mirror sessions using an LBG as a destination will use the existing LBC configured on a traffic map or a monitor port group (MPG). If no traffic map or MPG is configured, it uses the default LBC (SIP and DIP).
- The [Weighted Redistribute LBG failover action](#) does not fully function with mirror session.

### Limitations for all PFS 7000 devices except PFS 704x

- PFS hardware can support four resources for mirroring sessions. Refer to the following examples **PFS-01** and **PFS-02**.
- Each session uses one resource even if a source interface has not been configured (refer to PFS-01: Session#0).
- One resource is used for Rx in default even if no direction=RX is configured (refer to PFS-01: Session#2).
- One direction (TX or Both) uses one additional resource (refer to PFS-02: Session#3 and Session#4).
- One mirror session can use up to two resources. Since one resource for RX in default, a mirror session can include most directions as "RX & Both" or "RX & TX".



PFS-01	Source	Direction	Destination	Resource	PFS-02	Source	Direction	Destination	Resource
Session#0			#1-10	1	Session#3	#1-3	Both	#1-13	2
Session#1	#1-1	RX	#1-11	1		#1-4	RX		
Session#2	#1-2	TX	#1-12	2		#1-5	TX		
<b>Total Resources in use = 4 so no more sessions</b>									
<b>Total Resources in use = 4, so no more sessions</b>									

### Limitations on PFS 704x

- PFS 704x devices support a maximum of four mirror sessions (no hardware “resource” limitations).
- PFS 704x devices do not support load balance groups as a mirror session destination.

PFS-704x	Source	Direction	Destination
<b>Session#0</b>			1-10
<b>Session#1</b>	1-1	RX	1-11
<b>Session#2</b>	1-2	TX	1-12
	1-3	Both	1-13
<b>Session#3</b>	1-4	RX	1-14
	1-5	TX	
	1-6	Both	
<b>Up to 4 mirror sessions, No “Resource” limitations</b>			

## 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. They can be enabled or disabled on a per-port basis on the Port Settings page Advanced tab. For details about PFS 5000/7000 enhanced port features, refer to [PFS 5000/7000 Enhanced Port Features](#).

- [Packet Deduplication](#)
- [Port and Time Stamping](#)
- [Protocol De-encapsulation and Stripping](#)
- [Conditional Packet Slicing](#)
- [Conditional Packet Masking](#)
- [Extended Load Balancing](#)

### Packet Deduplication

**Note: The Packet Deduplication feature in this section is only available on PFS 6000 Series systems. Packet deduplication is available on PFS 5000/7000 systems with the use of PFX; refer to the PFX documentation for details.**

When accessing data from networks, duplicates of packets are often captured and aggregated together. This then requires that the tools identify and remove the duplicate packets, and if not, the tools will alarm on the duplicates or produce compromised data and results.



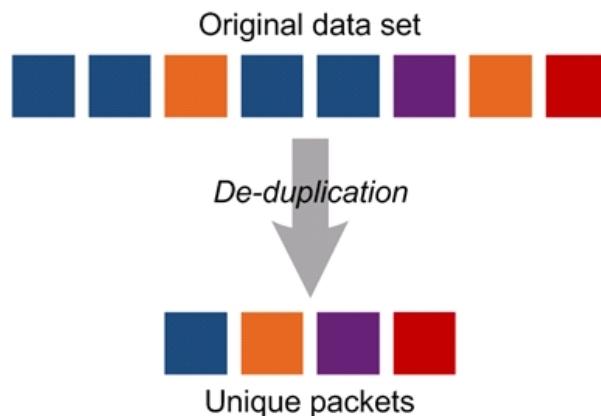
Typical causes of duplication include planned redundancies in network and monitoring design and filter overlap during traffic capture and aggregation, both leading to duplicate packets. This creates challenges such as consumption of bandwidth on a monitoring tool's receiving port, usage of valuable monitoring tool processing resources resulting in decrease of actual processing bandwidth, and generation of false positive errors reported in monitoring tools.

PFOS' ability to remove duplicates provides a substantial reduction in the volume of traffic to the tools, an increase in tool efficiency, reduction in errors on the monitoring tool, and closure of security holes that exist in other implementations.

Deduplication capabilities include:

- Selective packet de-duplication.
- Keyed secure hash for identifying duplicates.
- Configurable packet/time window.
- Full 10G line rate de-duplication per port.
- Discarding of all subsequent duplicates of any packet (within the specified time window).
- Generation of duplicated traffic statistics.

Deduplication is available on the 40SadvR line card for eight ports in each group, allowing up to 24 ports of deduplication per line card.



Three port classes are supported for packet de-duplication:

- **Span port:** Removes duplicates from packets as they arrive into the individual input port, prior to any aggregation, filter, or load balancing mapping.
- **Monitor port:** Removes duplicates from packets prior to sending out the individual port, after any aggregation, filter, or load balancing mapping.
- **Service port:** Removes duplicates from packets after aggregation, filter, or load balancing mapping from input ports and prior to aggregation, filter, or load balancing mapping towards output ports.

On a per-port basis, you can specify one or more fields that are to be ignored when comparing packets to determine whether duplicates exist. Available fields to ignore are:

- MAC address
- VLAN tags



- MPLS labels
- TOS/COS field
- TTL field
- Identification field
- Time stamp
- Port stamp

Also, you can specify a time window of between 1 and 4,000 milliseconds for tracking and comparison for each unique packet.

Traffic statistics available for de-duplication, on a per-port basis, are:

- Total packets received.
- Total duplicates received and discarded.
- Total unique packets forwarded.

## Enable Packet De-duplication

1. On the Applications page, select the **Deduplication** tab.
2. Click **Add**.
3. In the Name field, enter a name to identify the new entry.
4. Click **Add** to save the new entry and open the configuration page.
5. In the Layer 2, Layer 3, and End of Frame sections, select one or more checkboxes if you want to exclude fields from duplicate packet detection.
6. Specify a time window in milliseconds for tracking and applying deduplication.

The screenshot shows the 'vlan-ignore-dd' configuration page. At the top, there's a title bar with the name 'vlan-ignore-dd' and a close button. To the right of the title is a 'New Deduplication...' button. Below the title, there's a note: 'Use the check boxes, below to select packet fields to ignore (i.e. exclude) from duplicate packet detection.' Under 'Layer 2', 'MAC Header' and 'MPLS labels' are unchecked, while 'VLAN Tags' is checked. Under 'Layer 3', 'Type/Class of Service', 'Identification', and 'Time to Live' are unchecked. Under 'End of Frame', 'Time Stamp' and 'Port Stamp' are unchecked. A 'Time Window (milliseconds)' input field contains '1000', with a note below it stating 'Default: 10' and 'Valid values: 1—4000'. Below this is a section titled '^ Port List' which says 'De-duplication application library'. It shows a table with a single row containing 'Port Name' and '10-1'. At the bottom right of the table is the text 'Showing 1 to 1 of 1'.

7. Click **Apply** in the toolbar to save the settings to the running configuration.



8. Go to the Advanced tab of the Port Settings page for the desired port. See [Configuring Ports](#) for information on accessing the port settings pages.
9. Select the check box to enable the de-duplication feature, and click **Add** to create a new entry. Specify a name to identify the new entry, and click **Add** to create the entry and display the settings.

## Port and Time Stamping

**Note:** The port and time stamping options in this section are available only on PFS 6000 Series systems. For information about time stamping on PFS 7000 Series systems, refer to [PFS 7000 Timestamping](#).

Port and time stamping are available on the 40SadVR line card for up to six ports in each group of 14 with the Deduplication image, allowing up to 16 ports of stamping per line card, or all 14 ports with the Slicing image, allowing up to 40 ports of stamping.

### Port Stamping

Port stamping allows, on an input network port basis, the addition of a single or double byte to the end of the payload of each packet, immediately before the CRC (in the packet's trailer), indicating the input port of the system on which the packet was captured. The CRC is recalculated after the addition of the port stamp to preserve the integrity of the packet, thereby enabling the port stamped packet to be added to the destination ports as a standard Ethernet packet.

There are two port numbering methods for the byte stamp: single-byte and dual-byte. For the single-byte method, the first port is numbered 0 at the furthest left and uppermost port (by conceptually turning the line card on its side). From there, PFOS counts sequentially down the column of ports and moves on to the next column on the right, starting from the top down again, and so on, until all ports are counted for each line card slot, before moving on to the next slot. After the numbering reaches 255, it will stay at 255 for the rest of the ports.

For the dual-byte method, the ports are numbered in accordance with the value of the port minus 1. (Port stamp numbering is zero-based.)

For example, the following packet shows the single-byte port stamp 04 in a red box, and the four-byte recalculated CRC in a blue box.

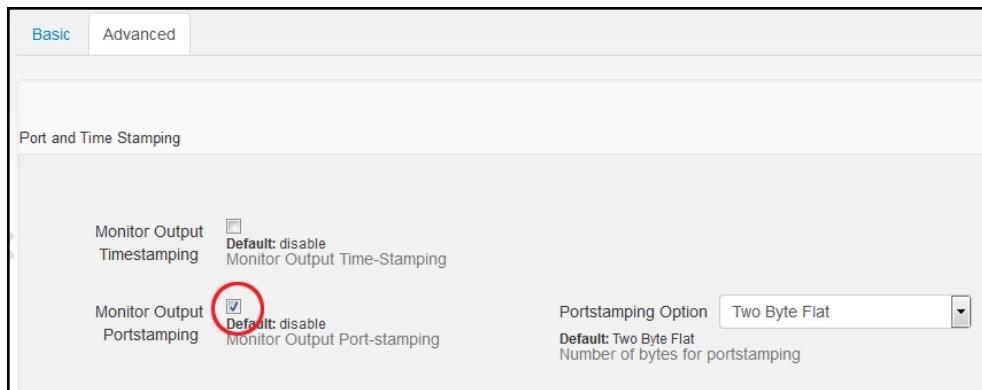
1440: 24 05 E4 0D 48 0B C8 1A - 98 17 98 34 20 2F 20 68
1456: 40 5E 40 D0 <b>04</b> 8D EF 7E - <b>10</b>

### Enable Port Stamping

1. Go to the Port Settings page for the port on which you want to configure port stamping.
2. Click the **Advanced** tab.
3. In the Monitor Output Portstamping section, select the checkbox.
4. Select **One Byte Flat** or **Two Byte Flat** as the portstamping option (Two Byte Flat is the default).



5. Click **Apply** in the toolbar to save the settings to the running configuration.



## Time Stamping

Time stamping provides, on an input network port basis, the addition of an eight-byte time stamp to the end of the data payload of each packet.

The eight-byte (64-bit) time stamp has this format:

**Table 5.2 - 64-bit Time Stamp Format**

Bits	Description
0-31	Time in seconds since Epoch (00:00:00 GMT January 1, 1970)
32-61	Subsecond time in nanoseconds, in 20nsec increments
62-63	Time synchronization source: 00: Uncalibrated; internal clock only 01: NTP synchronization 10: GPS (1PPS with TSIP) or 1PPS-only synchronization 11: PTP synchronization

The first four bytes count in seconds, and the second four bytes count in nanoseconds. These two groups of bytes are effectively separated by a decimal point. The time stamp is created as the first bit enters the input Network port.

For example, the following packet shows the eight-byte time stamp in a red box, and the four-byte recalculated CRC in a blue box. The value of the time stamp is 00000B7F = 2,943 seconds since Epoch time, 002DC940 = 3000640ns = 0.003000640 seconds, and 0 = internal clock source. The resulting value is 2943.003000640 seconds.

0896:	00 00 00 00 00 00 00 00	-	00 00 00 00 00 00 00 00
0912:	00 00 00 00 00 00 00 00	-	00 00 00 00 00 00 7F 00 20
0928:	C9 40 02 86 D7 52		

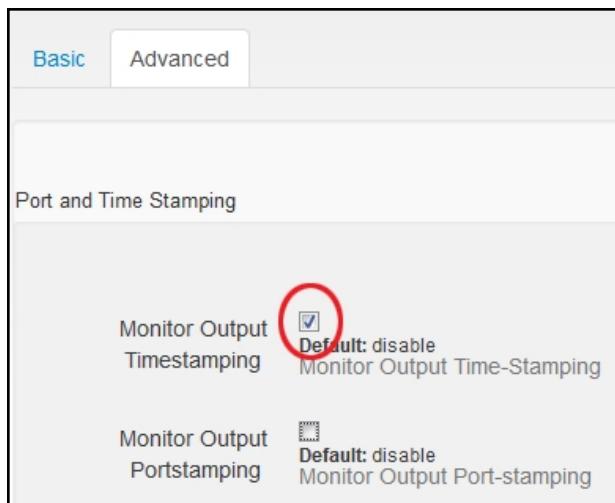
Time stamp values start at 0.0 seconds from PFOS boot time, but then switch over to values referenced to Epoch time as soon as the system time is accepted as stable. This can take a few minutes following boot. Each time stamp value is the number of seconds since Epoch time,



which is 00:00 UTC 1st January 1970, and does not take into account the leap seconds adjustment. All ports are exactly synchronized with one another because they use the same clock source. The timestamp is in TAI (Temps Atomique International) format.

## Enable Time Stamping

1. Go to the Port Settings page for the port on which you want to configure time stamping.
2. Click the **Advanced** tab.
3. In the Monitor Output Timestamping section, select the checkbox.
4. Click **Apply** in the toolbar to save the settings to the running configuration.



## About Time Stamp Synchronization Sources

Time stamp values can be based on either the internal clock source or an external clock source such as NTP, GPS, 1PPS with NTP (for time of day), PTP, or 1PPS with PTP (for time of day). Note that PTP requires correct time during initialization, so it is recommended that NTP be set to ensure proper time is loaded.

While time stamps between ports on the same system will be within plus or minus 8nsec regardless of time source, synchronization is important to ensure that time stamps between systems maintain a specific accuracy and do not drift too far apart.

GPS synchronization is based on receipt of a 1PPS signal and the Trimble Standard Interface Protocol (TSIP) for time of day and other ephemeral data.

PTP synchronization requires communication with a PTP master clock server over an Ethernet or IP network, where the system will be a PTP slave.

If the system that performs time stamping is equipped with the PTP option, and GPS or 1PPS with NTP is also being used as the synchronization source, then the PTP port becomes a PTP master clock, which can then be used to synchronize other systems that are equipped with the PTP option.



## About Time Stamp Accuracy

Although the time stamp is provided in nanoseconds, several accuracy characteristics must be understood:

- A packet must be deserialized, unscrambled, and decoded before being time stamped. This processing causes a small delay on the input ports. This delay has some nondeterministic components to it due to the way Ethernet interfaces function. In addition, there is always the possibility of a packet arriving just as the timing clock ticks. These two factors can lead to a non-deterministic jitter of plus or minus the "timing tick interval," making it possible that two simultaneously arriving packets on two ports could be stamped with a difference of as much as two times the "timing tick interval" between them. However, the likelihood of a packet (arriving after another packet) being stamped with a time more recent (than the other packet) is negligible.
- The time stamp "timing tick interval" is 8nsec for 1G ports and 6.5nsec for 10G ports, which gives the actual resolution of the time stamps.
- The hardware deserialization and decoding procedures for 10G fiber, 1G fiber, and 1G copper interfaces are not the same, and each type offers a differing static time delay in the input path before time stamping. Therefore, any comparison of time stamps between port types will not be accurate at the nanosecond level.

The following table summarizes the accuracy of time stamps:

**Table 5.6 - Time Stamp Accuracy**

Timing/sync source	Time stamp accuracy	Possible variation between ports	Possible variation between systems
Uncalibrated; internal clock only	Indeterminate	16nsec for 1G ports 13nsec for 10G ports	Indeterminate
NTP server	≤ 10msec	16nsec for 1G ports 13nsec for 10G ports	≤ 10msec
GPS (1PPS with TSIP)	≤ 200nsec	16nsec for 1G ports 13nsec for 10G ports	≤ 200nsec
PTP master	≤ 1μsec	16nsec for 1G ports 13nsec for 10G ports	≤ 1μsec
1PPS only	Depends on 1PPS timing source	16nsec for 1G ports 13nsec for 10G ports	Depends on 1PPS timing source

## Using Port Stamping and Time Stamping Together

Port stamping and time stamping can be enabled independently or together. If port stamping and time stamping are used on the same port at the same time, then the time stamp bytes precede the dual- or single-byte port stamp, followed by the packet's four-byte CRC.

Port stamping and time stamping never alter network through traffic. Inline tapping ports always contain an exact replica of the original packet. Only the monitor ports on the system see packets with port and/or time stamps.

Although port stamping and time stamping are sold as a package, they are independently enabled on a per-port basis.



## Protocol De-encapsulation and Stripping

**Note: The protocol de-encapsulation and stripping options in this section are available only on PFS 6000 Series systems. These options are available on the PFS 5000/7000 Series systems with the use of PFX; refer to the PFX documentation for details. For additional information about stripping on PFS 5000/7000 Series systems, refer to [Standard Stripping](#).**

### ERSPAN, GRE, GTP, MPLS-L2, and NVGRE De-encapsulation

Many monitoring and analysis tools are unable to handle data flows that are encapsulated within the Generic Routing Encapsulation (GRE) and GPRS Tunneling Protocol (GTP) protocols, which are primarily used to transport user traffic in a network from an access network through to and across the core network. Similarly, most monitoring and analysis tools are unable to handle flows whose entire frames are encapsulated within MPLS (Multi-Protocol Label Switching), often referred to as pseudo-wire tunneling or MPLS-L2.

GTP de-encapsulation strips the GTP user plane header information from each packet, thereby restoring the GTP payload, and hence the packet, to what it was prior to GTP encapsulation. It is then forwarded out to the Monitor ports. Removing the GTP tunnel, outer IP, and outer UDP headers also allows the packet to be more simply filtered and load balanced based on the inner Layer 3 and Layer 4 headers and beyond.

Likewise, GRE de-encapsulation strips the GRE header information from each packet, and removes the outer IP header as well.

NVGRE (Network Virtualization GRE) is a little different, since it encapsulates the entire original frame, and so both the outer Ethernet header and GRE headers are removed in NVGRE de-encapsulation. As ERSPAN is an extension to NVGRE, the ERSPAN header is also removed in ERSPAN de-encapsulation.

In the case of MPLS-L2 de-encapsulation, the MPLS header is removed from each packet, and the outer Ethernet header is removed as well.

After the packet has been de-encapsulated, standard header filters and load-balancing can be applied to the packets.

### MPLS-L3, VLAN and VN Tag Stripping

Many monitoring and analysis tools cannot handle data flows that are tagged with MPLS labels or multiple VLAN tags, which are primarily used to transport traffic across networks to provide services such as virtual private networks (VPNs), or with VN-tags, which are used between Cisco Nexus distributed virtual switches. Removing these labeling or tagging protocols also allows the packets to be more easily filtered and load-balanced based on the Layer 3 and Layer 4 headers.

[MPLS label stripping](#) removes all MPLS labels, and allows you to specify:

- The value of the source MAC address, for the purpose of (for example) retaining reference to the original outer MPLS label value.
- The packet's Ethertype, since the MPLS labels themselves do not contain the encapsulated frame's Ethertype.



[VLAN tag stripping](#) allows user-selectable number (such as 1, 2, or all) of tags and types (such as IEEE 802.1q, IEEE 802.1ad, and non-standard) of tags to be removed.

VN-tag stripping simply removes the VN-tag.

## Protocol Stripping

Many monitoring and analysis tools cannot handle data flows that are encapsulated within numerous protocols, which are primarily used to transport traffic across various managed networks to provide service level assurance or transparency. Removing the encapsulation or tagging protocols also allows the packets to be more easily filtered and load-balanced based on the inner Layer 2, Layer 3, and Layer 4 headers.

The [protocol stripping](#) feature supports pre-defined protocols that make use of the protocol stripping capability. The pre-defined protocols are:

- Cisco FabricPath
- MAC-in-MAC
- TRILL (Transparent Interconnection of Lots of Links)
- VxLAN (Virtual Extensible LAN)

Only one of these stripping protocols will be processed on any given packet.

## Stripping and De-encapsulation Details

This section describes the format of packets before and after de-encapsulation or stripping is applied.

Note that an Ethernet header contains a MAC header and an EtherType (Etype), and a MAC header contains destination and source MAC addresses.

This section describes the format of packets before and after stripping is applied.

### TRILL

Before de-encapsulation, a TRILL packet contains:

Outer MAC	TRILL Etype	TRILL header	Inner Ethernet	Payload	Old FCS
-----------	-------------	--------------	----------------	---------	---------

De-encapsulated packet has outer Ethernet and TRILL headers removed and Ethernet FCS recalculated on the new packet:

Inner Ethernet header	Payload	New FCS
-----------------------	---------	---------

### Cisco FabricPath

Before de-encapsulation, a Cisco FabricPath encapsulated packet contains:

Outer Ethernet header	Inner Ethernet header	Payload	Old FCS
-----------------------	-----------------------	---------	---------

De-encapsulated packet has outer Ethernet header removed and FCS recalculated:



Inner Ethernet header	Payload	New FCS
-----------------------	---------	---------

## MAC-in-MAC

Before stripping MAC-in-MAC encapsulated packet contains:

Outer Ethernet header	Inner Ethernet header	Payload	Old FCS
-----------------------	-----------------------	---------	---------

De-encapsulated packet has outer Ethernet header removed and FCS recalculated:

Inner Ethernet header	Payload	New FCS
-----------------------	---------	---------

## VXLAN

Before stripping, VXLAN encapsulated packet contains:

Outer Ethernet header	Outer IP header	Outer UDP header	VXLAN header	Inner Ethernet header	Payload	Old FCS
-----------------------	-----------------	------------------	--------------	-----------------------	---------	---------

De-encapsulated packet has outer Ethernet, IP, UDP, and VXLAN headers removed, and FCS recalculated:

Inner Ethernet header	Payload	New FCS
-----------------------	---------	---------

## GTP

An incoming packet is changed from:

MAC header	Outer Etype	Outer IPv4/IPv6	Outer UDP	GTP header	Inner Etype	Inner IPv4/IPv6	Inner UDP/TCP	Payload	Old CRC
------------	-------------	-----------------	-----------	------------	-------------	-----------------	---------------	---------	---------

to:

MAC header	Inner Etype	Inner IPv4/IPv6	Inner UDP/TCP	Payload	New CRC
------------	-------------	-----------------	---------------	---------	---------

## GRE

GRE encapsulated packet at tunnel source:

MAC header	Outer Etype	Outer IPv4/IPv6	GRE header	Inner Etype	Inner IPv4/IPv6	Inner UDP/TCP	Payload	Old CRC
------------	-------------	-----------------	------------	-------------	-----------------	---------------	---------	---------

De-encapsulated packet at tunnel endpoint:

MAC header	Inner Etype	Inner IPv4/IPv6	Inner UDP/TCP	Payload	New CRC
------------	-------------	-----------------	---------------	---------	---------

## NVGRE

All outer headers are stripped, leaving only inner Ethernet data frames intact.

NVGRE encapsulated packet:



Outer MAC header	Outer Etype	Outer IPv4/IPv6	GRE header	Inner MAC header	Inner Etype	Inner IPv4/IPv6	Inner UDP/TCP	Payload	Old CRC
------------------	-------------	-----------------	------------	------------------	-------------	-----------------	---------------	---------	---------

De-encapsulated packet:

Inner MAC header	Inner Etype	Inner IPv4/IPv6	Inner UDP/TCP	Payload	New CRC
------------------	-------------	-----------------	---------------	---------	---------

## ERSPAN

All outer headers are stripped, leaving only inner Ethernet data frames intact.

ERSPAN encapsulated packet:

Outer MAC header	Outer Etype	Outer IPv4/IPv6	GRE header	ERSPAN header	Inner MAC header	Inner Etype	Inner IPv4/IPv6	Inner UDP/TCP	Payload	Old CRC
------------------	-------------	-----------------	------------	---------------	------------------	-------------	-----------------	---------------	---------	---------

De-encapsulated packet:

Inner MAC header	Inner Etype	Inner IPv4/IPv6	Inner UDP/TCP	Payload	New CRC
------------------	-------------	-----------------	---------------	---------	---------

## VN-tag

Before stripping, packet contains:

MAC header	VN-tag Etype	VN-tag header	Inner Etype	Payload	Old CRC
------------	--------------	---------------	-------------	---------	---------

TPID and tag are removed, and CRC is recalculated:

MAC header	Inner Etype	Payload	New CRC
------------	-------------	---------	---------

## MPLS-L2 (Pseudo-wire)

All outer headers are stripped, leaving only inner Ethernet data frames intact.

MPLS-L2 encapsulated packet:

Outer Ethernet header	MPLS label	Control word (optional)	Inner Ethernet header	Inner IPv4/IPv6	Inner TCP/UDP	Payload	Old CRC
-----------------------	------------	-------------------------	-----------------------	-----------------	---------------	---------	---------

De-encapsulated packet:

Inner Ethernet header	Inner IPv4/IPv6	Inner TCP/UDP	Payload	New CRC
-----------------------	-----------------	---------------	---------	---------

## MPLS-L3

An incoming packet is changed from:

Ethernet header	VLAN (optionally present)	MPLS Etype	MPLS tag (one or more)	Payload	Old CRC
-----------------	---------------------------	------------	------------------------	---------	---------



to:

Ethernet header	VLAN (optionally removed)	New Etype	Payload	New CRC
-----------------	---------------------------	-----------	---------	---------

## VLAN

An incoming packet is changed from:

MAC header	TPID	Tag	Etype	Payload	Old CRC
------------	------	-----	-------	---------	---------

to:

MAC header	Etype	Payload	New CRC
------------	-------	---------	---------

For multi-tagged packets, an incoming packet is changed from:

MAC header	TPID <sub>0</sub>	VLAN Tag <sub>0</sub>	TPID <sub>i</sub>	VLAN Tag <sub>i</sub>	Etype	Payload	Old CRC
------------	-------------------	-----------------------	-------------------	-----------------------	-------	---------	---------

to, with TPIDs and tag(s) removed and CRC recalculated:

MAC header	Etype	Payload	New CRC
------------	-------	---------	---------

## Protocol Stripping Configuration

The Protocol Stripping tab on the Libraries>Applications page allows you to perform the following tasks:

- [Configure Protocols Used in Protocol Stripping](#)
- [Configure Protocol Stripping](#)
- [Configure MPLS-L3 Stripping](#)



**Applications**

Deduplication VLAN Tag Stripping Tunnel Termination Healthcheck Slicing Protocol Stripping Extended LB

Protocol stripping configurations

Name	Protocols	Port List
PSConfig	GRE, protocol1(Cisco-Fabricpath)	

Showing 1 to 1 of 1

Protocols used in protocol stripping

Name	Protocol Matching Field	Protocol Etype Value	IP Protocol Value	Dest Port Value	Strip Headers	Strip Reference Point	Strip Offset	Strip Length	Lib List
Cisco-Fabricpath	etype	8903			L2_header	end-L2	0	2	PSConfig
Mac-in-Mac	etype	88e7			L2_header	end-L2	0	3	
TRILL	etype	22f3			L2_header	end-L2	0	6	
VXLAN	udp-dest-port			4789	L2_L3_L4_header	end-L4	0	8	

Showing 1 to 4 of 4

MPLS-L3 configurations

Name	Labels	Lib List
MPLS-L3_Config1		

Showing 1 to 1 of 1

## Configure Protocols Used in Protocol Stripping

- From the Applications page, click **Protocol Stripping**. The middle of the page lists currently defined protocols (both user-defined and pre-defined) used in protocol stripping. Up to 20 protocols can be defined.
- To add a new protocol, click **Add**.
- In the Name field, enter a descriptive name, and click **Add**.
- In the Protocol Matching Field drop-down list, select **Etype** (the default), **IP Protocol**, **UDP Dest Port**, **TCP Dest Port**, or **SCTP Dest Port**.
- For the protocol matching field that you select, the appropriate value field displays. Enter, as appropriate, either the Protocol Etype Value, IP Protocol Value, or Dest Port Value.
- In the Strip Headers drop-down list, select **L2 Header** (the default), **L2 L3 Header**, or **L2 L3 L4 Header**.
- In the Strip Reference Point drop-down list, select **Start L2** (the default), **End L2**, **End L3**, or **End L4**.
- In the Strip Offset field, enter the number of bytes to offset from the strip reference point.
- In the Strip Length field, enter the number of bytes to strip from the strip offset point.



10. Click **Apply** in the toolbar to save the settings to the running configuration.

The form shows configuration for protocol stripping. It includes fields for Protocol Matching Field (Etype), Protocol Etype Value (string), Strip Headers (L2 Header), Strip Reference Point (Start L2), Strip Offset (0), Strip Length (0), and a Lib List section for Protocol Stripping Name.

Protocol Matching Field	Etype	Protocol Etype Value	string
Default: etype		enter hexadecimal value for Etype(16 bit value...)	
Select the protocol matching field which needs...			
Strip Headers	L2 Header		
Default: L2_header			
Strip Headers			
Strip Reference Point	Start L2	Strip Offset	0
Default: start-L2		Default: 0	
Strip Reference Point		Number of bytes to offset from the strip-refer...	
Strip Length	0		
Default: 0			
Number of bytes to be stripped of from strip o...			
<b>Lib List</b> Protocol Stripping configuration list referencing the protocol			
Protocol Stripping Name			
Table is empty			

## Configure Protocol Stripping

1. From the Applications page, click **Protocol Stripping**. The top of the page lists currently defined protocol stripping configurations.
2. To add a new protocol stripping configuration, click **Add**.
3. In the Name field, enter a descriptive name, and click **Add**.
4. In the De-Encapsulation section, select one or more protocols to choose for de-encapsulation: **GRE**, **GTP**, or **MPLS-L2**.
5. In the Generic Stripping section, select up to eight protocols from the protocol library.
6. In the MPLS-L3 field, optionally select a protocol from the MPLS-L3 configurations.



De-Encapsulation:

GRE       GTP       MPLS L2

Specify which protocols to choose for generic ...

Generic Stripping:

Protocol 1	<input type="text"/> Mac-in-Mac	...	x
Protocol 2	<input type="text"/> myprotocol	...	x
Protocol 3	<input type="text"/>	...	
Protocol 4	<input type="text"/>	...	
Protocol 5	<input type="text"/>	...	
Protocol 6	<input type="text"/>	...	
Protocol 7	<input type="text"/>	...	
Protocol 8	<input type="text"/>	...	

MPLS-L3:

MPLS-L3	<input type="text"/> myprotocol-l3	...	x
---------	------------------------------------	-----	---

^ **Port List** Port list for protocol stripping configurations

Port Name			
Table is empty			

7. Go to the Advanced tab of the Port Settings page for the desired port. See [Configuring Ports](#) for information on accessing the port settings pages.
8. In the Protocol Stripping section, select the checkbox.
9. In the Protocol Strip Name Library Settings drop-down list, select the name of the protocol stripping configuration that you want to use.
10. Click **Apply** in the toolbar to save the settings to the running configuration.



<a href="#">Basic</a>	<a href="#">Advanced</a>
<p>Port and Time Stamping</p> <p>Monitor Output Timestamping <input type="checkbox"/> Default: disable Monitor Output Time-Stamping</p> <p>Monitor Output Portstamping <input type="checkbox"/> Default: disable Monitor Output Port-stamping</p> <p>Protocol Stripping</p> <p>VN Tag Stripping <input type="checkbox"/> Default:Disable Select to enable VN tag stripping</p> <p>VLAN Tag Stripping <input type="checkbox"/> Default:Disable Select to enable VLAN Tag Stripping</p> <p>Protocol Stripping <input checked="" type="checkbox"/> Default: disable Protocol stripping</p> <p>Protocol Strip Name: <input type="text" value="my-stripping"/> Library Settings: <input type="button" value="Default: Settings from Protocol Stripping Library"/></p>	

## Configure MPLS-L3 Stripping

1. From the Applications page, click **Protocol Stripping**. The bottom of the pages lists the currently defined MPLS-L3 configurations. Up to eight protocols can be defined.
2. To add a new protocol, click **Add**.
3. In the Name field, enter a descriptive name, and click **Add**.
4. In the Label column, enter from one to eight MPLS labels to search for.
5. In the E-Type column, either enter an Etype directly in the Etype column, or use the shortcuts dropdown list to automatically select the Etype that corresponds to one of the listed items (IPv4, IPv6, ARP, RARP, 802.1p/q tagged, PPPoE discovery, PPPoE session, XNS, or custom).
6. To edit the MAC source address, select the checkbox in the MAC Source field and enter the new address in the field.



MPLS-L3 Configurations			
Label	E-Type	MAC Source (click checkbox to edit)	
10ab1	ARP	0806	<input checked="" type="checkbox"/> 00:00:00:01:0a:b1
10ab2	802.1p/q tagged	8100	<input type="checkbox"/>
10ab3	PPPoE session	8864	<input checked="" type="checkbox"/> 00:00:00:01:0a:b3
	shortcuts	0000	<input type="checkbox"/>
	shortcuts	0000	<input type="checkbox"/>
	shortcuts	0000	<input type="checkbox"/>
	shortcuts	0000	<input type="checkbox"/>
	shortcuts	0000	<input type="checkbox"/>
	shortcuts	0000	<input type="checkbox"/>
	shortcuts	0000	<input type="checkbox"/>

- Click **Apply** in the toolbar to save the settings to the running configuration.

#### Notes:

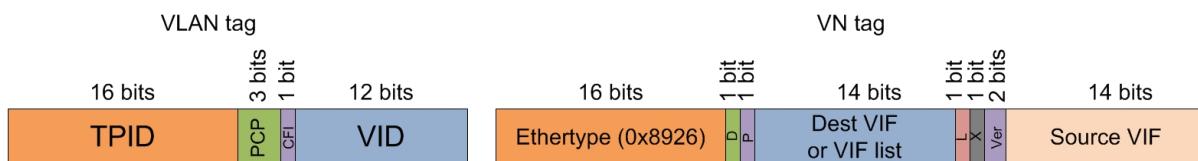
- To strip MPLS header for traffic including **both** MPLS+IPv4 and MPLS+IPv6 packets, configure E-Type as **IPv4**.
- If traffic includes both MPLS+IPv4 and MPLS+IPv6 packets but you only want to strip MPLS-IPv4 headers or you only want to strip MPLS-IPv6 headers (not both), use a filter to separate packets first, then strip the MPLS header.

### VLAN and VN Tag Stripping

Many monitoring and analysis tools cannot support more than a small number of VLAN tags, if any at all, and some network switches are also unable to handle more than a couple of hundred unique VLAN tags. Most monitoring tools and network switches do not recognize VN tags. VN is a Cisco protocol for virtual hosting environments.

VLAN and VN tag stripping remove such tagging information from packets that are forwarded out of the system's monitor ports. This can be one, two, or all VLAN or VN tags that might be nested in a packet, including Q-in-Q or bridging VLAN tags. While there can be up to three VLAN tags on a packet, there is usually only one VN tag.

Removing the VLAN tags, when more than one is present, also allows the packet to be load balanced based on the inner Layer 3 and Layer 4 headers.





VLAN and VN tag stripping is available on the 40SadvR line card for up to six ports in each group of 14, allowing up to 16 ports of stripping per line card.

A VLAN tag has the following general format, from most significant to least significant bits:

- 16 bits: Tag Protocol Identifier (TPID), which is the same as the Ethertype, with standard values of 0x8100 and 0x88A8. However, several non-standard vendor-specific values exist, such as: 0x9100, 0x9200, and 0x9300.
- 3 bits: Priority Code Point (PCP) = 0.
- 1 bit: Canonical Format Indicator (CFI) = 0.
- 12 bits: VLAN identifier (VID), which specifies the VLAN to which the packet belongs.

A VN tag has the following general format, from most significant to least significant bits:

- 16 bits: Ethertype = 0x8926.
- 1 bit: Direction indicator.
- 1 bit: Pointer bit.
- 14 bits: Destination VIF, identifies the destination port.
- 1 bit: Looped bit.
- 1 bit: Reserved.
- 2 bits: Version.
- 14 bits: Source VIF, identifies the source port.

## Configure VLAN and VN Tag Stripping

1. On the Applications page, select the **VLAN Tag Stripping** tab.
2. Click **Add**.
3. In the Name field, enter a name to identify the new entry.
4. Click **Add** to save the new entry and open the configuration page.
5. In the Number of Tags drop-down list, select **None, 1, 2 or All**.
6. In the TPIDs field, click **Add an entry**. Enter the TPID that you want to strip, and click **Add**.
7. Click **Apply** in the toolbar to save the settings to the running configuration.
8. Go to the Advanced tab of the Port Settings page for the desired port. See [Configuring Ports](#) for information on accessing the port settings pages.
9. Select the check box to enable the VLAN Tag Stripping feature, and click **Add** to create a new entry. Specify a name to identify the new entry and click **Add** to create the entry and



display the settings.

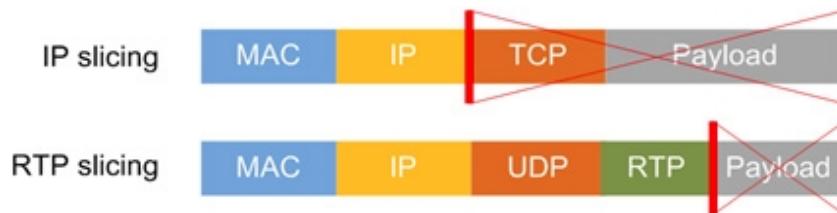
The screenshot shows the 'q-in-q' configuration page. At the top, there are fields for 'Number of Tags' (set to 2) and 'TPIDs' (set to 8100 and 88a0). Below this is a 'Port List' section with a single entry for 'Port Name' (10-9). A note at the bottom right indicates 'Showing 1 to 1 of 1'.

## Conditional Packet Slicing

**Note:** The slicing options in this section are available only on PFS 6000 Series systems. Conditional slicing is available on the PFS 5000/7000 Series systems with the use of PFX; refer to the PFX documentation for details. For information about slicing on PFS 7000 Series systems, refer to [Port Mirroring and Packet Slicing](#).

Many monitoring and analysis tools, such as for VoIP or video, need to see and analyze every packet in a flow for the protocols of interest but do not necessarily require seeing the entire contents of each packet. They might only require visibility into, for example, IP, UDP, and RTP header information. Other tools, such as those for security monitoring, might not be legally allowed to see or have access to the payload part of a flow, such as HTTP or email content.

PFOS supports conditional slicing of packets, from a user-defined point, such that any data following the defined point is removed from the packets that are forwarded out the system's Monitor ports. The method deployed for the conditional slicing uses PFOS "Type 2" filtering.



The point at which the slicing occurs is determined by an expression, similar to those used in creating filter expressions. The cyclic redundancy check (CRC) is recalculated for each packet.

Definition and capabilities of slice filtering are similar to normal filtering, except for the following specific differences, as well as the limitations specified in the Capabilities tab in the Web UI:

- Conditional slicing does not support a custom offset mask.
- Conditional slicing supports a maximum of eight filters per port.

Conditional slicing is available only on those ports for which a Slice application has been installed. In the Web UI, links to the slicing library and slicing settings page are shown only when this application is installed.

Conditional slicing is available on the 40SadvR line card for all ports in each group of 14, allowing up to 40 ports of stripping per line card.



## About Conditional Slicing and Packet Sizes

Conditional slicing has the following limitations on the size of packets that are received and sliced:

- The maximum offset that can be specified from one of the three starting points in a packet is 4,095 bytes.
- The minimum size of a packet that can be sliced depends on what the resulting sliced packet size will be, which must be 64 bytes or greater. If PFOS receives a packet less than 64 bytes, then conditional slicing forwards that packet without any padding. If slicing reduces a packet size to less than 64 bytes, then PFOS pads the packet to 64 bytes before forwarding it.
- After slicing a packet, the result must be at least 16 bytes long. If the resulting slice is less than 16 bytes long, then the slicing is not performed and the packet is forwarded unchanged.

## Configure Conditional Slicing

1. From the Applications page, click **Slicing**, scroll down to the Advanced Filter section, and create and save filters as desired. See [Traffic Filtering](#) for information on defining filters. For a complete list of packet field names that can be used in a filter expression, refer to [PFOS Packet Fields in Filter Expressions](#).

The screenshot shows the PFOS Applications page with the 'Slicing' tab selected. Below the tabs, there's a 'Slicing' section with an 'Advanced Filter' button. This 'Advanced Filter' button is circled in red. Below it is a table with two rows: one for 'http' (IP Protocol 6 and ( TCP Dest Port 80-81 or TCP Source Port 80-81 )) and another for 'nonmatch'. At the bottom of the 'Advanced Filter' section, it says 'Showing 1 to 2 of 2'. There are also sections for 'Offset' and 'Port List'.

2. Return to the Applications page, click **Slicing** again if necessary, scroll down to the Offset section, and then click **Add**.



- In the Name field, enter a name to identify the new entry.
- Click **Add** to create the entry and display the settings.

Slice Point: Start of Packet  
Default: start-of-packet  
At which point the slice start

Offset Value (bytes): 60  
Default: 60  
Valid values: 0—4095  
Offset after the slice point as the reference ...

Lib List Slicing configuration list referencing offset

Slicing Name:

- Select the slice point and the offset value in bytes. The minimum offset is 16 bytes if the slice point is Start of Packet, and 0 bytes in all other cases.
  - Click **Apply**.
3. Return to the Applications page, click **Slicing** again if necessary, scroll down to the Slicing section, and then click **Add**.
- In the Slicing Type section, select **Slice**.
  - In the Configuration sections, specify up to eight slicing settings of filter and offset. A single port can have up to eight different slicing settings, and the priority determines the order in which they are used.

Slicing Type:  Slice  Mask  
Slicing type

Configuration 1 1st priority configuration

Advanced Filter: http  
Advanced filter: 0

Offset: default-offset  
Slice point offset: 0

Configuration 2 2nd priority configuration

Advanced Filter:   
Offset:

- Click **Apply**.



4. Return to the Applications page, click **Slicing** again if necessary, and verify that you have created all of the entries to perform your desired slicing.

The screenshot shows the Slicing configuration page with three main sections:

- Slicing:** A table with columns **Name** and **Slicing Type**. It contains one entry: **slice-1** (slice).
- Advanced Filter:** A table with columns **Name** and **Expression**. It contains two entries: **http** (IP Protocol 6 and ( TCP Dest Port 80-81 or TCP Source Port 80-81 )) and **nonmatch**.
- Offset:** A table with columns **Name**, **Slice Point**, and **Offset Value**. It contains one entry: **default-offset** (start-of-packet, 60).

5. Go to the Advanced tab of the Port Settings page for the desired port. See [Configuring Ports](#) for information on accessing the port settings pages.
6. In the Conditional Slicing section, select **Slicing**, and select a slicing library from the drop-down list that displays.

The screenshot shows the Port 7-6 Settings page with the **Advanced** tab selected. The **Protocol Slicing** section contains the following configuration:

- Slicing:** A checkbox labeled **Slicing** is checked (indicated by a red oval).
- Default:** **Disable**
- Conditional Slicing/Masking:** (disabled)
- Slicing Library:** A dropdown menu set to **slice-1** (indicated by a red oval). Below the dropdown, the text "Provide Slicing Library name" is visible.



7. Click **Apply**.

## Conditional Packet Masking

**Note: The masking options in this section are available only on PFS 6000 Series systems. Conditional masking is available on the PFS 5000/7000 Series systems with the use of PFX; refer to the PFX documentation for details. For additional masking options for the PFS 5000/7000 Series systems, refer to [Traffic Filtering](#).**

Companies often need to see and analyze every packet for monitoring purposes, or even store various data types for troubleshooting or data retention compliance reasons. However, these packets typically contain sensitive or personal information which, if not removed or hidden, can result in noncompliance with regulations such as HIPAA, PCI-DSS, and GDPR.

Although slicing the packet, such as with [Conditional Packet Slicing](#), might be one way to address this, monitoring or security applications often want to have the original packet frame retained. Therefore, the ability to write over or mask out the data in the packet becomes necessary.

Conditional masking enables conditional masking of packets, from a user-defined point, such that a specified length of data following the defined point is written over within the packets that are forwarded out the Monitor ports. The method deployed for the conditional masking uses PFOS "Type 2" filtering.

With conditional masking, you can specify the packets to be masked, a mask pattern, the length of the mask, an offset for the mask, and an anchor point.

Conditional masking is available only on those ports for which a Slice application has been installed. In the Web UI, links to the slicing library and slicing settings page are shown only when this application is installed.

Conditional masking is available on the 40SadvR line card for all ports in each group of 14, allowing up to 40 ports of stripping per line card.

A conditional masking definition consists of:

- Port ID on which masking will be performed.
- Mask pattern.
- Mask length.
- Anchor point (start of packet, end of Layer 2, end of Layer 3, or end of Layer 4).
- Mask offset.
- Name of a previously created slicing (Type 2) filter.

For example, consider a conditional masking definition with an anchor point at the start of the packet, an offset of 100 bytes, a mask length of 100 bytes, and a mask pattern of 0xEE. After processing, a packet would look like this:



```
[+] Frame 1: 9000 bytes on wire (72000 bits), 9000 bytes captured (72000 bits)
[+] Ethernet II, Src: Performa_00:00:02 (00:10:94:00:00:02), Dst: Xerox_00:00:01 (00:00:01:00:00:01)
[+] Internet Protocol Version 4, Src: 192.85.1.2 (192.85.1.2), Dst: 192.0.0.1 (192.0.0.1)
[+] Transmission Control Protocol, Src Port: http (80), Dst Port: 1024 (1024), Seq: 1, Ack: 1, Len: 8942

0000  00 00 01 00 00 01 00 10  94 00 00 02 08 00 45 00  ....E.
0010  23 16 d0 80 00 00 ff 06  47 08 c0 55 01 02 c0 00  #....G.U...
0020  00 01 00 50 04 00 00 01  e2 40 00 03 94 47 50 10  ..P...@..GP.
0030  10 00 04 77 00 00 00 00  00 00 00 00 00 00 00 00 00  ...w....
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00  .....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00  .....
0060  00 00 00 00 ee ee ee ee  ee ee ee ee ee ee ee ee  .....
0070  ee ee ee ee ee ee ee ee  ee ee ee ee ee ee ee ee  .....
0080  ee ee ee ee ee ee ee ee  ee ee ee ee ee ee ee ee  .....
0090  ee ee ee ee ee ee ee ee  ee ee ee ee ee ee ee ee  .....
00a0  ee ee ee ee ee ee ee ee  ee ee ee ee ee ee ee ee  .....
00b0  ee ee ee ee ee ee ee ee  ee ee ee ee ee ee ee ee  .....
00c0  ee ee ee ee ee ee ee ee  00 00 00 00 00 00 00 00 00  .....
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00  .....
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00  .....
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 00  .....
```

Up to eight mask definitions can be present for any one slicing.

Conditional masking is supported on all port classes except pStack.

## Configure Conditional Masking

- From the Applications page, click **Slicing**, scroll down to the Advanced Filter section, and create and save filters as desired. See [Traffic Filtering](#) for information on defining filters. For a complete list of packet field names that can be used in a filter expression, refer to [PFOS Packet Fields in Filter Expressions](#).

Name	Slicing Type	Port List
http	IP Protocol 6 and ( TCP Dest Port 80-81 or TCP Source Port 80-81 )	Lib List
nonmatch		Showing 1 to 2 of 2

- Return to the Applications page, click **Slicing** again if necessary, scroll down to the Mask Definition section, and then click **Add**.
  - In the Name field, enter a name to identify the new entry.
  - Click **Add** to create the entry and display the settings.



### mask-1 ×

Anchor Point	Start L2	Offset (bytes)	60
Default: start-L2 At which point the maskdef start		Default: 60 Valid values: 0—4095 Offset after the anchor point as the reference...	
Length (bytes)	60	Pattern	00
Default: 60 Valid values: 0—4095 Length for first offset to maskdef		Default: 00 Maskdef pattern for offset	

- Select the anchor point, offset value in bytes, length in bytes, and mask pattern.
  - Click **Apply**.
3. Return to the Applications page, click **Slicing** again if necessary, scroll down to the Slicing section, and then click **Add**.
- In the Slicing Type section, select **Mask**.
  - In the Configuration sections, specify up to eight masking settings of filter and mask definition. A single port can have up to eight different settings, and the priority determines the order in which they are used.

### mask-library ×

Slicing Type	<input type="radio"/> Slice	<input checked="" type="radio"/> Mask	
Slicing type			
▲ Configuration 1 1st priority configuration			
Advanced Filter	http	Maskdef	mask-1
Advanced filter		Maskdef	
()		()	

- Click **Apply**.
4. Return to the Applications page, click **Slicing** again if necessary, and verify that you have created all of the entries to perform your desired slicing.



Slicing

Add ... Delete

Name	Slicing Type
mask_library	mask

Advanced Filter

Add ... Delete

Name	Expression
http	IP Protocol 6 and ( TCP Dest Port 80-81 or TCP Source Port 80-81)
nonmatch	

Offset

Add ... Delete

Name	Slice Point	Offset Value
default-offset	start-of-packet	60

Mask definition

Add ... Delete

Name	Anchor Point	Offset	Length	Pattern
mask-1	start-L2	60	60	00

5. Go to the Advanced tab of the Port Settings page for the desired port. See [Configuring Ports](#) for information on accessing the port settings pages.
6. In the Conditional Slicing section, select **Slicing**, and select a slicing library from the drop-down list that displays.



## Port 7-5 Settings

Reset Port ▾

Basic Advanced References

### Port and Time Stamping

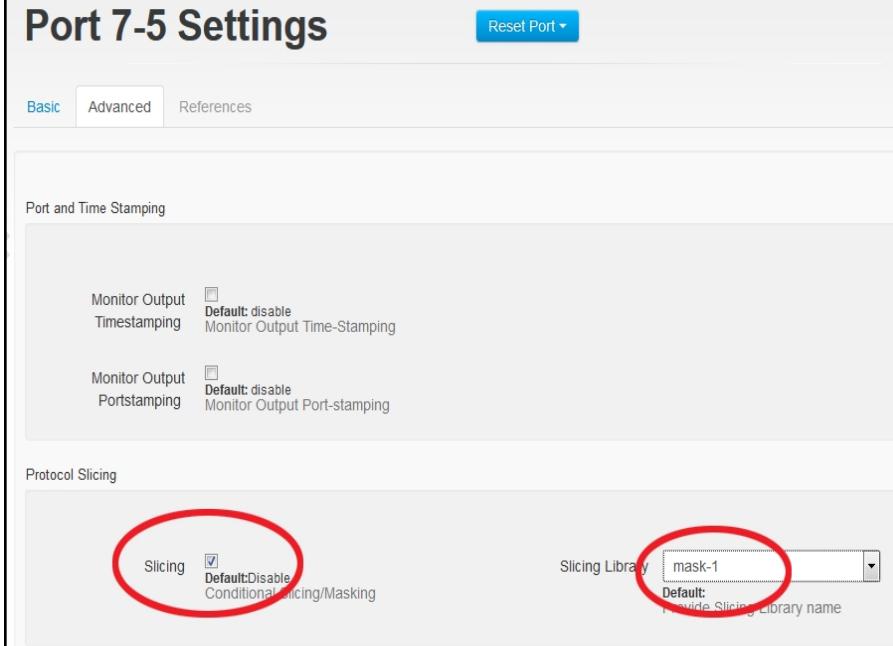
Monitor Output Timestamping  Default: disable Monitor Output Time-Stamping

Monitor Output Portstamping  Default: disable Monitor Output Port-stamping

### Protocol Slicing

Slicing  Default:Disable Conditional Slicing/Masking

Slicing Library  Default: Provide Slicing Library name



7. Click **Apply**.



## Extended Load Balancing

**Note: Extended load balancing is only available on the PFS 6000 Series with the 40SadvR line card. For information about load balancing for PFS 5000/7000 Series systems, refer to [Traffic Load Balancing](#).**

As an extension to standard load balancing, several additional criteria are available to allow load balancing to work in encapsulated traffic scenarios. This removes the need to de-encapsulate the packets before load balancing.

Extended load balancing is pre-configured with support for these protocols:

- Cisco-Fabricpath
- GRE, L2GRE/NVGRE, ERSPAN
- GTP
- MPLS
- MVDCAP
- Mac-in-Mac
- TRILL
- VLAN, VNTAG
- VXLAN

An extended load balancing configuration can use up to six of these protocols with any one of these combinations of load balancing criteria:

- IP Dest Src TCP UDP SCTP Dest Src Protocol Type
- IP Dest Src TCP UDP SCTP Dest Src
- IP Dest Src
- IP Dest
- IP Src
- IP Dest TCP UDP SCTP Dest
- IP Src TCP UDP SCTP Src
- Dest Inner MAC Address
- Src Inner MAC Address
- Dest Src Inner MAC Address

## Extended Load Balancing Workflow

Follow these steps to set up extended load balancing:

1. If needed, [define any protocol\(s\) that are not already defined](#).
2. [Select an extended load balancing configuration to use, or create a new one](#).
3. [Enable extended load balancing on the desired ports](#).
4. [Create a traffic map that uses the desired extended load balancing configuration](#).



## Define New Protocol to use in Extended Load Balancing

1. On the Applications page, select the **Extended LB** tab.
2. Scroll down to the "Protocols used in extended load balancing" section, and click **Add**.
3. In the Name field, enter a descriptive name for this protocol, and click **Add**.
4. In the **Protocol Matching Field** drop-down list, select one of the following: Etype, IP Protocol, UDP Dest Port, TCP Dest Port, Sctp Dest Port, NA. An additional field specific to the selected field displays; enter the appropriate value.
5. In the following fields, select desired values:
  - **Headers:** L2 Header, L2 L3 Header, L2 L3 L4 Header, L3 L4 Header, None, NA.
  - **Reference Point:** Start L2, End L2, End L3, End L4, NA.
  - **Offset:** Number of bytes to offset from the reference point.
  - **Length:** Number of bytes to use from the offset; must be less than 256.
6. Apply your changes.

### protocol1 ×

New Lb Protocol...

Protocol Matching Field	TCP Dest Port
Default: etype Select the protocol matching field	
Dest Port Value	8080
Valid values: 0—65535 Destination port number(16 bit positive integer)	
Headers	L2 Header
Default: L2_header Headers	
Reference Point	Start L2
Default: start-L2 Reference point	
Offset	32
Default: 0 Number of bytes to offset from the reference point	
Length	8
Default: 0 Number of bytes from offset(<256)	
Lib List Load Balancing configuration list referencing the protocol	

## Define New Extended Load Balancing Configuration

1. On the Applications page, select the **Extended LB** tab.
2. Scroll down to the "Extended Load balancing configurations" section, and click **Add**.
3. In the Name field, enter a descriptive name for this configuration, and click **Add**.
4. In the six **Protocol** drop-down lists, select up to six protocols (pre-configured or user-defined) to use in this extended load balancing configuration.



5. In the **Criteria** drop-down list, select the criteria to be used.
6. Apply your changes.

**elb-config1** × New Extended Lb...

Protocol 1	<input type="button" value=""/> GTP	...	x
Select the protocol for extended load balancin...			
Protocol 2	<input type="button" value=""/> GTP	...	x
Select the protocol for extended load balancin...			
Protocol 3	<input type="button" value=""/> protocol1	...	x
Select the protocol for extended load balancin...			
Protocol 4	<input type="button" value=""/>	...	
Select the protocol for extended load balancin...			
Protocol 5	<input type="button" value=""/>	...	
Select the protocol for extended load balancin...			
Protocol 6	<input type="button" value=""/>	...	
Select the protocol for extended load balancin...			
Criteria	<input type="button" value=""/> IP Dest TCP UDP SCTP Dest		
Default: IP_Dest_Src_TCP_UDP_SCTP_Dest...			
Select the criteria for selected protocols (IP Dest Src TCP UDP SCTP Dest Src Protocol Type)			

### Enable Extended Load Balancing on a Port

1. Go to the Port Settings page for the port on which you wish to perform extended load balancing.
2. Click the **Advanced** tab.
3. Scroll down to the Protocol Extended Load Balance section. If you do not see this section of the page, then this port cannot perform extended load balancing.
4. Select the **Extended Load Balancing** checkbox to enable this capability on this port.
5. In the Extended LB Name Library Settings drop-down list, select the pre-defined or user-created library to use with extended load balancing on this port.

Protocol Extended Load Balance

Extended Load Balancing	<input checked="" type="checkbox"/> Default: disable	Extended Load Balancing feature
		Extended LB Name Library Settings
		<input type="button" value=""/> VXLAN+IPD&L4D
Default: Provide Extended Load Balancing Library name		



6. Repeat these steps for every additional port on which you want to perform this type of extended load balancing.
7. Apply your changes.

### Create Traffic Map Using Extended Load Balancing

1. Go to the Traffic Maps page, and click **Add**.
2. In the Name field, enter a descriptive name for this traffic map, and click **Add**.
3. In the Mode drop-down list, select **Extended**.
4. In the Load Balance Criteria drop-down list, select **ELB**.
5. Specify other values as desired for the traffic map. For more information, refer to [Traffic Maps](#).
6. Apply your changes.

New Traffic Map...

### elb-map1 ×

Description	<input type="text" value="string"/> 1 characters or more.	Type	Monitor
Mode	<input type="button" value="Extended"/> <span>(Basic)</span>	Default:	Monitor A map type.
Input Ports *	<input type="button" value="configure"/> Input port(s)	Selected Input Ports:	10-3, 10-4
Output Ports	<input type="button" value="configure"/> Output port(s)	Selected Output Ports:	
Remote Monitor Groups	<input type="button" value="configure"/> Remote Monitor Port Groups	Selected Remote Groups:	
Output Load Balance Groups	<input type="text" value="lbgroup1"/> <span>x</span> Output load-balance groups		
Load Balance Criteria	<input type="button" value="ELB"/> <span>0</span>		

### Extended Load Balancing Considerations

- Extended load balancing works only on ports used as ingress ports in a traffic map, which can be either Span, Span-Monitor, or Service port classes. It will not work if the feature is on the ports in the load-balance group.
- Extended load balancing cannot be used with remote monitor ports that are part of a pfsMesh.

## 6 Inline Traffic

The PFS Inline Security function enables pervasive security and service chaining across multiple tools with the flexibility of bypassing and skipping tools from any tool in the toolchain. This enables failsafe mechanism of tools along with aggregation, filtering, and balancing.

Inline traffic flow is bidirectional traffic composed of two major port classes on PFS – Inline Network and Inline Monitor ports. Additional monitor ports can be used for passive tools with inline configuration.

- **Inline Network:** A bidirectional class of port that exists in user-configured pairs of ports, and connects in-line with a network link. The primary purpose of each port in the pair is to forward network traffic to one or more inline active monitoring and/or analysis tools (such as an IPS) via Inline Monitor ports. The other port in each Inline Network port pair forwards traffic, which has been received from the inline tool via the Inline Monitor ports, back into the network. Optionally, network traffic can be forwarded directly between each Inline Network port within each pair (such as network pass-through), or can be completely dropped. User-defined VLAN IDs are supported on Inline Network ports with [limitations](#).
- **Inline Monitor:** A bidirectional class of port that exists in user-configured pairs of ports, and connects to an inline active monitoring and/or analysis tool, such as an IPS, for the purpose of forwarding traffic, from one or more Inline Network ports, or from other Inline Monitor ports in a tool chain, to the connected inline tool. The other port in each Inline Monitor port pair receives traffic from the inline tool and forwards it to the appropriate Inline Network port. VLAN tagging is not allowed on Inline Monitor ports.

Each monitoring port can be configured to collect data from any combination of network ports. Ports configured as Inline Network inputs are buffered as a pair, thus preserving packet ordering within each port pair and keeping network latency to a minimum.

Differing speeds are supported across input ports, across output ports, and between input and output ports. Inline Network or Inline Monitor port pairs can have the same speed or different speeds between each port with the pair. Each port can also be configured for auto-negotiation.

PFOS provides traffic redirection and load balancing for active inline tools, such as intrusion protection systems (IPSSs) and WAN optimizers. As a part of this, it allows you to select bypassing of the monitor tools as well as various failure behaviors and states, which is critical for maintaining high availability and security monitoring applications. As an example, if one or more inline appliances are down for maintenance, replacement, or failure, traffic can be bypassed to ensure uninterrupted traffic flow on the network.



The [PowerSafe](#) feature provides bypass switch support for failover protection for the PFS 7000 Series. The PowerSafe TAP allows guaranteed uninterrupted network connectivity on each of its segments in instances of power failures or system crashes. Its state can also be manually controlled from the PFOS user interface.

## Tool Chain - Simple Mode vs. Advanced Mode

As of v5.5.1, PFOS provides two types of tool chains. The Advanced Tool Chain is based on the original tool chain available in earlier releases; a new Simple Tool Chain provides a simpler configuration for inline tools in series process.

- **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. Additionally, the Simple Tool Chain supports [Source Port VLAN Forwarding](#) that allows packets to be forwarded based on the VLAN ID assigned at the ingress inline network ports. See
- **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.

You can modify a tool chain's type at any time. However, note that data will be lost when changing from Advanced to Simple:

- **Advanced-to-Simple:** When changing a tool chain's type from Advanced to Simple, all the existing next-tool connections are discarded and replaced with the default "nonmatch" connections. PFOS warns you of the lost data and allows you to cancel the operation.
- **Simple-to-Advanced:** When changing a tool chain's type from Simple to Advanced, all the default "nonmatch" connections remain between each tool. You can then modify the connections to add filtering as required.

## Inline Traffic Workflow

Managing inline traffic uses several PFOS components that all must be configured before the system can process traffic. In general, you can configure these components in any order, and you can switch from one incomplete task to another, but NETSCOUT recommends that you configure components in this order to minimize switching among incomplete tasks.

1. Decide which ports will carry inline traffic or will be used for passive monitoring. Configure the physical settings of the ports (see [Configuring Ports](#)).
2. Define Inline Network and Inline Monitor [port groups](#), which includes defining the port pairs that you will use. Define Monitor [port groups](#) for passive monitor.
3. Create a [simple tool chain](#) with traffic flow over inline tools in series.
4. Create [advanced tool chains](#) for more complicated service chains.
5. Configure the traffic maps that will process inline traffic. Refer to [Inline Traffic Maps](#).

Additional Features to Support Tool Chain Function:



6. Enable [LinkSafe](#) at Inline Network Port Groups (most common); or at Inline Monitor Port Groups if desired.
  7. Configure the health check function for Inline Monitor Port Groups to monitor tool status. Refer to [Health Check Profiles](#).
  8. Enable [PowerSafe](#) settings after connecting PFS to an external powersafe tap (EPT).

# Simple Tool Chaining

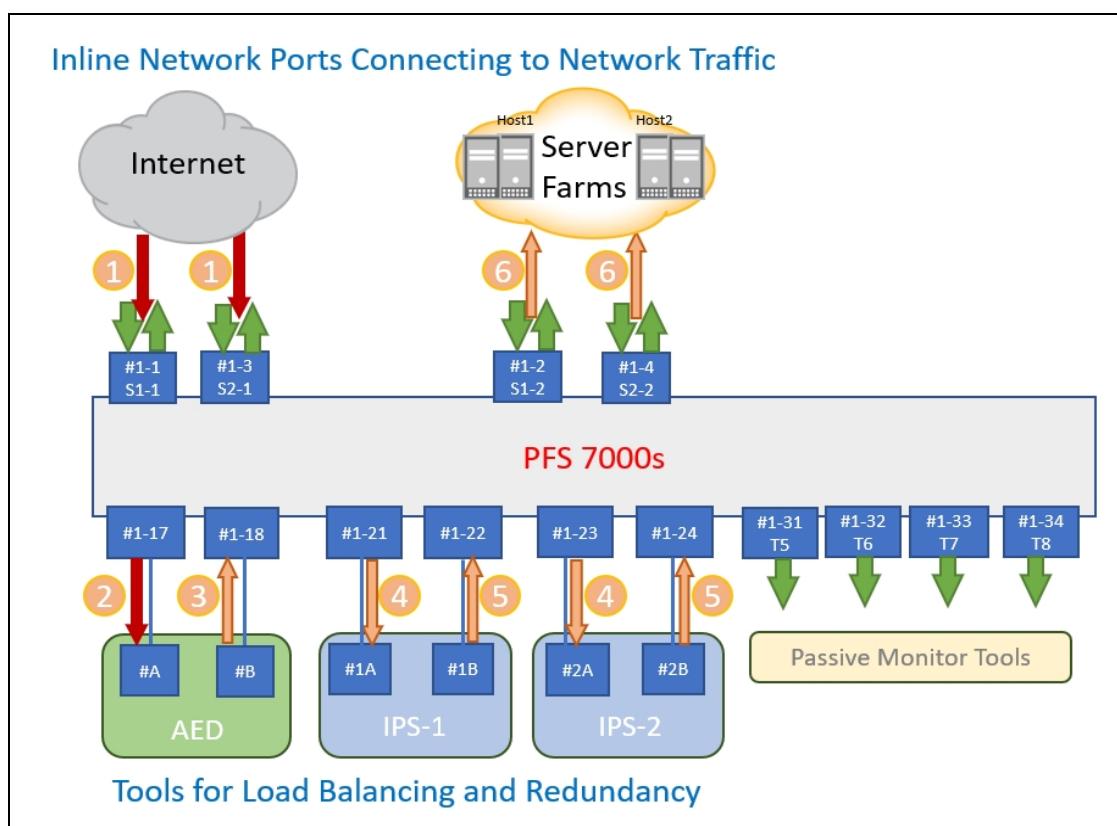
**Note:** This feature is only supported on PFS 6000 and PFS 7000 Series.

The Simple Tool Chain redirects live bidirectional network traffic to multiple active inline tools in series. It allows you to chain multiple security services for defense-in-layers architecture and to centralize application of network monitoring and security protection. Refer to [Simple Tool Chain Use Case](#) for details.

Additionally, the Simple Tool Chain supports [Source Port VLAN Forwarding](#) that allows packets to be forwarded based on the VLAN ID assigned at the ingress inline network ports.

## Simple Tool Chain Use Case

The following diagram shows two pairs of inline network ports from traffic to two inline tool groups-- AED and IPS that provide load balance and redundancy. Another four monitoring ports can be used for passive monitoring tools.



**Figure 6.1 - In-Series Tool Chain Use Case Diagram**



## Prerequisites

The following components must be configured prior to configuring tool chains. You will be selecting these components as you build the tool chain:

- [Port Settings](#)
- [Inline Network Port Groups](#)
- [Inline Monitor Port Groups](#)
- [Monitor Port Groups](#)
- [Forwarding Filters](#)

Also, refer to [Tool Chain Resource Limits and Considerations](#) for additional information.

## Port Settings

The following graphic shows example port settings for [Figure 6.1](#). See [Configuring Ports](#) for port configuration details.

Port ID	Name	Class	Link	Speed	XCVR Model	XCVR Type	PWR Rx (dBm)	PWR Tx (dBm)
1-1	S1-1_B5	Inline-Network	up	1000	FINISAR CORP. FCLF8522P2BTL	1000Base-T	-N/A-	-N/A-
1-2	S1-2_TZone	Inline-Network	up	1000	FINISAR CORP. FCLF8522P2BTL	1000Base-T	-N/A-	-N/A-
1-3	S2-1_B5	Inline-Network	up	1000	FINISAR CORP. FCLF8522P2BTL	1000Base-T	-N/A-	-N/A-
1-4	S2-2_TZone	Inline-Network	up	1000	FINISAR CORP. FCLF8522P2BTL	1000Base-T	-N/A-	-N/A-
1-17	AED_A	Inline-Monitor	up	10000	INNOLIGHT TR-PX85S-NRS	1G/10GBase-SR	-2.75	-2.98
1-18	AED_B	Inline-Monitor	up	10000	INNOLIGHT TR-PX85S-NRS	1G/10GBase-SR	-2.42	-3.85
1-21	IPS-1_1A	Inline-Monitor	up	10000	INNOLIGHT TR-PX85S-NRS	1G/10GBase-SR	-3.48	-3.02
1-22	IPS-1_1B	Inline-Monitor	up	10000	INNOLIGHT TR-PX85S-NRS	1G/10GBase-SR	-3.78	-2.82
1-23	IPS-2_2A	Inline-Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-2.47	-2.21
1-24	IPS-2_2B	Inline-Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-2.41	-2.37
1-31	T5_OOB	Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-2.58	-2.43
1-32	T6_OOB	Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-1.19	-1.94
1-33	T7_OOB	Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-2.31	-2.17
1-34	T8_OOB	Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-2.29	-2.25

## Inline Network Port Groups

The following graphic shows example inline network port configuration for the ports connecting to network traffic in [Figure 6.1](#). See [Configuring Ports](#) for port configuration details.



The screenshot shows the NETSCOUT UI for configuring a Port Group named "S1S2\_Servers". The left sidebar menu includes Event Notifications, pfsMesh, Configuration (Ports Settings, Port Groups, Powersafe, Tool Chain, Trigger Policies, Tunnel Settings, Load Balance Groups, Traffic Maps, Libraries, Forwarding Filters, Load Balance Criteria, Applications), Notifications, and Events. The "Port Groups" option is selected. The main panel displays the "S1S2\_Servers" group with the following settings:

Vlan Tag	Enable	Power Safe
Default: enable		<input type="checkbox"/> Enable if connected to External PowerSafe Tap

Below this is a "Port Pair" section titled "Inline Network Pair" with two entries:

A Port	B Port	Link Safe
1-1	1-2	Enabled
1-3	1-4	Enabled

At the bottom right of the table, it says "Showing 1 to 2 of 2".

## Inline Monitor Port Groups

The following graphic shows example inline monitor port configuration for the AED in [Figure 6.1](#). See [Port Groups](#) for configuration details.

The screenshot shows the NETSCOUT UI for configuring a Port Group named "AED". The left sidebar menu is identical to the previous screenshot. The main panel displays the "AED" group with the following settings:

A Port	B Port	Link Safe	A Health Check Status	B Health Check Status
1-17	1-18	disable	down	down

At the bottom right of the table, it says "Showing 1 to 1 of 1".



The following graphic shows example inline monitor port configuration for the IPS components in [Figure 6.1](#). See [Port Groups](#) for configuration details.

The screenshot shows the NETSCOUT interface for configuring an inline monitor port pair. The top navigation bar includes Home, Port Group, Inline Monitor, and Group = IPS#1#2. On the left, a sidebar lists Event Notifications, pfsMesh, Configuration (Ports Settings, Port Groups selected), Powersafe, Tool Chain, Trigger Policies, and Tunnel Settings. The main area displays a table titled "Port Pair Inline Monitor Pair" with two rows:

A Port	B Port	Link Safe	A Health Check Status	B Health Check Status
1-21	1-22	disable	down	down
1-23	1-24	disable	down	down

## Monitor Port Groups

The following graphic shows example monitor port configuration for the Passive Monitoring Tool components in [Figure 6.1](#). See [Port Groups](#) for configuration details.

The screenshot shows the Passive Monitoring Tool interface for configuring monitor port groups. The top navigation bar includes Network, Monitor (selected), Inline Network, and Inline Monitor. The main area displays a table with four rows:

Name	Lb Criteria	pfsMesh Visibility	Status
T5_OOB-1		disable	PortGroupNameResolved
T6_OOB-2		enable	PortGroupNameResolved
T7_OOB-3		enable	PortGroupNameResolved
T8_OOB-4		enable	PortGroupNameResolved



## Forwarding Filters

The following graphic shows example forward filtering configuration for the network traffic in [Figure 6.1](#). You will assign these filters when configuring the [Inline Traffic Map](#). See [Forwarding Filters](#) for filter configuration details.

A screenshot of a web-based configuration interface titled "Forwarding Filter". At the top right are buttons for "Add ...", "Delete", and other actions. Below is a table with columns: Name, Description, Used in Maps, and Expression. The table contains four rows:

Name	Description	Used in Maps	Expression
All_Traffic		0	( mac offset 0 0 mask 0 )
WebTraffic		0	( Dest Port 443 or Dest Port 80 or Dest Port 81 ) or ( Src Port 443 or Src Port 80 or Src Port 81 )
nonmatch		0	
unfiltered		0	

## Create a Simple Tool Chain

Perform the following steps to create a Simple tool chain.

1. In the Web UI, select Configuration>Tool Chain. Select Type as **Simple**. As a Simple tool chain, traffic will flow tools in series so we only need to configure inline monitor port groups to each tool in sequence.

A screenshot of the "AED-IPS\_ToolChain" configuration page. On the left is a sidebar with options like Event Notifications, pfmMesh, Configuration (Ports Settings, Port Groups, Powersafe), Tool Chain (selected), Trigger Policies, Tunnel Settings, and Load Balance Groups. The main area shows the tool chain type set to "Simple" and "Default: Advanced". It includes fields for "Tool Name", "Inline Monitor Group", and "A Side Passive Monitorgroups" (T5\_OOB-1, T6\_OOB-2) and "B Side Passive Monitorgroups" (T7\_OOB-3, T8\_OOB-4). An "Add" button is visible.

2. To add a tool to the chain, click **Add**. Fields appear for you to modify. Add both tools (AED and IPS) as one service chain.

A screenshot of the "AED-IPS\_ToolChain" configuration page after adding two tools. The "Tool Name" column lists "AED" and "IPS". The "Inline Monitor Group" column lists "AED" and "IPS#1#2". The "A Side Passive Monitorgroups" column lists "T5\_OOB-1" and "T7\_OOB-3". The "B Side Passive Monitorgroups" column lists "T6\_OOB-2" and "T8\_OOB-4". The "Tool Failover Action" column lists "SKIP" for both entries.

- In the **Tool Name** field, enter a descriptive name of up to 64 characters for this tool.



- In the **Inline Monitor Group** field, select the inline monitor port group that will forward traffic to this tool.
  - In the **A Side Passive Mongroups** field, optionally select a monitor port group to receive traffic from the A side of this tool that matches all specified next-tool filters on the A side.
  - In the **B Side Passive Mongroups** field, optionally select a monitor port group to receive traffic from the B side of this tool that matches all specified next-tool filters on the B side.
  - In the **Tool Failover Action** field, select the action to apply when the tool is unavailable:
    - **Skip:** Bypass the failed tool and continue based on its next tool table.
    - **Drop:** Block the traffic at the failed tool.
    - **Bypass:** Bypass the entire tool chain when the tool fails.
3. Continue adding tools in the order of the inline traffic flow (see [Figure 6.1](#)), in sequence, to each tool, then exit the tool chain.
  4. Add the tool chain to an [Inline Traffic Map](#). The associated Inline Traffic Map name will appear in the Ref Map section at the bottom of the Tool Chain page.

## Simple Tool Chain with Source Port VLAN Forwarding

When the Source Port VLAN Forwarding feature is enabled in Simple Tool Chain mode, 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.

Source Port VLAN Forwarding can be helpful in the following use cases:

- **Customer Packets Including Double VLAN Tags**  
PFOS adds a VLAN ID to packets entering a tool chain at inline network ports, resulting in packets being sent to tools having three VLAN tags. Hardware limitations prevent PFOS from processing filters on packets with three VLAN tags.
- **Cascading Multiple PFS Devices with Inline Function**  
PFS devices only have one USB port, providing connection to one EPT for eight pairing ports. Using Source Port VLAN forwarding allows multiple PFS devices to be cascaded, supporting additional EPT connections to shared tools.

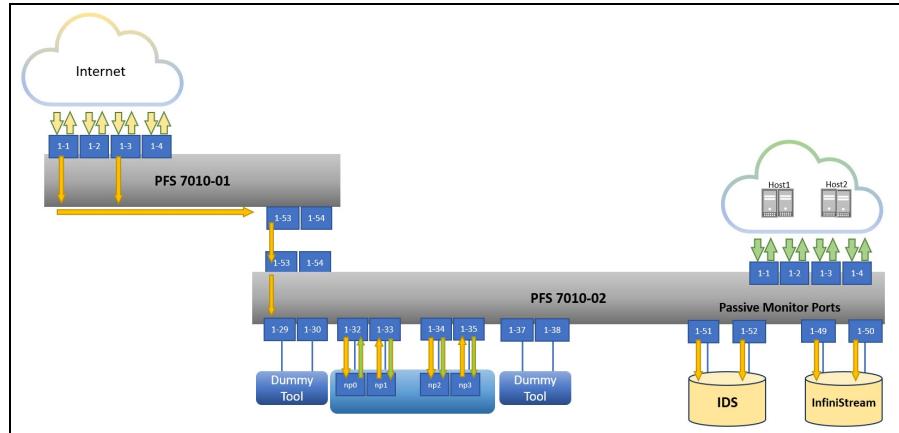
## Simple Tool Chain with Source Port VLAN Forwarding Use Case

The following diagram shows two pairs of inline network ports from traffic to cascading PFS devices. Another four monitoring ports can be used for passive monitoring tools.

- Customer packets include one VLAN tag.
- PFOS adds one VLAN tag to packets entering toolchain at PFS 7010-01.



- PFOS adds another VLAN tag to packets traveling from PFS 7010-01 to PFS 7010-02, when entering PFS 7010-02 Toolchain.
- Packets cascading to PFS 7010-02 tools will have three VLAN Tags, exceeding hardware filter processing limitations.

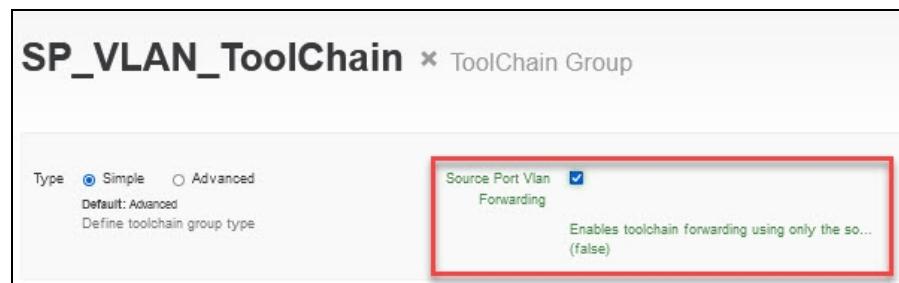


To configure Source Port VLAN Forwarding in this scenario:

- Enable VLAN Tags at Inline Network Port Group. See [Configure Port Group Details - Inline Network Port Group](#).



- Create a Simple Tool Chain with Source Port VLAN Forwarding enabled.



## Advanced Tool Chaining

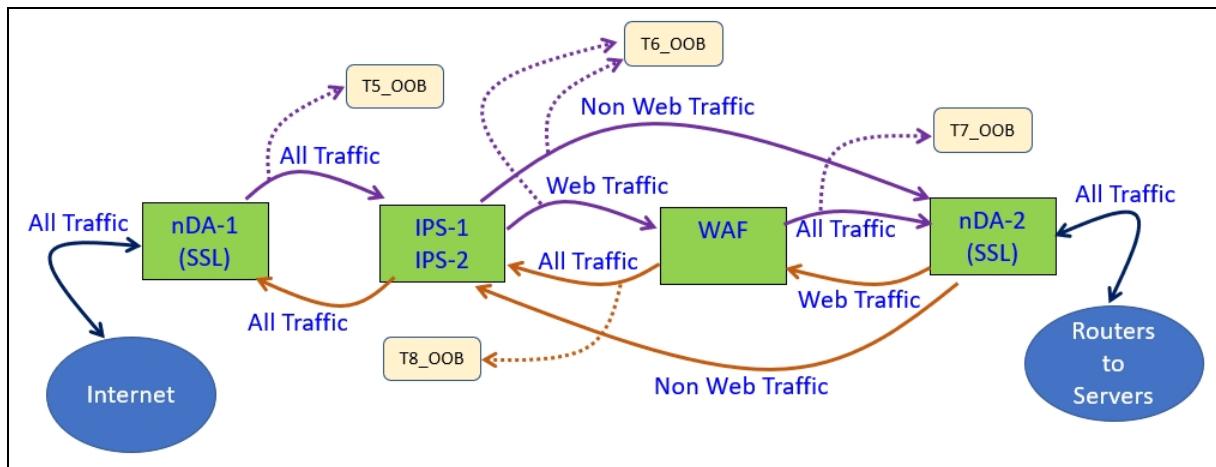
**Note:** This feature is only supported on PFS 6000 and PFS 7000 Series.

Advanced Tool Chain allows filters settings between tools that give flexibility on traffic flow to any direction or exit tool chain.



## Advanced Tool Chain Use Case

The following diagram shows network traffic feeding into the nGenius Decryption Appliance (nDA) to decrypt SSL encryption. The nDA-1 sends decrypted traffic to IPS tools for security, and Web Application Firewall (WAF) tool to analyze HTTP and HTTPS packets. PFOS Advanced tool chain feature allows traffic to be filtered at each tool and forwarded to different tools.



**Figure 6.2 - Advanced Tool Chain Use Case Diagram**

### Prerequisites

The following components must be configured prior to configuring tool chains. You will be selecting these components as you build the tool chain.

- [Port Settings](#)
- [Inline Network Port Groups](#)
- [Inline Monitor Port Groups](#)
- [Monitor Port Groups](#)
- [Forwarding Filters](#)

Also, refer to [Tool Chain Resource Limits and Considerations](#) for additional information.

### Port Settings

The following graphic shows example port settings for [Figure 6.2](#). See [Configuring Ports](#) for port configuration details.



Port ID	Name	Class	Link	Speed	XCVR Model	XCVR Type	PWR Rx (dBm)	PWR Tx (dBm)
1-1	S1-1_Primary-Int	Inline-Network	up	1000	FINISAR CORP. FCLF8522P2BTL	1000Base-T	-N/A-	-N/A-
1-2	S1-2_Primary-Server	Inline-Network	up	1000	FINISAR CORP. FCLF8522P2BTL	1000Base-T	-N/A-	-N/A-
1-3	S2-1_Secondary-Int	Inline-Network	up	1000	FINISAR CORP. FCLF8522P2BTL	1000Base-T	-N/A-	-N/A-
1-4	S2-2_Secondary-Server	Inline-Network	up	1000	FINISAR CORP. FCLF8522P2BTL	1000Base-T	-N/A-	-N/A-
1-13	nDA_1A	Inline-Monitor	up	10000	INNOLIGHT TR-PX85S-NRS	1G/10GBase-SR	-2.86	-3.27
1-14	nDA_1B	Inline-Monitor	up	10000	INNOLIGHT TR-PX85S-NRS	1G/10GBase-SR	-2.68	-3.28
1-15	nDA_2A	Inline-Monitor	up	10000	INNOLIGHT TR-PX85S-NRS	1G/10GBase-SR	-2.72	-2.94
1-16	nDA_2B	Inline-Monitor	up	10000	INNOLIGHT TR-PX85S-NRS	1G/10GBase-SR	-2.8	-3.86
1-17	AED_A	Inline-Monitor	up	10000	INNOLIGHT TR-PX85S-NRS	1G/10GBase-SR	-2.81	-3.05
1-18	AED_B	Inline-Monitor	up	10000	INNOLIGHT TR-PX85S-NRS	1G/10GBase-SR	-2.48	-3.91
1-21	T1_IPX-1	Inline-Monitor	up	10000	INNOLIGHT TR-PX85S-NRS	1G/10GBase-SR	-3.54	-3.08
1-22	T1_IPX-2	Inline-Monitor	up	10000	INNOLIGHT TR-PX85S-NRS	1G/10GBase-SR	-3.77	-2.92
1-23	T2_IPX-1	Inline-Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-2.46	-2.29
1-24	T2_IPX-2	Inline-Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-2.42	-2.45
1-25	T3_WAF-1	Inline-Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-3.81	-1.97
1-26	T3_WAF-2	Inline-Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-1.85	-2.53
1-31	T5_OOB	Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-2.65	-2.51
1-32	T6_OOB	Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-1.17	-2.02
1-33	T7_OOB	Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-2.38	-2.19
1-34	T8_OOB	Monitor	up	10000	FINISAR CORP. FTLX8571D3BCV	1G/10GBase-SR	-2.25	-2.14

## Inline Network Port Groups

The following graphic shows example inline network port configuration for the ports connecting to network traffic in [Figure 6.2](#). See [Configuring Ports](#) for port configuration details.

### S1S2\_Servers

Vlan Tag:  Default: enable  
Vlan tagging enable/disable

Power Safe:  Enable if connected to External PowerSafe Tap

**Port Pair** Inline Network Pair

Add ...	Delete	
A Port	B Port	Link Safe
1-1	1-2	Enabled
1-3	1-4	Enabled



## Inline Monitor Port Groups

The following graphic shows example inline monitor port configurations for the IPS-1, IPS-2, nDA-1 (SSL1), nDA-2 (SSL2), and WAF components in [Figure 6.2](#). See [Port Groups](#) for configuration details.

**IPS#1#2**

A Port	B Port	Link Safe	A Health Check Status	B Health Check Status
1-21	1-22	disable	down	down
1-23	1-24	disable	down	down

**SSL1**

A Port	B Port	Link Safe	A Health Check Status	B Health Check Status
1-13	1-14	enable	up	down

**SSL2**

A Port	B Port	Link Safe	A Health Check Status	B Health Check Status
1-15	1-16	enable	up	down

**WAF**

A Port	B Port	Link Safe	A Health Check Status	B Health Check Status
1-25	1-26	enable	down	down

## Monitor Port Groups

The following graphic shows example monitor port configuration for the Passive Monitoring Tool components in [Figure 6.2](#). See [Port Groups](#) for configuration details.

Name	Lb Criteria	pfsMesh Visibility	Status
T5_OOB-1		enable	PortGroupNameResolved
T6_OOB-2		enable	PortGroupNameResolved
T7_OOB-3		enable	PortGroupNameResolved
T8_OOB-4		enable	PortGroupNameResolved

Showing 1 to 4 of 4



## Forwarding Filters

The following graphic shows example forward filtering configuration for the network traffic in [Figure 6.2](#). See [Forwarding Filters](#) for filter configuration details.

Name	Description	Used in Maps	Expression
All_Traffic		0	( mac offset 0 0 mask 0 )
WebTraffic		0	( Dest Port 443 or Dest Port 80 or Dest Port 81 ) or ( Src Port 443 or Src Port 80 or Src Port 81 )
nonmatch		0	
unfiltered		0	

## Create an Advanced Tool Chain

Perform the following steps to create an Advanced tool chain.

1. In the Web UI, select Configuration>Tool Chain. Select Type as **Advanced**. As an Advanced tool chain, traffic filters can be configured between tools to define flow, next tool, or exit the tool chain to specific inline network ports.

Type  Simple  Advanced  
Default: Advanced  
Define toolchain group type

Add

Tool Name *	Inline Monitor Group *	A Side Passive Monitorgroups	B Side Passive Monitorgroups	Tool Failover Action
-------------	------------------------	------------------------------	------------------------------	----------------------

2. To add a tool to the chain, click **Add**. Fields appear for you to modify. Add the four tools from [Figure 6.2](#) and associated Inline Monitor Port groups as shown in the following graphic. (See the [Simple Tool Chain procedure](#) for descriptions of these fields).

Tool Name *	Inline Monitor Group *	A Side Passive Monitorgroups	B Side Passive Monitorgroups	Tool Failover Action
nDA-1	SSL1			SKIP Delete Move
IPS	IPS#1#2			SKIP Delete Move
WAF	WAF			SKIP Delete Move
nDA-2	SSL2			SKIP Delete Move

3. Configure A-side and B-side next tools for the first tool **nDA1** based on traffic flow in [Figure 6.2](#) as shown in the following graphic.



Type  Simple  Advanced  
Default: Advanced  
Define toolchain group type

Tool Name *	Inline Monitor Group *	A Side Passive Monitorgroups	B Side Passive Monitorgroups	Tool Failover Action
nDA-1	SSL1			SKIP

**A Side Next Tool**

Filter	Next Tool	Ignore Ingress Vlan	Inline Network Ports
nonmatch	IPS	<input type="checkbox"/>	1-1 1-10

**B Side Next Tool**

Filter	Next Tool	Ignore Ingress Vlan	Inline Network Ports
nonmatch	End of chain	<input type="checkbox"/>	1-1 1-10

- You have the following options:
  - In the **Filter** field, select a filter to apply before sending traffic to the next tool, or use **nonmatch** for no filtering. **Note:** As with all PFOS filter processing, if you use the "nonmatch" special filter, that entry should be at the bottom of the filter list. If not, all filters below "nonmatch" have no effect.
  - To send traffic to the next tool, select the name of the tool in the **Next Tool** field. If you do not want PFOS to prepend any VLAN to the filter, select **Ignore Ingress VLAN**.
  - To Bypass the rest of this tool chain, select **End of Chain** in the **Next Tool** field. PFOS prepends "VLAN filter" to send traffic back to 1-1 pair of inline-network ports.
  - In **Inline Network Ports** field, specify the port in the inline network port pair to forward traffic; PFOS will not prepend VLAN for this option.
- 4. Configure A-side and B-side next tools for the second tool **IPS** based on traffic flow in [Figure 6.2](#) as shown in the following graphic.



Tool Name *	Inline Monitor Group *	A Side Passive Monitorgroups	B Side Passive Monitorgroups	Tool Failover Action
nDA-1	SSL1			SKIP
IPS	IPS#1#2			SKIP

**A Side Next Tool**

Filter	Next Tool	Ignore Ingress Vlan	Inline Network Ports
WebTraffic	WAF	<input type="checkbox"/>	1-1 1-10
nonmatch	nDA-2	<input type="checkbox"/>	1-1 1-10

**B Side Next Tool**

Filter	Next Tool	Ignore Ingress Vlan	Inline Network Ports
nonmatch	nDA-1	<input type="checkbox"/>	1-1 1-10

5. Configure A-side and B-side next tools for the third tool **WAF** based on traffic flow in [Figure 6.2](#) as shown in the following graphic.

Tool Name *	Inline Monitor Group *	A Side Passive Monitorgroups	B Side Passive Monitorgroups	Tool Failover Action
nDA-1	SSL1			SKIP
IPS	IPS#1#2			SKIP
WAF	WAF			SKIP

**A Side Next Tool**

Filter	Next Tool	Ignore Ingress Vlan	Inline Network Ports
nonmatch	nDA-2	<input type="checkbox"/>	1-1 1-10

**B Side Next Tool**

Filter	Next Tool	Ignore Ingress Vlan	Inline Network Ports
nonmatch	IPS	<input type="checkbox"/>	1-1 1-10

6. Configure A-side and B-side next tools for the fourth tool **nDA2** based on traffic flow in [Figure 6.2](#) as shown in the following graphic.



Tool Name *	Inline Monitor Group *	A Side Passive Monitorgroups	B Side Passive Monitorgroups	Tool Failover Action		
nDA-1	SSL1			SKIP	<input type="button" value="Delete"/>	<input type="button" value="Move"/>
IPS	IPS#1#2			SKIP	<input type="button" value="Delete"/>	<input type="button" value="Move"/>
WAF	WAF			SKIP	<input type="button" value="Delete"/>	<input type="button" value="Move"/>
nDA-2	SSL2			SKIP	<input type="button" value="Delete"/>	<input type="button" value="Move"/>

**A Side Next Tool**

Filter	Next Tool	Ignore Ingress Vlan	Inline Network Ports		
WebTraffic	WAF	<input type="checkbox"/>	<table border="1"><tr><td>1-1</td><td>1-10</td></tr></table> <input type="button" value="Delete"/>	1-1	1-10
1-1	1-10				

**B Side Next Tool**

Filter	Next Tool	Ignore Ingress Vlan	Inline Network Ports		
nonmatch	End of chain	<input type="checkbox"/>	<table border="1"><tr><td>1-1</td><td>1-10</td></tr></table> <input type="button" value="Delete"/>	1-1	1-10
1-1	1-10				

7. Add passive monitoring ports group for each tool

### nDA-IPS-WAF\_ToolChain

New Group

Type  Simple  Advanced  
Default: Advanced  
Define toolchain group type

Tool Name *	Inline Monitor Group *	A Side Passive Monitorgroups	B Side Passive Monitorgroups	Tool Failover Action		
nDA-1	SSL1	T5_OOB-1		SKIP	<input type="button" value="Delete"/>	<input type="button" value="Move"/>
IPS	IPS#1#2	T6_OOB-2		SKIP	<input type="button" value="Delete"/>	<input type="button" value="Move"/>
WAF	WAF	T7_OOB-3	T8_OOB-4	SKIP	<input type="button" value="Delete"/>	<input type="button" value="Move"/>
nDA-2	SSL2			SKIP	<input type="button" value="Delete"/>	<input type="button" value="Move"/>

- Click **Apply** in the toolbar to save the settings to the running configuration.
- Add the tool chain to an [Inline Traffic Map](#). The associated Inline Traffic Map name will appear in the Ref Map section at the bottom of the Tool Chain page.

## Inline Traffic Maps

To map Inline Network input port groups to Inline Monitor output port groups, go to the Traffic Maps page. Inline traffic map settings are different from those of other traffic maps. The main differences are:

- Inline traffic maps can only use port groups, while other traffic maps can use port groups or individual ports.
- Different processing criteria (tool chain filters, passive monitor groups, and load balancing criteria) can be specified for A-side and B-side ports.



- Load balancing criteria can be specified in inline traffic maps, but output load balancing groups are not available.
- The combined load balancing criteria of inline traffic maps on the A side and the B side apply to inline monitor port groups associated with the traffic maps through a tool chain.

## Create an Inline Monitor Traffic Map

1. From the Traffic Maps page, click **Add**.
2. Enter a name to identify the map, and click **Add** to save the map and display the settings.

The screenshot shows the 'Traffic\_to\_Servers' configuration dialog. It includes fields for Description (string), Type (inline Monitor), Inline Flow (Forward), Inline Network Group (S1S2\_Servers), A Side Toolchain Filter (WebTraffic), B Side Toolchain Filter (All\_Traffic), A Side Passive Mongroup, B Side Passive Mongroup, A Side Lb Criteria (IP\_Dest\_Src), B Side Lb Criteria (IP\_Dest\_Src), Toolchain (AED-IPS\_ToolChain), and Map Status.

3. In the Type drop-down list, select **Inline Monitor**.
4. In the Inline Flow section, select **Forward** (the default), **Bypass**, or **Drop** to define the disposition of traffic that matches this map:
  - **Forward:** Transmit traffic through the tool chain configured in the Toolchain field below.
  - **Bypass:** Send filtered traffic directly to the other ports.
  - **Drop:** Drop filtered traffic ingressing into any of the inline network ports in the specified inline monitor port group.
5. In the Inline Network Group section, select the name of a previously defined inline network port group to use as input to this traffic map.
6. Configure the A side of this traffic map:
  - **A Side Toolchain Filter:** Select a previously defined filter. If traffic matches this filter, it is transmitted to the A side of the cool chain.
  - **A Side Passive Mongroup:** Optionally select a previously defined monitor port group. If specified, matching traffic is also sent to the specified port group.
  - **A Side Lb Criteria:** Optionally select a pre-defined or user-defined set of load balancing criteria to apply to A-side traffic. For more information on load balancing criteria, refer to [Traffic Load Balancing](#).
7. Repeat the previous step for the B side fields.
8. Choose **Tool Chain**. In the Use Case examples, select **Simple** tool chain "AED-IPS\_ToolChain" or **Advanced** tool chain "nDA-IPS-WAF\_ToolChain".



Group		
Name	Type	
AED-IPS_ToolChain	simple	
nDA-IPS-WAF_ToolChain	advanced	

9. Click **Apply**. The traffic map is now automatically applied.

For details on reordering, moving, deleting, and merging traffic maps, and viewing traffic map status, refer to [Traffic Maps](#).

## Tool Chain Resource Limits and Considerations

The following resource limits apply to tool chains:

- Up to 32 tool chain groups can be configured on one system.
- Up to 16 tools can be configured in one tool chain.
- Additionally, the limits on inline network port groups and inline monitor port groups apply. For details, refer to [Port Groups](#).

The following additional considerations apply:

- An inline monitor port group can be associated with multiple tools, even tools in different tool chains. In such cases, all filters defined in those tools associated with the inline monitor port group are applied to this inline monitor port group in the order of inline traffic maps containing those tools. You should carefully design those tools and arrange the inline traffic maps to achieve the intended traffic forwarding.
- The next-tool configuration is highly flexible. It can even point to the tool itself, without warning. NETSCOUT recommends that you design tool chains carefully to avoid possible misconfiguration and loops.
- When configuring an Inline Tool Chain where the [VLAN Tag is disabled at the inline network port group \(INPG\)](#), in order to apply a filter containing a VLAN at both inline network ports (map filter) and any of the inline monitor ports (next tool filter), both filters must contain the same VLAN(s).
- User-defined VLAN IDs are supported on Inline Network (IN) ports with the following limitations:
  - The VLAN IDs must be unique across the IN ports (as the VID is the key component in passing traffic across the tool chain).
  - The VLAN IDs must be configured on the IN Ports **prior** to configuring the tool chain. Configuring VLAN IDs on the IN ports after configuring the tool chain may affect tool chain functionality.



- PFS platforms DO NOT support VLAN, Layer-2, or Layer-3 filtering on packets with more than two VLAN tags. By default VLAN tagging is enabled at all inline network port groups. This VLAN tag helps tool chains segregate the flows. If VLAN tagging is enabled, all packets entering inline tool chains carry one extra VLAN tag so the system can determine traffic destination when exiting tools. Refer to [Filtering on Packets with Multiple VLAN Tags](#) for limitations and impacts on inline tool chains.
- The VLAN Tagging property of the ports in the Passive Monitoring port groups will be ignored, when the port group is attached to traffic running through Inline-Monitoring ports.

## LinkSafe

Inline Network port pairs can be configured to use the NETSCOUT proprietary LinkSafe algorithm to enforce the same state on both interfaces.

Most aggregation taps act as an actual Ethernet end device on each of their network ports. For example, when the tap is turned on, each network element establishes a link with the tap itself, rather than with the other network element. The tap takes the received and decoded data from the one link and re-encodes and transmits it on the paired link. This procedure is duplicated in the other direction, making the tap a simple bridge between the two network elements.

However, this has a serious drawback for devices with redundant links. If one of the network links to the tap fails for any reason, this failure is never propagated to the link on the other side of the tap. This means that the device on the still-working side never knows that there is a problem and, therefore, never takes any action to correct the problem, such as routing packets over a redundant link. Because of this problem, most aggregation-capable taps are a failure point that can stop network flow even if the network elements themselves have a backup path.

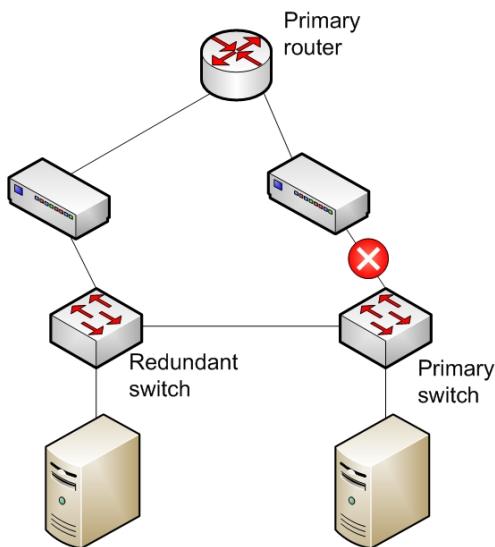
LinkSafe solves this problem by using an intelligent controller inside the device to watch the link status of both sides. If one side fails, then the other side is forced down, thus propagating the error condition to the other network device. When the failed link is fixed, the device immediately re-enables the other side. This behavior is bi-directional; therefore, a failure on either link is propagated to the opposite side, which allows the device to establish a redundant path around the failure. No user intervention is required when the link fails or is re-established.

To simplify installation, LinkSafe is not enabled until both links are up. Immediately after power up, the system will leave both links enabled. This allows for easy link status verification during the installation process. After both network links are up, LinkSafe begins to watch the link status and propagate any error conditions.

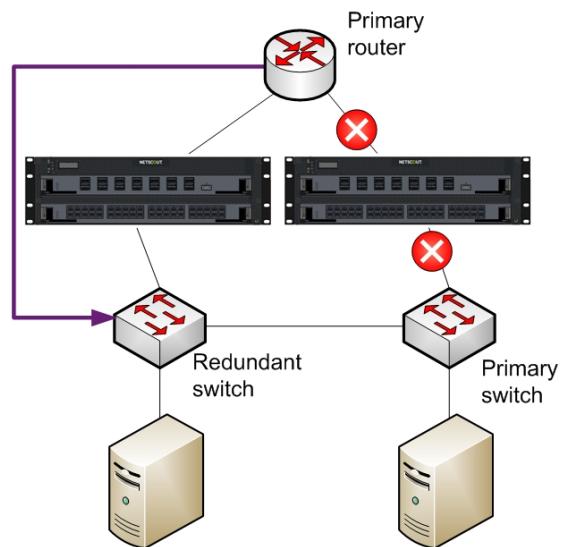
This diagram shows sample networks without LinkSafe (on the left) and with LinkSafe (on the right):



Without LinkSafe



With LinkSafe



### Configure LinkSafe

1. Go to the Port Groups page for the Inline Network port that you want to configure.
2. In the A Port column, click the A-side of the port pair that you want to configure.

The screenshot shows the 'INPG1' Port Group configuration page. Under the 'Port Pair' section, the 'A Port' column for the first entry (1-1) is circled in red. The table rows are:

A Port	B Port	Link Safe
1-1	1-2	Disabled

3. In the Linksafe section, select **Enabled** to enable LinkSafe, or deselect it to disable.
4. Click **Apply** in the toolbar to save the settings to the running configuration.

The screenshot shows the detailed configuration for port pair 1-1. The 'B Port' dropdown is set to '1-2'. The 'Link Safe' checkbox is checked and circled in red. Below the checkbox, the text 'Enable/Disable Link safe on these ports' is visible.

For more information on configuring an inline network port group, refer to [Port Groups](#).



## About interconnected LinkSafe ports

When connecting ports on two systems to each other, you should avoid enabling LinkSafe on both ends of such connections. Any interconnect of LinkSafe-enabled ports can lead to race conditions that could cause the ports to stay down and fail to re-establish the link between them.

NETSCOUT recommends that, when connecting ports on two systems to each other, you enable LinkSafe on only one side of the connection.

## Health Check Profiles

You can use Health Check profiles to monitor the status of inline tools on a subsecond basis.

Health checks work by sending Control traffic into the tool and expecting either a pattern or same packets egressing out of the tool. By recording or counting the packets egressed out of the tool, PFOS can analyze and determine the status of the tool. If the packet is not received, PFOS considers the tool to be offline. If the packet received is modified other than specified in the configuration, PFOS considers the tool to be malfunctioning. In either case, an event and Syslog message are triggered.

There are two types of health check packets: one for positive health check validation, and other one for negative health check validation. You can enable either or both types for a single health check definition.

A health check library is attached to Inline Monitor ports in Inline Monitor port groups.

This example shows a health check library entry that contains both positive (return) and negative (no return) validation. The one on the top is designed to return under normal operation, and the one on the bottom is designed to not return:



asc x

Return  Enable for Positive Health Check

**Return Info**

Transmit Rate  Default: 10000  
Valid values: 200—4294967295  
Packet to send for millisecond

Destination Mac Address  Default: ff:ff:ff:ff:ff:ff  
Destination MAC Address

Payload  Default: 08000000000000000000000000000000...  
Packet Payload

Filer-Expression:  Selected Expression: IP Protocol 6 and ( TCP Dest Port 22 or TCP Source Port 22 )

Filter Expression to match on return Packet

Wait Time  Default: 500  
Valid values: 200—4294967295  
Expect return packet in millisecs

No Return  Enable for Negative Health Check

**Noreturn Info**

Transmit Rate  Default: 10000  
Valid values: 200—4294967295  
Packet to send for millisecond

Destination Mac Address  Default: ff:ff:ff:ff:ff:ff  
Destination MAC Address

Payload  Default: 08000000000000000000000000000000...  
Packet Payload

Filer-Expression:  Selected Expression: IP Protocol 6 and ( TCP Dest Port 443 or TCP Source Port 443 )

Filter Expression to match on return Packet

## Health Check Configuration Parameters

Use the following parameters to create a positive (return) or negative (no return) health check.

### Transmit Rate

Specify the number of milliseconds to wait between sending send health check packets. The default value is 10,000 milliseconds (10 seconds); valid values are 200 to 4294967295 milliseconds.

### Destination MAC Address

Specify the Destination MAC address in `ff:ff:ff:ff:ff:ff` format. If you are creating both positive and negative health checks, the entries must use different MAC addresses.

**Note:** If the destination MAC address is not critical, then the default value of `ff:ff:ff:ff:ff:ff` can be used.



## Payload

Specify the string to send in the health check. The string must be a 232-character hexadecimal string; the default value is 08 followed by 230 zeros.

## Filter Expression

Specify a filter expression to apply to returned health check packets. Health check profiles support the following filters on the incoming packet from the inline tool:

- Source and Destination IPv4 addresses and masks
- IP Protocols (UDP/TCP/ICMP/IGMP/OSPF/RSPV/ARP/RARP/Custom)
- L4 (TCP/UDP) Ports
- VLAN ID (Decimal format, 0 to 4095)
- Ethernet type (4 Hex digits); use the pull-down list to restrict the EType settings to a particular protocol

**Note:** Boolean expressions such as OR and AND are not supported for health check packet matching.

For additional details about creating filter expressions, refer to [Traffic Filtering](#).

## Wait Time

Wait time is only applicable for positive (return) health checks. Specify the number of milliseconds to wait for a reply. The default is 500 milliseconds (0.5 second); valid values are 200 to 4294967295 milliseconds.

## Health Check Considerations

- In a health check profile, the positive (return) filter and negative (no return) filter should not be the same. Such misconfiguration will cause the health check status to be always down due to the conflicting filters.
- While load balance is enabled by default inside inline monitor port groups and failover in the event of port state changes, logical load balance failover for inline monitor port groups is enabled only with health check profiles configured and health check triggers associated to them. As of 5.2, this applies to all platforms. See [Health Check triggers](#).

## Create a Health Check

Perform the following to create a health check profile.

1. Go to the Applications page, and click the **Healthcheck** tab. The list of currently defined health checks displays.
2. Click **Add** to begin creating a new health check. Refer to the above example for available fields.
3. Enter a name to identify the health check, and click **Add** to save the map and display the settings.

4. Select **Return**, **No Return**, or both as desired to create a positive and/or negative health check.
  5. Enter [Health Check Configuration Parameters](#) to create a positive (return) health check or negative (no return) health check.
  6. Click **Apply** in the toolbar to save the settings to the running configuration.

When health checks fail, PFOS triggers an event and Syslog message. You can define a [Health Check policy](#) to trigger when health check status fails and, for example, force link down of the ports in the inline monitor port group.

## Delete Health Checks

1. From the Health Checks page, click the line containing the health check that you want to delete. The line is highlighted with a gray background.
  2. If you want to delete additional health checks, control-click on the lines containing those health checks, or shift-click to select a range of lines. Each line you select is highlighted with a gray background.
  3. Click **Delete**.
  4. A confirmation prompt displays. Click **Yes** to confirm the deletion of all selected health checks, or click **No** to cancel the deletion.



## PowerSafe

**Note:** This feature requires the PFS 7000 functionality license.

The External PowerSafe TAP platform provides bypass switch support for failover protection for the PFS 7000 Series. The PowerSafe TAP guarantees uninterrupted network connectivity on each of its segments in instances of power failures or system crashes. Each segment's state can be manually controlled by the PFOS user interface to either bypass or forward traffic.

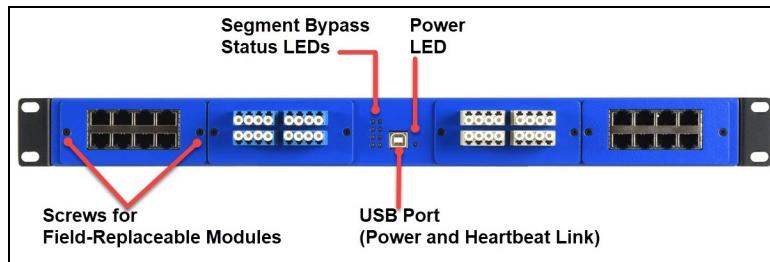


**Note:** Refer to the [\*\*External PowerSafe TAP Quick Connect Guide\*\*](#) for installation details.

### External PowerSafe TAP 3296 Components

The External PowerSafe TAP 3296 supports:

- Up to four field-replaceable modules. Modules are pre-configured with one or two bypass segments, for a total of up to eight bypass segments per chassis. The External PowerSafe TAP 3296 supports the following modules:
  - 1G Copper, RJ45 CAT5e, 2 segments
  - 10G/1G Copper, RJ45 CAT6a, 2 segments
  - 1G/10G/25G/40G/100G SM LC, 2 segments
  - 1G/10G/25G/BiDi(40G/100G) 50 um MM SX/SR LC, 2 segments
  - 1G/10G 62.5 um MM SX/SR LC, 2 segments
  - 40G/100G MM SR4 MPO, 1 segment
- Eight segment bypass status LEDs. ON indicates the segment is in normal operation (traffic flowing to PFS); OFF indicates the segment is in bypass mode, bypassing the PFS.
- USB port connection that provides chassis power and heartbeat link for automatic device-loss detection. PFOS supports USB hot swap for the EPT as follows:
  - When the USB is disconnected, the EPT device handles traffic based on the configured [Poweroff mode](#). PFOS detects USB cable disconnect and sends a SysLog notification and SNMP trap. When heartbeat packets are not received from the PFS, the External PowerSafe TAP assumes the PFS is non-functional.
  - When PFOS detects USB cable reconnect, it sends a SysLog notification and SNMP trap, initializes the Powersafe device and configures EPT modules, and sends the heartbeat again.
  - PFOS generates a SysLog notification and SNMP Trap for USB cable disconnect/reconnect even if PowerSafe feature is disabled.



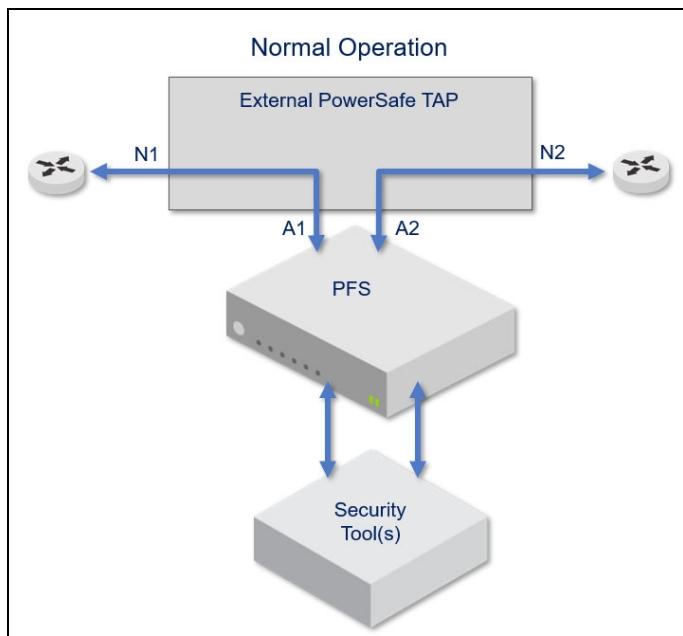
## Understanding PowerSafe

The following sections describe the different traffic flow scenarios supported by the External PowerSafe TAP:

- [Normal Operation](#)
- [Heartbeat Failure Using Poweroff Bypass Mode \(Default\)](#)
- [Power Failure Using Poweroff Forward Mode](#)
- [Heartbeat Failure Using Poweroff Block Mode](#)
- [Heartbeat Failure Using Poweroff Inpairdown Mode](#)

### Normal Operation

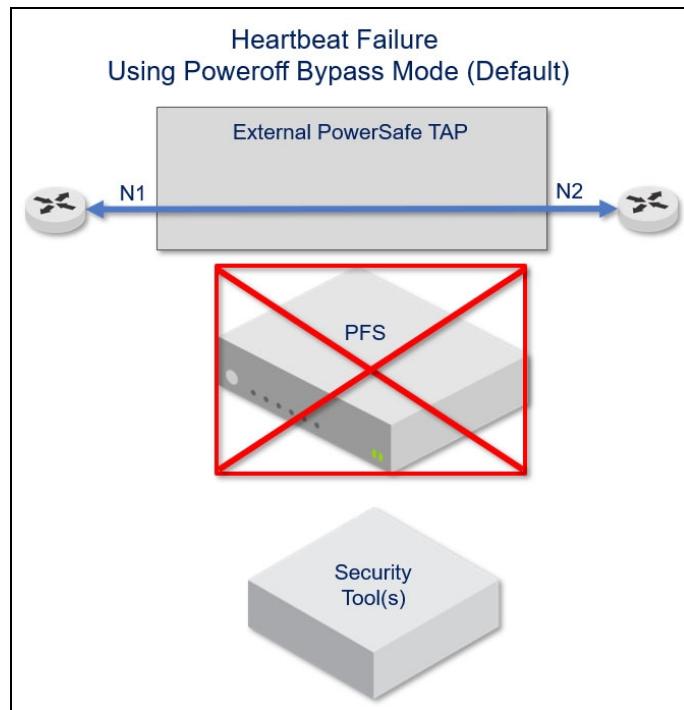
Network traffic passes through the External PowerSafe TAP to the PFS and the security tools. Based on content, the tool(s) may decide to filter or block traffic returned to the network.





### Heartbeat Failure Using Poweroff Bypass Mode (Default)

If the heartbeat between the External PowerSafe TAP and PFS fails (such as in case of power failure), the PowerSafe TAP will bypass the PFS and send traffic directly to the network. This scenario is enabled by setting the [Poweroff mode](#) for this segment to **Bypass**.

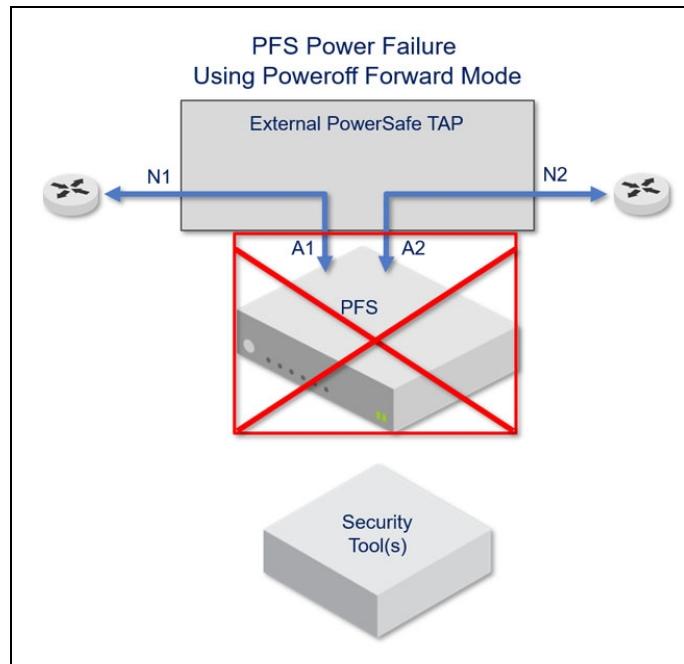




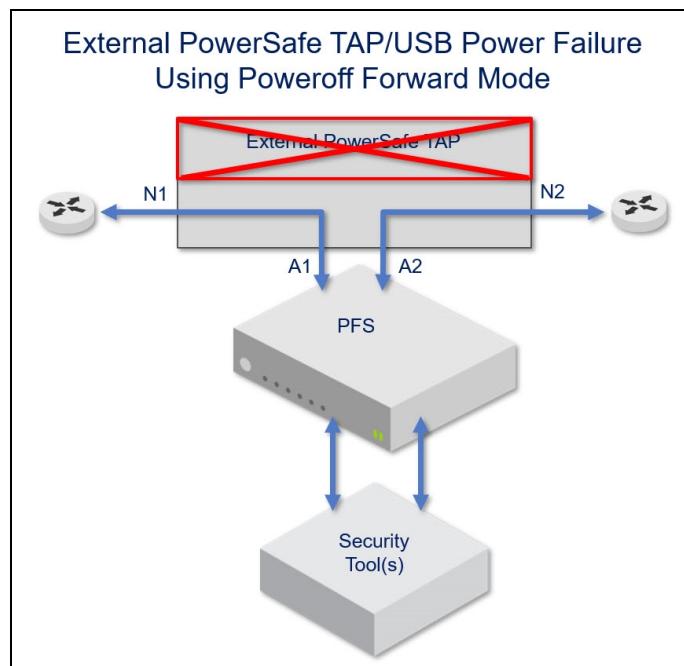
## Power Failure Using Poweroff Forward Mode

The following scenarios are enabled by setting the [Poweroff mode](#) for this segment to **Forward**.

If the External PowerSafe TAP detects a power failure or loss of heartbeat from the PFS, the PowerSafe TAP will continue to forward all network traffic through the PFS. If the PFS has lost power then this will result in the network link being brought down.



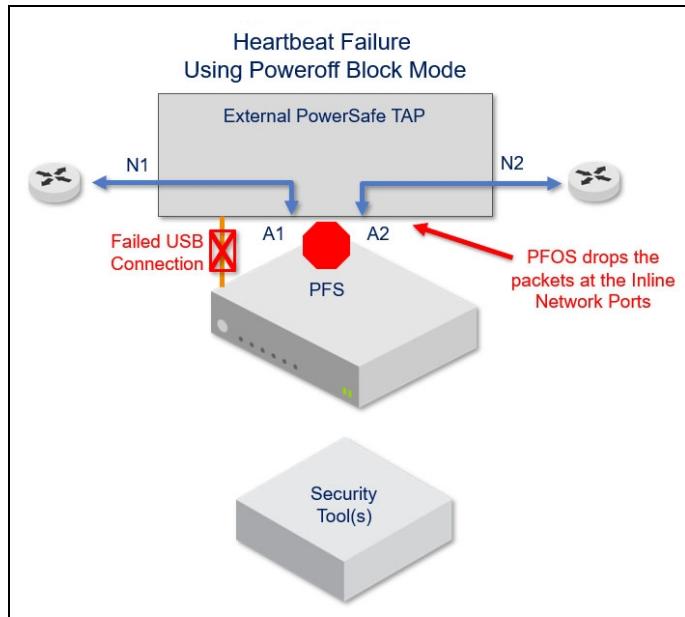
If, on the other hand, the failure is caused by the removal of the USB cable then the network link will stay up and the PFS will process traffic normally.





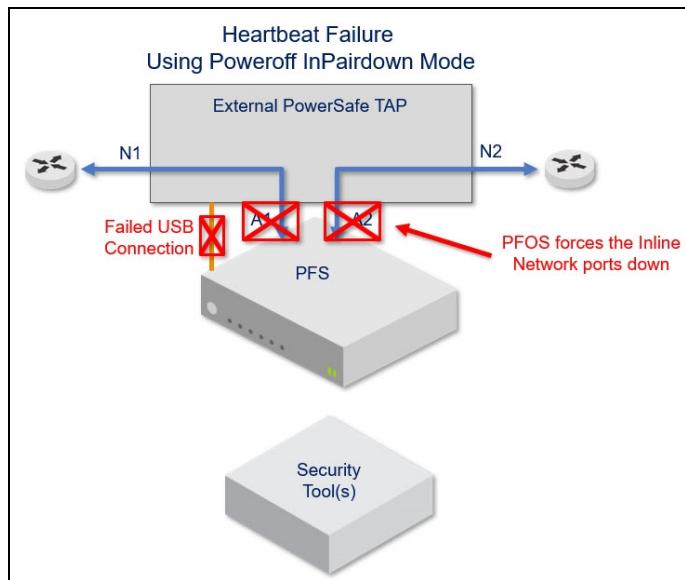
## Heartbeat Failure Using Poweroff Block Mode

If the heartbeat between the External PowerSafe TAP and PFS fails (such as due to the removal of the USB cable), the PowerSafe TAP continues to forward traffic to the PFS which drops the packets at the inline network ports. This scenario is enabled by setting the [Poweroff mode](#) for this segment to **Block**.



## Heartbeat Failure Using Poweroff Inpairdown Mode

If the heartbeat between the External PowerSafe TAP and PFS fails (such as due to the removal of the USB cable), the PowerSafe TAP continues to forward traffic to the PFS which forces the inline-network ports down. This scenario is enabled by setting the Poweroff mode for this segment to **Inpairdown**.





## Enabling the PowerSafe Feature

Once the External PowerSafe TAP is connected to the PFS unit with the USB cable, you can enable it on the System>Features page by selecting the **Powersafe** checkbox. Once enabled, PFOS detects the PowerSafe modules and segments.

### System

Basic Information Network Source Port VLAN Tagging Features **Syslog Trace Log nCM NMS**

FIPS Mode <input type="checkbox"/> <small>Enable FIPS mode to use only FIPS-validated cr...</small>	Powersafe <input type="checkbox"/> <small>Enable/Disable powersafe feature</small>	Hash Algorithm <input type="button" value="Xor 16"/> <small>Default: xor16 Hash algorithm to use for load balancing. xor1...</small>
Tunnel <input type="button" value="Enable"/> <small>Default: enable Enable Tunnel to use tunnel features Warning!...</small>	Map Profile <input type="button" value="Auto"/> <small>Default: auto profile to be applied towards traffic maps</small>	
MPLS <input type="checkbox"/> <small>Enable MPLS Stripping to use MPLS Stripping fe...</small>	MPLS Max Labels <input type="text" value="1024"/> <small>Default: 1024 Valid values: 1—24576 Number of MPLS labels supported Max dynamic la...</small>	
MPLS Cleanup Mode <input type="button" value="Manual"/> <small>Default: manual Cleanup method used to flush dynamic MPLS labe...</small>		
Common Criteria Mode <input type="checkbox"/> <small>Enable common criteria compliant mode Warning!...</small>	Custom Hash <input type="button" value="Enable"/> <small>Default: disable Custom hash support for traffic distribution. ...</small>	Custom Bytes <input type="text" value="4"/> <small>Default: 2 Number of custom hash bytes to support for tra...</small>

## Viewing PowerSafe Hardware Details

You can view the External PowerSafe TAP device details on the Hardware>Powersafe page.

### Hardware

State... Slots Fabric Module Management Module Fan Tray Power Supplies Powersafe Module

State	online	Product ID	3296
	<small>Default: offline PowerSafe device Connection State</small>	<small>Default: NA PowerSafe device Product ID</small>	
Vendor ID	14A6	Serial Number	1F30B145180003
	<small>Default: NA PowerSafe device Vendor ID</small>	<small>Default: NA PowerSafe device Serial Number</small>	
Firmware Revision	4	<small>Default: NA PowerSafe device Firmware Revision</small>	
Module ID	Module Type	Segments	
1	LC-SingleMode	2	
2	LC-MultiMode-50	2	
3	MPO-MultiMode	1	
4	RJ45-10G/1G-Copper	2	

**Note:** Verify the USB connection from PFS to the External PowerSafe TAP (EPT) is established before you configure the EPT. Once the USB connection is established and the EPT receives power from the PFS, the *Powersafe Module State* will display as “online” after the PowerSafe feature is enabled at System>Features>Powersafe.



## PFS 7110-Specific EPT Connection Procedure

Due to a hardware limitation, the EPT needs to connect to the PFS 7110 USB port **prior** to the PFS 7110 booting up or powering up. If the EPT is connected to the PFS 7110 USB port when the PFS is up and running (also known as "Hot Plug-in"), the PFS cannot detect the EPT.

If the EPT is connected to the PFS 7110 while running, verify the EPT is physically connected to PFS 7110 USB port and PowerSafe is enabled at Global Settings>System>Feature>PowerSafe. If Hardware>PowerSafe>State displays as *offline*, perform the following steps to establish the connection from the PFS 7110 to the EPT:

1. At the Web UI, go to the Configuration>PowerSafe>Usbreconnect page and click **Usbreconnect** to establish connection from the PFS 7110 to the EPT.

**Note:** You can also use the following command at CLI for PFS 7110:

```
PFOS# powersafe usbreconnect  
USB reconnected
```

2. At the Web UI, go to the Hardware>PowerSafe page to confirm the EPT state is online before continuing to configure other EPT settings.

## Configuring PowerSafe Settings

You configure PowerSafe settings on the PowerSafe Configuration page. From the Powersafe page, click the module number that corresponds to the segment you want to configure.

The screenshot shows the NETSCOUT Powersafe Configuration interface. On the left, there's a navigation sidebar with various options like Configuration, Ports Settings, Port Groups, Powersafe (which is highlighted with a red circle), Tool Chain, Trigger Policies, Tunnel Settings, Load Balance Groups, Traffic Maps, Libraries, Forwarding Filters, Load Balance Criteria, Applications, and Notifications. The main area is titled 'Powersafe Configuration' and contains a 'Module Info' section with a table for 'Powersafe Segments'. The table has columns for Module, Segment, Module Type, Segment Name, Fiber Pair State, Operational State, Manual Mode, Trigger Mode, and Poweroff Mode. Row 1 is selected and highlighted with a red arrow. The 'Segment Name' field for row 1 is set to 'string'. Below the table, there's a detailed configuration panel for 'Powersafe Segments' with fields for Segment Name, Fiber Pair State, Operational State, Manual Mode, Poweroff Mode, Inline Network Ports, Trigger Mode, Trigger Name, and State.

For all segments on the External PowerSafe device, you can configure:

- Segment Name
- Poweroff Mode
- Manual Mode
- Inline Network Ports
- PowerSafe Trigger Mode



## Poweroff Mode

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 choices are:

- **Bypass (pass-through or fail-open):** When PFS fails, traffic continues through the network, bypassing the PFS device.
- **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.
- **Block** - If the heartbeat between the External PowerSafe TAP and PFS fails (such as due to the removal of the USB cable), the PowerSafe TAP continues to forward to the PFS which drops the packets at the inline network ports (see [PowerSafe Inline Network Port Group Settings](#) for details).
- **Inpairdown** - If the heartbeat between the External PowerSafe TAP and PFS fails (such as due to the removal of the USB cable), the PowerSafe TAP continues to forward traffic to the PFS which forces the inline-network ports down (see [PowerSafe Inline Network Port Group Settings](#) for details).

The [PowerSafe Manual Mode](#) and [PowerSafe Trigger Mode](#) features can override this configuration.

## PowerSafe Manual Mode

The PowerSafe Manual Mode allows you to control traffic flow, on demand, for any module segment. The configuration takes effect immediately and overrides the [Poweroff Mode](#) setting that is applied when the PFS unit loses power.

The manual control override options are:

- **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 network.
- **Off:** Normal operational mode. This is the default behavior for the PowerSafe segments. When manual override is off, the [Poweroff Mode](#) is applied when the PFS loses power. [Trigger mode](#) settings only take effect when Manual mode is set to OFF.



- **Block** - Prevent traffic from continuing through the network by dropping the packets at the Inline Network Ports connected to the PowerSafe segment (see [PowerSafe Inline Network Port Group Settings](#) for details).
- **Inpairdown** - Bring down the defined inline-network ports connected to the PowerSafe segment (see [PowerSafe Inline Network Port Group Settings](#) for details).

## PowerSafe Inline Network Port Group Settings

The Inline Network Ports option on the PowerSafe Configuration page allows you to define the list of inline-network ports connected to the PowerSafe segment. The ports selected in this setting are the ports PFOS brings down if the manual mode or poweroff mode `InPairdown` or `Block` setting is enabled.

Additionally, Inline Network port groups connected to the External PowerSafe TAP must have the **Power Safe** option enabled. Refer to the [Inline Network Port Group settings](#).

## PowerSafe Trigger Mode

**Note:** Trigger Mode is only available when Manual Mode is set to OFF.

The Trigger Mode 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.

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.

The screenshot shows a configuration dialog for a trigger mode. It has three main sections: 1. Trigger Mode: A dropdown menu showing "Forward" (selected), "Bypass", and "Disable". Below it is a note: "Powersafe action on trigger event". 2. Trigger Name: An input field containing "linkstate1". To its right is a small icon of a gear and a "...". Below the input field is the note: "Name of the trigger to be monitored". 3. State: A dropdown menu showing "Active" (selected), "Inactive", and "Disabled". Below it is the note: "Apply trigger mode when trigger's state is active/inactive".

Perform the following to enable the External PowerSafe TAP mode based on the outcome of a trigger policy:

1. For **Trigger Mode**, select Forward (force fail-close) or Bypass (force fail-open) to configure how you want the External PowerSafe TAP to control traffic flow when triggered. (**Note:** To turn off trigger mode, select Disable.)
2. For **Trigger Name**, select a predefined trigger policy to be monitored.
3. 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.

**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, and then reconfigure the trigger mode settings (refer to Step 4). See also [Use Case: Using PowerSafe Trigger Mode with Inline Network Ports](#) for an example.



4. After the trigger is activated and the event recovers, to return the PowerSafe TAP back to normal operation, perform the following:
  - a. First, configure the Power Trigger Mode to **Disable** to deactivate the trigger. Verify the Fiber Pair (latch) State returns to *Closed* and traffic flow to PFS is normal operation.
  - b. Reconfigure the Trigger mode settings again so when the link between the PFS and the EPT fails again, the Trigger Mode setting can change the PowerSafe latch back to the trigger action.

## PowerSafe Operation Status

Current External PowerSafe TAP operation status are displayed on the PowerSafe Configuration page, in the Operational State and Fiber Pair State columns.

**Note:** If the PowerSafe Fiber Pair State does not match the current manual or trigger mode setting, check the USB connection from the PFS device to the External PowerSafe TAP. Refer to [Viewing PowerSafe Hardware Details](#).

Powersafe Powersafe Configuration									
Module Info Powersafe Segments									
Module	Segment	Module Type	Segment Name	Fiber Pair State	Operational State	Manual Mode	Trigger Mode	Poweroff Mode	
1	1	RJ45-1G-Copper		closed	normal	off	forward	bypass	
1	2	RJ45-1G-Copper		opened	normal	off	bypass	bypass	
2	1	RJ45-1G-Copper		closed	manual-inpairdown	inpairdown	bypass	bypass	
2	2	RJ45-1G-Copper		closed	normal	off	disable	bypass	
3	1	LC-MultiMode-62.5	IT-Network	opened	normal	off	bypass	bypass	
3	2	LC-MultiMode-62.5	Eng-Network	closed	normal	off	forward	bypass	
4	1	LC-MultiMode-50		opened	normal	off	bypass	bypass	
4	2	LC-MultiMode-50		closed	normal	off	disable	bypass	

## Operational State

The Operational State column displays the current Manual Mode settings.

**Note:** The Operational state is not affected when a trigger configured in PowerSafe Trigger mode is activated; only [Fiber Pair State](#) is affected.

Operational State	Definition
Normal	Module operates as manually off; traffic normally comes to the PFS.
Manual-bypass	Module operates as manually bypass.
Manual-forward	Module operates as manually forward.
Manual-Block	Module operates as manually blocked traffic at the Inline Network Ports.
Manual-inpairdown	Module operates as manually inpairdown to shut down the Inline Network Ports.



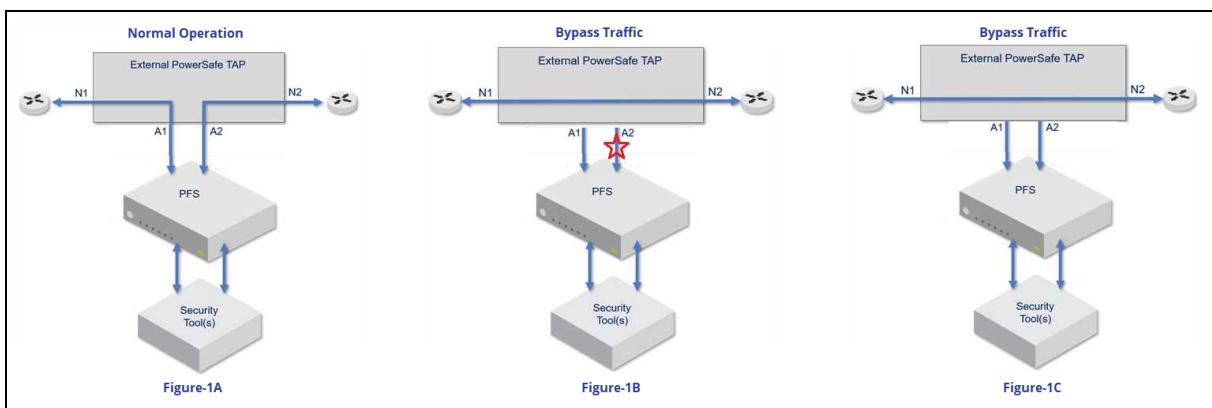
## Fiber Pair State

The Fiber Pair State column displays the current PowerSafe latch state for both copper and fiber modules.

Fiber Pair State	Definition
Closed	PowerSafe TAP fiber or copper latch is set to Forward traffic into PFS. When module mode is configured as Forward, Off, Block, or Inpairdown, or when trigger mode is activated as Forward; <i>Closed</i> is the correct status.
Opened	PowerSafe TAP fiber or copper latch is set to Bypass traffic; traffic is forwarded from network to network, bypassing the PFS. When module mode is configured as Bypass, or when trigger mode is activated as Bypass, <i>Opened</i> is the correct status.

## Use Case: Using PowerSafe Trigger Mode with Inline Network Ports

This use case describes how to use the PowerSafe Trigger Mode with Inline Network Port status. Figure-1A below displays a normal EPT operation with inline function at PFS. If Link A2 between the PFS and the EPT is dropped, as shown in Figure-1B, the Trigger Mode setting can change the PowerSafe latch to bypass traffic (Figure-1C).



1. Configure a [trigger policy](#) to monitor inline network port at PFS to EPT. Example below shows INPG\_Down trigger with initial inactive status.

Name	Status
INPG_Down	inactive

2. Configure [PowerSafe trigger mode](#) as Bypass when the trigger is active.

Trigger Mode <input type="button" value="Bypass"/> Default: disable Powersafe action on trigger event	Trigger Name <input type="text" value="INPG_Down"/> Name of the trigger to be monitored	State <input type="button" value="Active"/> Default: active Apply trigger mode when trigger's state is active/inactive
---	---	--



Before Trigger is activated, the Fiber Pair (latch) State is *Closed* as shown below. Traffic flow to PFS is normal operation as shown in Figure-1A.

Module	Segment	Module Type	Segment Name	Fiber Pair State	Operational State	Manual Mode	Trigger Mode	Trigger Name	State	Poweroff Mode
4	1	LC-MultiMode-50	IT-Network	closed	normal	off	bypass	INPG_Down	active	bypass
4	2	LC-MultiMode-50		closed	normal	off	disable		active	bypass

Showing 1 to 8 of 8

Once the INPG\_Down Trigger is activated due to the inline network port going down at PFS, the Fiber Pair (latch) State is *Opened*. Traffic flow to PFS is Bypass as shown in Figure-1B.

Name	Status
INPG_Down	active

Module	Segment	Module Type	Segment Name	Fiber Pair State	Operational State	Manual Mode	Trigger Mode	Trigger Name	State	Poweroff Mode
4	1	LC-MultiMode-50	IT-Network	opened	normal	off	bypass	INPG_Down	active	bypass
4	2	LC-MultiMode-50		closed	normal	off	disable		active	bypass

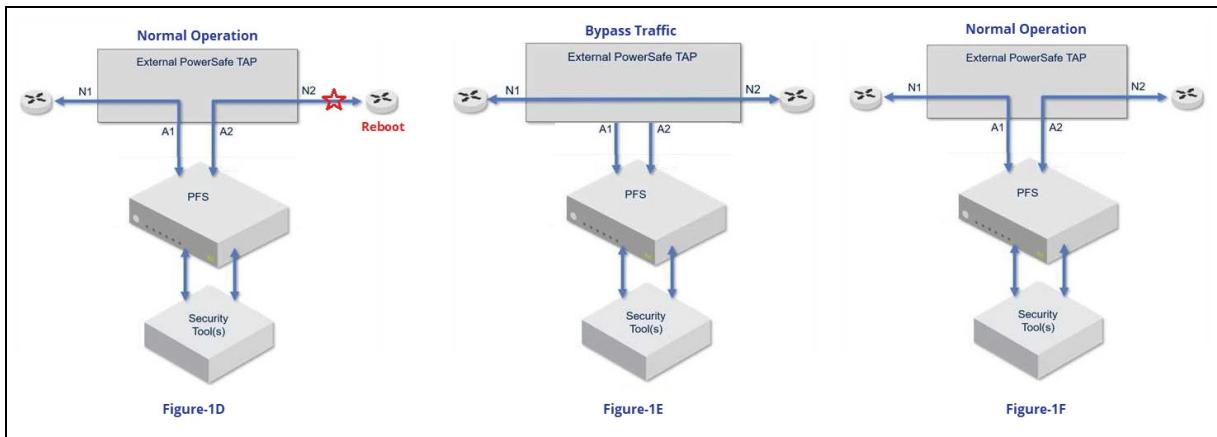
3. After the broken link connection is recovered, to bring up the Inline Network Port at PFS after EPT was set to Bypass mode:
  - a. First, configure the Power Trigger Mode to **Disable** to deactivate the trigger. Verify the Fiber Pair (latch) State returns to *Closed* and traffic flow to PFS is normal operation as shown in Figure-1A.
  - b. Reconfigure the Trigger mode settings again (see Step 2) so when the link between the PFS and the EPT fails again, the Trigger Mode setting can change the PowerSafe latch back to bypass traffic.

**Trigger Mode** Disable ▼

Default: disable

Powersafe action on trigger event  
(Bypass)

**Note:** When the PowerSafe Trigger mode is configured with Inline Network Ports, the trigger could be activated when network devices (such as a router or a gateway) reboot or drop links. Refer to Figure-1D. To avoid this scenario during network maintenance, you can set Manual Mode to Forward prior to the maintenance window. If this is not done, after the network devices are recovered, traffic may be still bypass as shown in Figure-1E. To recover the EPT and PFS back to normal operation state as shown in Figure-1F, refer to the details in Step 3.



# 7 PFOS Maintenance

The following topics describe processes that you might need to perform as part of the ongoing maintenance of your system:

- [Uploading Files](#)
- [Downloading Files](#)
- [Saving and Loading Configurations](#)
- [Maintaining Core Files](#)
- [Maintaining Log Files](#)
- [Maintaining Certificate Files](#)
- [Maintaining SSH Public Key Files](#)
- [Maintaining NTP Key Files](#)
- [Maintaining SSH Knownhost](#)
- [Upgrading PFOS](#)
- [Rebooting PFOS](#)
- [Managing Redundancy](#)

## Uploading Files

Uploading files is a first step in several maintenance procedures.

### Upload a file to the system

1. On the File Management page, if this system has more than one management module installed, click the tab to select the desired management module.
2. On the File Management page, scroll down to the Upload File to Chassis section.



The screenshot shows a user interface for managing files on a chassis. At the top, there's a section titled "Upload File to Chassis". Below it, a "Type" dropdown menu is open, showing several file types: Certificate, Configuration, Firmware, License, Software, and SSHPubkey. The "Certificate" option is currently selected. To the right of the dropdown is a blue "Select files..." button. Further down, there's another section titled "Download File from Chassis" with a "Download Individual File(s)" button.

3. Select the file type (Certificate, Configuration, Firmware, License, Software, or SSHPubkey) from the Type pull-down menu.
4. Click **Select files**, navigate to the location of the file on your local computer, and click **Open**.

**Warning:** Do not interrupt the upload process. Interrupting the upload could cause the file to be corrupted. If you corrupt the upload, you need to delete the incomplete file and upload the file again.

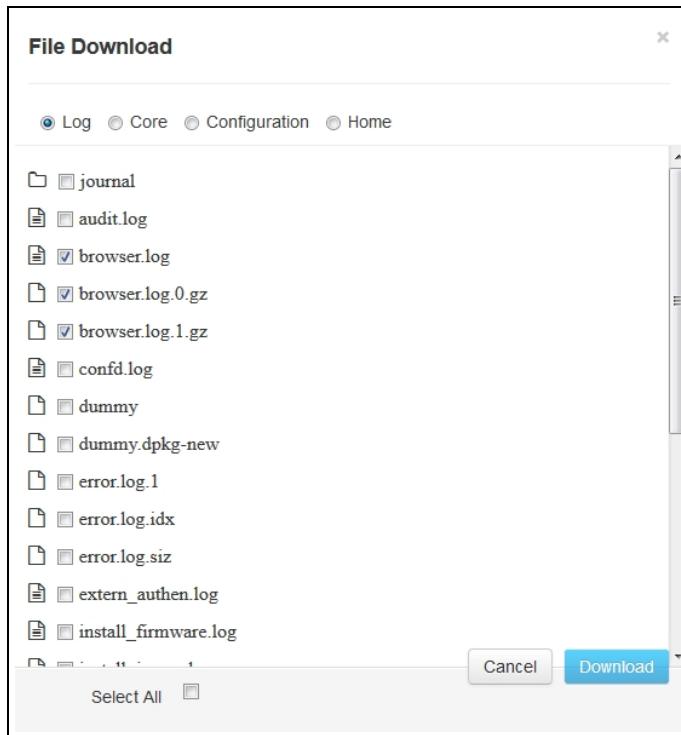
There is a progress bar for the upload. When the upload is complete, the notification icon at the top right of the Toolbar banner changes, and the file displays in the appropriate File Management list.

## Downloading Files

You can download one or more individual files from the system, or you can download a zipped archive of the system's log files.

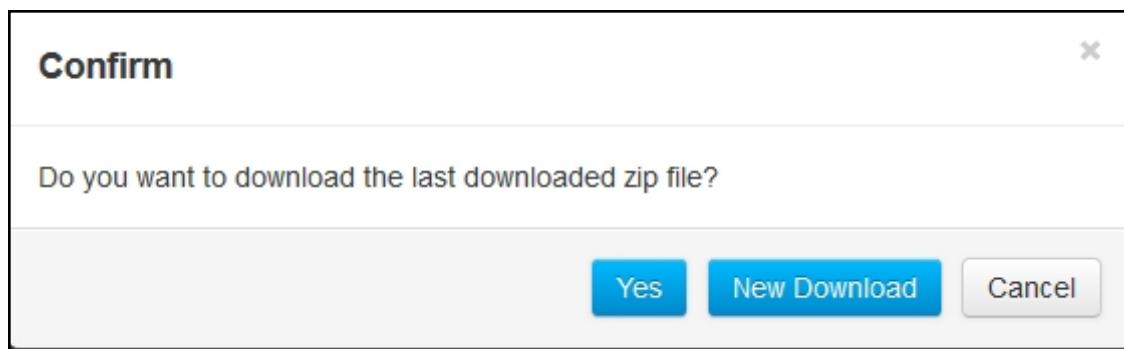
### Download individual files

1. On the File Management page, if this system has more than one management module installed, click the tab to select the desired management module.
2. On the File Management page, scroll down to the Download File from Chassis section.
3. In the Download Individual File(s) section, click **Select & Download**.
4. The four types of downloadable files display. Select one of **Log**, **Core**, **Configuration** or **Home**.
5. A list of available files of the selected type displays. Select the files that you want to download, or click **Select All**, and then click **Download**.



### Download log files

1. On the File Management page, if this system has more than one management module installed, click the tab to select the desired management module.
2. On the File Management page, scroll down to the Download File from Chassis section.
3. In the Retrieve Log Files section, click **Download**.
4. If a log file archive had been created before, then a prompt displays to either download the existing file or create a new one. To download the existing archive, click **Yes**, and proceed to Step 5. To create a new archive, click **New Download**. (If no log file archive had been created before, then this prompt does not display.)



5. The system begins to create a zipped archive of the log files. This process might take several minutes to complete.



Download File from Chassis

Download Individual File(s): [Select & Download](#)

Retrieve Log Files: [Download](#)

Zipping files to : VB6000\_4.3.0.160510~1516\_2016-05-12\_15:41:16.log.tar.gz  
32%

Last downloaded log: No Entries found

6. Your web browser prompts you to open or save the downloaded archive. Respond as desired. The filename has the format `vxosbuild_timestamp.log.tar.gz`, where `vxosbuild` is the build number of the running configuration, and `timestamp` is of the format `yyyy-mm-dd hh:mm:ss`.

**Note:** Only one user can perform a download at a given time. If another user tries to download a file while one is already active, the system displays: "Still communicating, this could take a moment. Press ESC to abort (not recommended)."

## Saving and Loading Configurations

Save or load running configurations to the startup configuration file, or load and restore a PFOS configuration file to your local computer.

### Save a Configuration File

1. On the File Management page, if this system has more than one management module installed, click the tab to select the desired management module.
2. From the File Management page Configuration Files section, click the active link for the configuration you want to save.

File Management

Configuration

Config Name	Size	Updated Time
running-config	N/A	Dec 20 2015 02:54:57
startup-config	N/A	Nov 30 2015 22:01:43

Showing 1 to 2 of 2

3. The Configuration File options page displays. One or more of the following options displays, depending on the original file type selected:
  - **View:** The selected file displays in plain text.
  - **Apply:** The selected configuration is applied as the running configuration.
  - **Save to Node:** The selected file is saved with a user-defined file name to the PFOS file system, where it displays in the configuration file list available for later use.
  - **Save to Workstation:** The selected file is downloaded to your workstation using HTTP.



- **Delete:** The selected file is deleted.
4. Click **Save to Workstation**.

## Load a Configuration File Stored on PFOS

Note the following when restoring a previously saved configuration file:

- Restoring a previously saved configuration file will not restore the previously saved admin user password regardless of which user performs the file restore; the current admin user password remains unchanged after restore. If the previously saved admin password is preferred; reconfigure the admin password after restoring and copying to startup.
  - If a user other than admin restores a previously saved configuration file, the user's *and* admin's previously saved passwords are not restored; the current user *and* admin passwords remain unchanged after restore.
1. Select an existing configuration on PFOS from the Configuration Files list, or upload a previously saved configuration file to PFOS using the Upload File to Chassis utility found on the File Management page of the System Administration section of the Web UI.
  2. Click the active link for the configuration you want to load, such as the Startup Configuration.
  3. The Configuration File options page opens. The available options depend on the original file type selected:
    - **View:** The selected file displays in plain text.
    - **Apply:** The selected configuration is applied as the running configuration.
    - **Save to Node:** The file is saved with a user-defined file name to the PFOS file system, where it displays in the configuration file list available for later use.
    - **Save to Workstation:** The selected file is downloaded to your workstation using HTTP.
    - **Delete:** The selected file is deleted.

If the startup configuration is selected, then the Apply and Delete options are not available.

## Save the Running Configuration to Startup Configuration

NETSCOUT strongly recommends that you copy the running configuration to the startup configuration. Otherwise, all changes since the last save to startup configuration will be lost at the next system boot up. There are two methods for saving the running configurations to the startup configuration file:

- Through File Management, select the **running\_config** link in the Configuration Files list, and click **Apply to Startup Config** in the options window.
- In the toolbar, click **Copy to startup**, and click **OK** to confirm.

## Maintaining Core Files

PFOS automatically generates a core file when an internal error occurs. When contacting technical support, you can help diagnose the problem by including any core files that were generated.



Core files are stored on the PFOS disk until you delete them. If a large number of core files accumulates, the PFOS disk can become full and can prevent PFOS from functioning normally. NETSCOUT recommends that you periodically review the list of core files, save those that are still needed, and delete the others. To view the current percentage of PFOS disk space in use, go to the System Status page or the Basic Information section of the System page.

The list of core files displays on the File Management page:

Cores		
Core Name	Size	Time
core-snmp.gz	350841	Dec 14 2015 05:30:49
Showing 1 to 1 of 1		

### Save or delete a core file

1. On the File Management page, if this system has more than one management module installed, click the tab to select the desired management module.
2. From the File Management page Cores section, click the active link for the core file you want to save.
3. The core file options page displays. The following options are available:
  - **Save to Workstation:** Save the file to your local workstation, with a dialog that depends on the operating system of your workstation. Saving a core file to a workstation does not automatically delete the core file.
  - **Delete:** Immediately delete the core file.
4. Click the desired option.

**core-snmp.gz**

Updated Time	Dec 15 2015 10:43:52	Size	356097
<a href="#">Save to Workstation</a>		<a href="#">Delete</a>	

## Maintaining Log Files

PFOS maintains several log files that can be helpful when reporting issues to technical support.

### Save one log file to your workstation

1. On the File Management page, if this system has more than one management module installed, click the tab to select the desired management module.
2. Go to the Log section of the File Management page.
3. Click the active link for the file that you want to save. A pop-up window displays information about the file.
4. Click **Save to Workstation**.



The screenshot shows the PFOS Log Management interface. At the top, there's a header with a magnifying glass icon and a search bar. Below it is a table listing log files:

Name	Size	Time
audit.log	15395	Dec 19 2015 06:01:39
browser.log	0	Dec 19 2015 01:06:38
confd.log	56037	Dec 19 2015 05:57:24
durandal.log	0	Dec 17 2015 17:00:14

A red arrow points from the main log list to the 'confd.log' file details. A modal window for 'confd.log' is open, showing its updated time (Dec 19 2015 05:57:24), size (56037), and a 'Save to Workstation' button.

### Save all log files to your workstation

1. On the File Management page, if this system has more than one management module installed, click the tab to select the desired management module.
2. Go to the Log Files section of the File Management page.
3. Click **Save to Workstation**. PFOS creates a GZIP archive of all log files. This command might take some time to complete.
4. Open or save the archive. The specific prompts and options depend upon your browser and your workstation's operating system.

The screenshot shows the PFOS File Management interface. On the left, there are sections for 'Log Files' (with a 'Save Log Files' button), 'Upload File to Chassis' (with a 'Type' input field), and 'Reboot Operations'. A modal dialog box titled 'Opening vB6000\_4.2.0.9\_2015-12-20\_23\_41\_40.log.tar.gz' is displayed. It shows the file path, size (22.6 MB), and source (http://10.250.177.60). It asks 'What should Firefox do with this file?' with options: 'Open with' (radio button), 'Browse...', 'Save File' (radio button, selected), and 'Do this automatically for files like this from now on.' buttons for 'OK' and 'Cancel' are at the bottom.

## Maintaining Certificate Files

The following table summarizes the types of certificate files PFOS supports.

**Note:** All certificates must be PEM (base 64 ASCII) encoded and have a file name ending with ".crt". DER-encoded certificates or certificates stored in PKCS#7 (.p7b) or PKCS#12 (.p12 or .pfx)



containers must be converted to PEM format for use with PFOS. Most certificate providers can supply PEM-encoded certificates; if not, free tools such as OpenSSL are available to convert or extract the certificates.

Certificate Type	Files	Notes
<b>Certificate</b> Provides authentication and data encryption	xxx.key - Private key file	PFOS provides default files that are installed at startup and allow any new installation to support HTTPS.  The first time each web browser communicates with PFOS, it will not allow you to connect to the system unless you accept and add an exception for this self-signed certificate. For more information, refer to <a href="#">Logging in to the Web UI</a> .  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 (see <a href="#">Add a Syslog Server</a> for details).
	xxx.crt - Contains the TLS certificate and optionally the chain of signing certificates.	<b>Note:</b> You cannot use PFOS to create a new certificate; however PFOS can generate a Certificate Signing Request (CSR, see below) which can be used by a Certificate Authority to generate a new certificate.  See also <a href="#">Certificate Limitations and Configuration Considerations</a> .
<b>Certificate-Authority</b> Used to upload trust anchor and other intermediate issuer certificate files for browser, Syslog, and LDAP certificates.	xxx.crt	<ul style="list-style-type: none"><li>A certificate file is considered a certificate authority if it contains a Basic Constraints certificate extension with CA set to TRUE.</li><li>PFOS only allows up to 10 certificate authority files to be uploaded.</li><li>Uploaded CAs are used to validate browser certificates in Common Criteria mode and to validate the peer's certificate if syslog TLS is used.</li><li>If <a href="#">Common Criteria mode</a> 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.</li></ul>
<b>Certificate-Syslog</b> Used to authenticate PFOS to Syslog servers.	xxx.key - Private key file	Syslog certificates are used as a client certificate for Syslog TLS mutual authentication (see <a href="#">Add a Syslog Server</a> for details). If no syslog-certificate is installed, the (browser) Certificate (see above) is used as the syslog client certificate.
	xxx.crt	
<b>Certificate-LDAP</b> Used to authenticate PFOS to LDAP servers.	xxx.key - Private key file	LDAP certificates are used as a client certificate for LDAP TLS mutual authentication (see <a href="#">Add an LDAP Server</a> for details). If no certificate-LDAP is installed, mutual authentication is not enabled.
	xxx.crt	



Certificate Type	Files	Notes
<b>Certificate-RADIUS</b> Used to authenticate PFOS to RADIUS servers.	xxx.key - Private key file	RADIUS certificates are used as a client certificate for RADIUS TLS mutual authentication (see <a href="#">Add a RADIUS Server</a> for details). A RADIUS certificate must be installed prior to enabling RADIUS over TLS.
	xxx.crt	
<b>Certificate Signing Requests (CSRs)</b> Contains information a CA needs to create the TLS certificate.	xxxxxxxxx.key - Private key file (file name is user defined)	This file can be generated by using the CLI command <code>generate csr</code> . PFOS generates a new private key file and the <code>server.csr</code> (RSA) or <code>ecc_server.csr</code> (ECC). Both the <code>.key</code> and <code>.csr</code> files are copied to certificate folder. Refer to the <a href="#">PFOS CLI Reference Guide</a> for details.
	server.csr or ecc_server.csr	
<b>Certificate Revoke List (CRL)</b> Contains a list of revoked digital certificates	xxxxxxxxx.crl - Private key file (file name is user defined)	CAs or other trusted authorities generate CRL files; PFOS does not generate <code>.crl</code> files.

## Installing Certificates and Keys

To install a properly signed private key and CA certificate, each file must first be uploaded to PFOS, and then a valid certificate/key pair can be installed. Before installing, refer to [Certificate Limitations and Configuration Considerations](#).

Refer to the following sections for details:

- [Upload a Certificate, Key, or CRL File](#)
- [View, Install, or Delete Certificate Files](#)

### Upload a Certificate, Key, or CRL File

Perform the following steps to upload certificate files, private keys and CRLs.

1. On the File Management page, if this system has more than one management module installed, click the tab to select the desired management module.
2. Go to the Upload File to Chassis section of the File Management page.
3. In the Type drop-down list, select **Certificate**, **Certificate-syslog**, **Certificate-LDAP**, **Certificate-RADIUS**, or **Certificate-Authority** corresponding to the type of certificate the file is for (both certificates and their matching private key must be uploaded with the same Type).
4. Click **Select files**, and use your local workstation's file dialog to select the file that you want to upload.
  - Certificates must have the `.crt` file extension.
  - Private key files must have the `.key` file extension.
  - CRLs must have the `.crl` extension.



After upload, a certificate can have one of the following states:

- **Invalid:** The certificate file is not a valid public key, or there is no matching private key.
- **Current:** The certificate is currently used.
- **Expired:** The certificate end date is past the current date.
- **Standby:** The certificate has a valid private key, but it is not currently used.

A private key file has the same possible states, except that it is invalid only when it is not a valid private key file. A private key does not have an expiration date; this is only for a public certificate.

**Note:** PFOS does not support TLS keys protected by pass phrases (passwords). When a TLS key with a pass phrase is uploaded, PFOS does not have a password to confirm the key file. Therefore, PFOS cannot link the key file to a corresponding certificate file and the certificate/key pair installation fails.

## View, Install, or Delete Certificate Files

1. On the File Management page, if this system has more than one management module installed, click the tab to select the desired management module.
2. Go to the Certificates section of the File Management page. All currently saved certificates and private keys are displayed. There are separate sections for Certificate, Certificate-Authority, Certificate-syslog, and Certificate-LDAP.

The screenshot shows the PFOS File Management interface with four tables:

- Certificate:** Shows 6 entries. One entry (ec\_cert.key) is current, while others are standby. Private keys are listed next to their respective certificates.
- Certificate-authority:** Shows 2 entries, both valid. Descriptions indicate they are Public Key Algorithm: id-ecPublicKey.
- Certificate-syslog:** Shows 4 entries. One is current, while others are standby. Private keys are listed next to their respective certificates.
- Certificate-LDAP:** Shows 4 entries. One is current, while others are standby. Private keys are listed next to their respective certificates.

Name	Size	State	Start Date	End Date	Private Key	Status Message
ec_cert.key	302	standby	0000-00-00T00:00:00+00:00	0000-00-00T00:00:00+00:00		
ecdsaKey.key	302	current	0000-00-00T00:00:00+00:00	0000-00-00T00:00:00+00:00		
acmeCert.crt	2155	standby	2017-01-30T21:59:39-00:00	2027-02-07T21:59:39-00:00	acmeKey.key	Public Key Algorithm: rsaEncryption
ecdsaCert.crt	566	current	2021-06-11T23:37:22-00:00	2022-06-11T23:37:22-00:00	ecdsaKey.key	Public Key Algorithm: id-ecPublicKey
ec_cert.crt	749	standby	2021-04-30T15:21:13-00:00	2031-05-08T15:21:13-00:00	ec_cert.key	Public Key Algorithm: id-ecPublicKey
acmeKey.key	3272	standby	0000-00-00T00:00:00+00:00	0000-00-00T00:00:00+00:00		

Showing 1 to 6 of 6

Name	Size	State	Start Date	End Date	Description
ecdsaCa.crt	558	valid	2021-06-11T23:36:10-00:00	2031-06-09T23:36:10-00:00	Public Key Algorithm: id-ecPublicKey
vsslabadca.crt	1415	valid	2022-02-28T18:13:02-00:00	2027-02-28T18:23:02-00:00	Public Key Algorithm: rsaEncryption

Showing 1 to 2 of 2

Name	Size	State	Start Date	End Date	Private Key	Status Message
ec_cert.key	302	current	0000-00-00T00:00:00+00:00	0000-00-00T00:00:00+00:00		
acmeCert.crt	2155	standby	2017-01-30T21:59:39-00:00	2027-02-07T21:59:39-00:00	acmeKey.key	Public Key Algorithm: rsaEncryption
ec_cert.crt	749	current	2021-04-30T15:21:13-00:00	2031-05-08T15:21:13-00:00	ec_cert.key	Public Key Algorithm: id-ecPublicKey
acmeKey.key	3272	standby	0000-00-00T00:00:00+00:00	0000-00-00T00:00:00+00:00		

Showing 1 to 4 of 4

Name	Size	State	Start Date	End Date	Private Key	Status Message
vm6243.key	1704	current	0000-00-00T00:00:00+00:00	0000-00-00T00:00:00+00:00		
acmeCert.crt	2155	standby	2017-01-30T21:59:39-00:00	2027-02-07T21:59:39-00:00	acmeKey.key	Public Key Algorithm: rsaEncryption
vm6243cert.crt	2053	current	2022-02-28T19:37:22-00:00	2024-02-28T19:37:22-00:00	vm6243.key	Public Key Algorithm: rsaEncryption
acmeKey.key	3272	standby	0000-00-00T00:00:00+00:00	0000-00-00T00:00:00+00:00		

Showing 1 to 4 of 4



3. To display details about any one item, or to access the certificate editor for any item except the default browser certificate or certificate-authority files, click the name of that item. Click **Install** to install the certificate, or **Delete** to delete it.
  - A certificate cannot be installed if it is not in the Standby state.
  - The default certificate is automatically installed and cannot be manually installed.
  - A saved private key can only be viewed or deleted, not installed.
  - When a certificate is installed for HTTPS; the same certificate will be installed to the TCP port used for nGenius Configuration Manager.

**Note:** Not all uploaded certificate files can be installed at PFOS. PFOS does not allow installation of certificates when:

- A certificate “End Date” is expired.
- An incorrect certificate file is uploaded.
- A certificate does not link to any key file (for reasons such as a corresponding key file has not been uploaded yet or the key file is uploaded with a pass phrase (password)).

**cacert.crt**

Size	1000	State	StandBy
Start Date	Jan 24 02:40:06 2017 GMT	End Date	Jan 24 02:40:06 2020 GMT
Private Key	server.key		
		<a href="#">Install</a>	<a href="#">Delete</a>

## Certificate Limitations and Configuration Considerations

- EC certificates are only supported for PFS 5000/7000 platforms.
- For PFOS 6.0.3 and earlier, if [FIPS Mode](#) is enabled on a system with RSA browser certificates installed, on upgrade to PFOS 6.0.4 or later, FIPS mode will be disabled when upgrade completes (PFOS sends a Syslog notification that FIPS is disabled).
- **For PFOS 6.0.4 and later:**
  - FIPS mode cannot be enabled if system has installed RSA browser certificates.
  - RSA browser certificates cannot be installed if FIPS mode is enabled.
  - If system has EC browser certificates installed, downgrade to PFOS 6.0.3 or earlier is disabled. Therefore, NETSCOUT recommends backing up RSA browser certificates before installing EC browser certificates to support potential downgrade scenarios.

## Maintaining SSH Public Key Files

**Note:** PFOS “SSH Public Key” support is for Local authentication only.

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

RSA and ECDSA types of SSH public keys are supported. The SSH public key file should have at least one sshpubkey of type RSA or ECDSA; 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.

### Upload an SSH public key

1. Go to the Upload File to Chassis section of the File Management page.
2. In the Type drop-down list, select **SSHPubkey**.
3. Click **Select files**, and use your local workstation's file dialog to select the file that you want to upload.

### View or delete an SSH public key

1. On the File Management page, if this system has more than one management module installed, click the tab to select the desired management module.
2. Go to the SSHPubkey section of the File Management page. If an SSH public key file is currently installed, information about it displays.

SSHPubkey		
Name	Size	Time
id_rsa.pub	630	Dec 08 2017 00:39:16

3. To display details about the SSH public key file, or to delete the file, click the name of that item. Click **Delete** to delete it.

id_rsa.pub			
Size	630	Time	Dec 08 2017 00:39:16
<a href="#">Delete</a>			

## Maintaining NTP Key Files

Secure Network Time Protocol allows authentication of the NTP servers so only approved time sources provide time values. Users upload an NTP authentication key file and select the corresponding key while [setting the NTP server](#).



## NTP Key File Format

The NTP key file is a text file that has the following format:

**<key number> <authentication method> <key-value>**

Key Number	An integer from 1-65534 used for identifying each key-value
Authentication Method	Specify either <b>MD5</b> and <b>SHA1</b> . For STIG or FIPS compliance, use only SHA1.
Key-value	Create a key with up to 20 character ASCII, or 64 character hexadecimal. Refer to <a href="https://docs.ntpsec.org/latest/ntp_keys.html">https://docs.ntpsec.org/latest/ntp_keys.html</a> for details.

## Upload an NTP Key File

- Once you have created an NTP key file, go to **File Management > Upload File to Chassis**.
- In the **Type** drop-down list, select **NTP key**.
- Click **Select files**, and use your local workstation's file dialog to select the file that you want to upload.

If successful, the name appears in the NTP Key area. The upload will fail if any of the lines in NTP key file do not have the [correct format](#).

Name	Size	Time
ntp.key.txt	11	Jul 28 2020 23:36:08

**Note:** To delete a file, click the name of the file and click **Delete** to delete it.

- Refer to [Timing Sources > NTP](#) to configure NTP servers and assign authentication keys.

## Maintaining SSH Knownhost

PFOS supports a Strict Host Key Checking function for approved servers. The administrator can upload an ssh-knownhost file with server host IP addresses and Public Keys from multiple server hosts to limit PFOS to only establish SSH connections to those server hosts.

## Strict Host Key Checking

Strict Host Key Checking allows authentication of remote servers so PFS devices connect only to approved servers using SSH connections (scp/sftp/ssh tunnel).

Strict host key checking is only enabled if [Common Criteria Mode](#) is enabled. When enabled, the PFS device connects only to known hosts with valid SSH host keys that are stored in a known hosts file. Connections to hosts whose SSH key is not in the known hosts file are refused. When Common Criteria is disabled, there is no host connection restrictions.



If both [Common Criteria Mode](#) and [FIPS Mode](#) are enabled, PFOS will only use ECDSA key type for Strict Host Key Checking. If FIPS mode is disabled, both RSA and ECDSA types of SSH public keys are supported; however, ECDSA is preferred by SSH servers. That is, if the server supports ECDSA, users must upload an ECDSA; an RSA key will not be used if the SSH server negotiates to use ECDSA.

Users can upload an SSH known host file containing server public host keys using CLI or the Web UI.

The example below shows one entry in a knownhost file. It includes three fields: <Server Host IP> <RSA or ECDSA> <Host public key>. Once a file with the entry below is uploaded to PFOS, and [Common Criteria Mode](#) is enabled, PFOS can only allow SSH connections to the server IP address 10.10.10.100 with the matching SSH-RSA public key at the server host.

```
10.10.10.100 ssh-rsa
AAAAB3NzaC1yc2EAAAQABAAQDA1pCJjTjistFdzMZtdbtexu/gX089HnJ9y6qZfspt
7IUkb4vqs7+H1Ozt3pYNkojsVj6cDNxb8KJfnvst+RSj+vsFmwmVSTvyfsuWJLkqmzwIeUp
rw0xYXiE8zPcNH8AsqBbdFX605TwAFHQxCSQWVNUf/8xfPE+9pGX69CH9XgNZx5X6kn35229
kQGiP0ei4HsLzO7EB1xSj8XwCB2DN+4qiF/NMOxwcLssTMmLk1tjFl6SCNOSqAt/kLYP+7gF
XC/vGcq2Nj4J0faMWBP5jg6+d1FnxG5p2PevAPEqyFu1+oj1Pg3KjgRyrxv+I05KqduiT
Af0kBA0KYWNz
```

**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 remote host public keys. 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.

## Upload an SSH Known Host File

The ssh-knownhost file can contain keys from multiple server hosts, but only one ssh-knownhost file can be present on PFOS at any one time. If a new ssh-knownhost file is uploaded, the existing file will be overwritten.

**Note:** Strict host key checking is only enabled if [Common Criteria Mode](#) is enabled.

- Once you have created an SSH Known Host file, go to **File Management > Upload File to Chassis**.
- In the **Type** drop-down list, select **SSH Knownhost**.
- Click **Select files**, and select the file that you want to upload.

If successful, the name appears in the SSH knownhost area.

SSH knownhost		
Name	Size	Time
135_user_known_host_new.txt	589	Apr 20 2021 01:43:33
Showing 1 to 1 of 1		

**Note:** To delete a file, click the name of the file and click **Delete** to delete it.



## Upgrading PFOS

NETSCOUT periodically releases updates to PFOS (vxos image). This software is available only to customers who have a valid software contract in place. In addition to the vxos image upgrade, kernel and chassis firmware upgrades may also be required. Therefore, each PFOS release may require different upgrade procedures. Refer to the **PFOS 6.x Release Notes** for PFOS upgrade details and procedures.

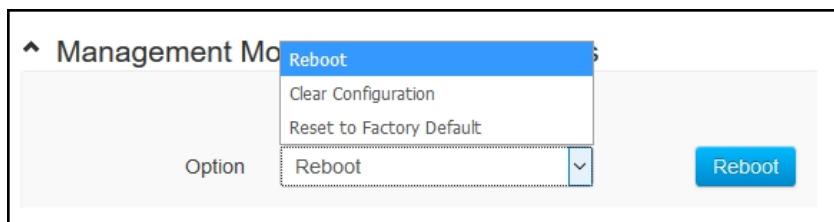
## Rebooting PFOS

You can reboot the entire system from the **System Reboot** button in the toolbar at the top of every page.

Alternately, to reboot just one management module on a system with multiple management modules, you can use the Management Module Reboot Operations section of the File Management page.

### Reboot the system

1. On the File Management page, if this system has more than one management module installed, click the tab to select the desired management module to reboot.
2. Scroll down to the Management Module Reboot Operations section.
3. In the drop-down list, select one of these options:
  - **Reboot:** Reboot the system.
  - **Clear configuration:** Clears all settings except basic system and networking settings (such as IP addresses).
  - **Reset to factory default:** Clears all settings including system and networking settings.
4. Click **Reboot**.



## Managing Redundancy

**Note: This feature is available only on PFS 6010 systems with two management modules.**

On a PFS 6010 with two installed management modules, one management module is always considered active, and the other is on standby.

You can:

- Configure management IP addresses.
- Switch current operation from one management module to the other.



- Upload configuration files to either management module.
- View the redundancy status of management modules.

## Configure Management IP Addresses

PFOS redundancy uses three management interfaces and requires three management IP addresses:

- Management interface 0 is for the virtual IP address of the entire system.
- Management interface 1 is the local IP address for Management Module A.
- Management interface 2 is the local IP address for Management Module B.

NETSCOUT recommends that, during normal operation, you access the system only through the virtual IP address on management interface 0. The local IP addresses are used to log in to each specific management module for debugging purposes only.

The active (primary) management module supports both Web UI and serial console access for local management. However, the standby (secondary) management module supports only serial console access.

1. Go to the Global Settings > System page, and click the **Network** tab.

ID	IP - IP 4 Address	IP - IP 4 Gateway	IP - IP 4 DNS	IPv6 - IP 6 Address	Mac Address
0	10.250.177.240/23	10.250.176.1	10.1.6.70	::/0	C4:EE:AE:05:33:75
1	10.250.177.181/23			::/0	C4:EE:AE:05:33:75
2	10.250.177.182/23			::/0	C4:EE:AE:00:C6:D2

2. Click the number of the management interface that you want to configure.
3. Enter the desired IP address(es).



The screenshot shows a configuration interface for two management modules. Under the 'IP' section, Module 1's IP is set to 10.250.177.182/23. Under the 'IPv6' section, Module 2's IP is set to ::/0 with a default value of ::/0.

- Click **Apply** in the Toolbar to save the changes to the running configuration.

## Switch Current Management Module

In the toolbar at the top of any page, click **Switchover**, and then click **OK** in the confirmation pop-up that displays.



While the redundancy state is Ready, traffic is not affected when a switchover occurs. The configuration database is partially locked to prevent any configuration change during the switchover. The configuration database is unlocked after the transfer of warmboot files is complete.

## Uploading Files to Each Management Module

You can upload files to each management module individually from the File Management page of the System Administration section of the Web UI.

The top of the File Management page displays a tab for each management module installed on the system and indicates which module is currently active. On systems without removable management modules, one tab displays and is always selected.

The File Management page shows two tabs: 'Mgmt-1(active)' and 'Mgmt-2(standby)'. The 'Mgmt-1' tab is selected, displaying a configuration file named 'startup-config' with a size of 0186. The 'Mgmt-2' tab is shown in light blue.

For details on uploading specific types of configuration files, refer to the following sections:



- [Maintaining Certificate Files](#)
- [Maintaining Core Files](#)
- [Maintaining SSH Public Key Files](#)
- [Maintaining Log Files](#)
- [Saving and Loading Configurations](#)
- [Uploading Files](#)

**Notes:**

- License files, SSH public key files, and certificate files are applicable for both management modules and are always uploaded to both at the same time.
- Firmware files can be uploaded only to the currently active management module.

## View Management Module Status

### Front Panel LCD Screen

You can use the LCD screen of the PFS 6010 to identify which management module is active. In this example, CPU1 is currently active, and CPU2 is on standby.

The displays for the active management module look like this:

```
>CPU cards
Fan Tray
Power Supply
Port(8-10): Link UP

>CPU1
CPU2

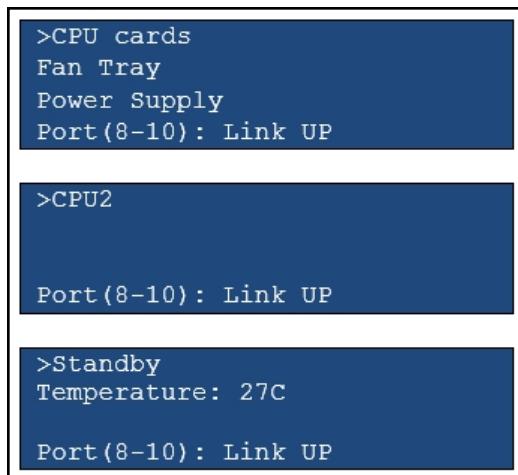
Port(8-10): Link UP

>Active
Temperature: 28C

Port(8-10): Link UP
```



The displays for the standby management module look like this:



For more information on using the LCD screen, refer to the *PFS 6000 Series Hardware Installation Guide*.

## Management Module Status LED

The Status LED of each management module indicates its current redundancy status. The active management module has a green Status LED; the standby module has a yellow Status LED.

For information on management module hardware status indicators, refer to the *PFS 6000 Series Hardware Installation Guide*.

## In the Web UI

On the System Status page, the redundancy status displays at the top of the page. Possible values are:

- **Disabled:** Redundancy is disabled. No switchover can be performed.
- **Syncing:** Initial configuration database replication and any warmboot-related file synchronization.
- **Ready:** Redundancy is available. Switchover can be performed.
- **N/A:** Redundancy is not applicable if a standby CPU is not installed on a PFS 6010 when booting up.

The screenshot shows the 'System Status' page with the following details:

System Information					
Name: SW-189	Location: Sunnyvale, CA USA	Mgmt-1: active	Data Disk Usage: 59%	System Status: OK	
Product ID: 2301	Contact: tsupport@vssmonitoring.com	Mgmt-2: standby	System Disk Usage: 11%	Temperature: 44 °C	
Serial Number: 14100444	Support License: Current	Platform: PFS6010	Redundancy Status: ready		

On the Hardware page, the active and standby management modules are shown on the Management Modules tab:



## Hardware

CPU Cards													
ID	State	SKU P/N	Module P/N	Module Rev	Module S/N	PCBA P/N	PCBA Rev	PCBA S/N	FPGA	Fan 1 Speed	Fan 2 Speed	Fan 3 Speed	Temperature
1	active	VP_02011	VP_01940	AE	VSPV1940-1620001	VA_00779	AA	VMSVSNC-16050210	00007000 rev 0017	15542	16016	15420	31
2	standby	VP_00692	VP_01940	AD	1620010	VA_00779	08	VMSNC-16070736	00007000 rev 0018				

Showing 1 to 2 of 2

## About Licensing and Redundancy

PFOS license keys are linked to the MAC address of the system chassis, not the MAC address of individual management modules. While PFOS is running, the license key files are synchronized between the active and standby management modules.

Therefore, if you switch from one management module to the other, the same license key continues to be active and valid.

However, if you move a management module from one system to another, the license key will be invalid because the chassis MAC address will be different. Before moving a management module from one system to another, be sure to save the existing license key file on the target system and restore it after you have moved the hardware.

## Redundancy Considerations and Limitations

- You cannot run PFOS release 5.x on one management module and PFOS release 4.x on the other management module. NETSCOUT recommends that you run the same build of PFOS on both management modules.
- The management module status LED will not blink when the latch is opened.
- There is no temperature and fan speed reading on the standby management module.
- There is no fabric card reset.
- Each management module must have CPU version 1.3 to use the redundancy features of PFOS release 5.1 and later. Additionally, specific types of line cards require specific firmware versions to support redundancy. For more information, refer to the current release notes.
- If PFS 6010 active and standby management modules are running different PFOS images, the following limitations may apply. **For best practice, NETSCOUT recommends upgrading both management modules so they have the same image installed.**
  - Redundancy synchronization is disabled until both management modules have the same image installed.
  - If the active management module has a newer PFOS image than the image at the standby module, pStack and LLDP functionality may stop working.

# 8 PFOS Diagnostics

These diagnostics tools help you investigate how PFOS is operating and can help in troubleshooting. Some issues might require additional investigation by Technical Support.

- [System Status](#)
- [Statistics](#)
- [Event Notifications](#)
- [Hardware Information](#)
- [SNMP MIBs](#)
- [nGeniusONE PFS Monitoring](#)
- [Syslog Messages](#)

## System Status

The System Status page in the Status section displays the overall status of the system and each chassis line card slot. See [System Status](#) for details.

**System Status**

**System Information**

Name	Location	Mgmt-1	Data Disk Usage	System Status
SW-189	Sunnyvale, CA USA	active	59%	OK
Product ID: 2301	Contact: tsupport@vssmonitoring.com	Mgmt-2:	standby	System Disk Usage: 11%
Serial Number: 14100444	Support License: Current	Platform:	PFS6010	Temperature: 44 °C
		Redundancy Status:	ready	Energy Consumption: 0.13 kWh

**Line Card Status**

ID	State	Time Left	Product ID	Configured Card	SKU P/N	Module Part Number	Module Revision Number	Module Serial Number	PCBA Part Number
1	OK		1310	36S6Qstd	VP_01960	VP_01938	AJ	NSP160881725	VA_00672
2	empty			36S6Qstd					
3	OK		1311	15Qstd	VP_02111	VP_02060	01	16040059	VA_00811
4	empty			40SadVR					
5	empty			36S6Qstd					
6	OK		1312	6Cstd	VP_01961	VP_01939	AC	16095464	VA_00759
7	OK		1410	40SadVR	VP_01986	VP_01982	AF	1234	VS_00724
8	OK		1313	6Q28std	6000NBBGE100	VP_02171	01	17105420	VA_00823



## Statistics

The Statistics page in the Status section shows tabular and graphical views of activity on various system components. Refer to the following sections for details:

- [Network Statistics](#)
- [Deduplication Statistics](#)
- [Flow Statistics](#)
- [Control Packets Statistics](#)
- [Tunnel Statistics](#)
- [Port Group Statistics](#)

Click a listed slot to display information for all of the configured ports in that slot.

The screenshot shows the 'Statistics' page with the 'Network' tab selected. A table displays the configuration for Slot 1:

Slot	Configured Card	Network Reset Time
1	pre-configured	Tue Sep 5 21:55:59 2023

Below the table, a message indicates 'Showing 1 to 1 of 1'.



## Network Statistics

The following example shows network statistics for a specific slot.

Slot 1														
Reset Counters		Statistics Reset Time		Tue Sep 5 21:55:59 2023										
Configured Card		pre-configured		Counters Reset Time										
^ Network Statistics														
Port ID	Speed	Rx Packets	Tx Packets	Rx Pkt/Sec (PPS)	Tx Pkt/Sec (PPS)	Rx Dropped	Tx Dropped	Rx Throughput (Mbps)	Tx Throughput (Mbps)	Rx Utilization (%)	Tx Utilization (%)	Rx Errors	Tx Errors	
1-1	10000	512578955467	0	8454191	0	0	0	8658.88	0.0	100.0	0.0	0	0	
1-2	10000	0	499088069434	0	8208739	0	0	0.0	8405.74	0.0	97.19	0	0	
1-3	10000	0	0	0	0	0	0	0.0	0.0	0.0	0.0	0	0	
1-4	10000	0	0	0	0	0	0	0.0	0.0	0.0	0.0	0	0	
1-5	10000	0	0	0	0	0	0	0.0	0.0	0.0	0.0	0	0	
1-6	10000	0	0	0	0	0	0	0.0	0.0	0.0	0.0	0	0	
1-7	10000	60588	2562894699014	2	4234107	0	0	0.0	4471.14	0.0	51.48	0	0	
1-8	10000	256289462252	60588	4221841	2	0	0	4458.5	0.0	51.34	0.0	0	0	
1-9	10000	60588	256289450015	2	4218666	0	0	0.0	4454.47	0.0	51.29	0	0	
1-10	10000	256289443629	60588	4216739	2	0	0	4453.15	0.0	51.27	0.0	0	0	
1-11	10000	60588	256289424234	2	4229798	0	0	0.0	4466.7	0.0	51.43	0	0	
1-12	10000	256289418015	60588	4228269	2	0	0	4465.89	0.0	51.42	0.0	0	0	
1-13	10000	60588	256289406464	2	4225547	0	0	0.0	4462.15	0.0	51.38	0	0	
1-14	10000	256289400223	60588	4213551	2	0	0	4449.78	0.0	51.23	0.0	0	0	
1-15	10000	0	499087795081	0	8227602	0	13490863459	0.0	8688.36	0.0	100.0	0	0	
1-16	10000	49908778329	0	8225481	0	0	0	8686.98	0.0	100.0	0.0	0	0	
1-17	10000	0	499087752858	0	8225314	0	0	0.0	8686.31	0.0	100.0	0	0	
1-18	10000	499087744363	0	8223382	0	0	0	8684.65	0.0	100.0	0.0	0	0	
1-19	10000	512576584288	512576575120	8442948	8443741	0	1979426	8647.11	8646.36	99.97	99.97	0	0	
1-20	10000	512576566304	512576566383	8441620	8442246	0	1979426	8644.85	8644.88	99.95	99.95	0	0	
1-21	10000	256289271092	256289262732	4219989	4221128	0	0	4321.49	4322.52	49.96	49.97	0	0	
1-22	10000	256289255836	256289254665	4218908	4219780	0	0	4321.34	4320.68	49.96	49.95	0	0	
1-23	10000	0	0	0	0	0	0.0	0.0	0.0	0.0	0.0	0	0	

The following statistics are available to view for each port. To control which statistics display on the page, click the wrench icon. To reset network statistics, select a slot number, click **Reset Counters**, and then select either **This slot only** or **All network counters**.

**Note:** Statistics for Span-Monitor ports are displayed under one physical port.

### Default Statistics

- Port Id:** Indicates the port to which this row pertains. The port identifiers shown correspond to the port identification on the front panel (faceplate) of the line card. For PFOS, the port designation consists of the chassis line card slot position and the port on the line card, such as 1-1. For 40G ports that can be broken out into multiple 10G ports, the format includes a subport designation, such as 1-37.1.
- Speed:** Show the current actual speed of the port, if a link has been fully established. If no link has been established, then these columns are blank.
- (Rx/Tx) Packets:** Cumulative number of good packets through each port.
- (Rx/Tx) Dropped:** Cumulative number of packets that were dropped due to buffer overflow, typically as a result of oversubscription on a monitor port
- (Rx/Tx) Throughput (Mbps):** Relative total amount of traffic through each port at each sampled interval, where each interval is about three seconds.



- **(Rx/Tx) Utilization (%)**: Percentage of utilization of the port at each sampled interval, where each interval is about three seconds.
- **(Rx/Tx) Errors**: Cumulative number of packets that had CRC errors. CRC Errors is a subset of Bad Packets.

### Additional Statistics

- **Link Recovery Count**: Cumulative count of link recovers
- **Link Recovery Time**: Time of last link recovery
- **Rx/Tx 64**: Receive/transmit 64-byte packets
- **Rx/Tx 65 to 127**: Receive/transmit 65-byte to 127-byte packets
- **Rx/Tx 128 to 255**: Receive/transmit 128-byte to 255-byte packets
- **Rx/Tx 256 to 511**: Receive/transmit 256-byte to 511-byte packets
- **Rx/Tx 512 to 1023**: Receive/transmit 512-byte to 1023-byte packets
- **Rx/Tx 1024 to 1518**: Receive/transmit 1024-byte to 1518-byte packets
- **Rx/Tx 1519 to 2047**: Receive/transmit 1519 bytes to 2047 bytes packets
- **Rx/Tx 1519 up**: Receive/transmit packets larger than 1518 bytes
- **Rx/Tx 2048 to 4095**: Receive/transmit 2048 bytes to 4095 bytes packets
- **Rx/Tx 4096 to 9216**: Receive/transmit 4096 bytes to 9216 bytes packets
- **Rx/Tx 9217 up**: Receive/transmit packets greater than 9216 bytes
- **Rx/Tx Broadcast**: Receive/transmit broadcast packets
- **Rx/Tx Bytes**: Receive/transmit bytes counter
- **Rx Collisions**: Receive collision packets
- **Rx CRC Align**: Receive CRC error packets
- **Rx/Tx Drop Percent**: Percentage of dropped packets out of total packets that should have been received/transmitted. **Note:** These statistics are only supported on the PFS 5000/7000 series.
- **Rx/Tx Error Percent**: Percentage of error packets out of total packets that should have been received/transmitted. **Note:** These statistics are only supported on the PFS 5000/7000 series.
- **Rx Fragments**: Receive fragment packets
- **Rx Jabbers**: Receive jabber packets
- **Rx/Tx Multicast**: Receive/transmit multicast packets
- **Rx Jumbo**: Receive jumbo packets
- **Rx Oversize**: Receive oversize packets
- **Rx Undersize**: Receive undersize packets
- **Rx/Tx Peak Time**: Receive/transmit maximum utilization time
- **Rx/Tx Pkt/Sec (PPS)**: Receive/transmit Packets Per Second (PPS). **Note:** These statistics are only supported on the PFS 5000/7000 series.
- **Rx/Tx Max Throughput**: Receive/transmit maximum throughput in Mbps



- **Rx/Tx Unicast:** Receive/transmit unicast packets
- **Rx/Tx Max Utilization:** Receive/transmit maximum utilization percentage

## Deduplication Statistics

On systems with one or more line cards that support deduplication, the following example shows deduplication statistics for a specific slot. To reset deduplication statistics, click **Reset Counters**, and then select either **This slot only** or **All Deduplication counters**.

Port ID	Input Packets	Duplicate Packets	Drop Packets	Forwarded Packets
10-1	0	0	0	0
10-2	0	0	0	0
10-3	0	0	0	0
10-4	0	0	0	0

The statistics for each port on the line card include:

- **Input packets:** Ingress packet count.
- **Duplicate packets:** Number of duplicate packets received subject to the specified time window.
- **Drop packets:** Number of erroneous packets received, whether they were duplicates or not.
- **Forwarded packets:** Number of packets forwarded over the egress interface.

## Flow Statistics

Flow statistics show the statistics for each filter, which defines a flow. It also shows this for each individual port or traffic map, as well as for each entire filter used across multiple ports or maps.

### Notes:

- **Available flow statistics vary depending on PFS product:**
  - **For PFS 6000 series, both *Statistics->Flow->Ports* and *Statistics->Flow->Maps* statistics are available.**
  - **For PFS 5000/7000 series, only *Statistics->Flow->Maps* is available.**
- **Due to a hardware limitation, pStack+ flow map statistics for PFS 704x devices are not incremented; they will display a 0 value.**

To reset flow statistics, click **Reset Counters**, and then select either **This slot only** or **All Flow counters**.



## View flow statistics by port or by map

1. Select the desired option, **Ports** or **Maps**, at the top of the page:

The screenshot shows the 'Statistics' screen with tabs for Network, Deduplication, Flow, and Control Packets. Below the tabs, there is a 'Flow Views:' section with two radio buttons: 'Ports' (selected) and 'Maps'. A red oval highlights the 'Ports' button.

2. When **Ports** is selected, to view by port, click a slot number, and then click the desired port. The flow statistics display.

The screenshot shows the 'Ports' view. At the top, there is a 'Flow Views:' section with 'Ports' selected (radio button highlighted). Below it is a table titled 'Ports View' with the following data:

Slot	Configured Card	Flow Reset Time
5	36S6Qstd	Thu Dec 7 21:26:14 2017
7	36S6Qstd	Thu Dec 7 21:26:15 2017

The screenshot shows the 'Flow Statistics' section. At the top, there is a 'Reset Counters' button and a status message: 'Statistics Reset Time: Thu Dec 7 21:26:14 2017' and 'Counters Reset Time'. Below this, there is information about the 'Configured Card' (36S6Qstd) and 'Configured Model'. The 'Flow Statistics' section displays the following table:

Port	Sub-Port
5	5-1
5	5-2



## Port 5-2

### ▲ Port To Filter Statistics

Filter Name	Packets
https	0
nonmatch	0
ssh	0

3. When **Maps** is selected, the flow statistics by map display. **Note:** The PPS statistic is only supported on the PFS 5000/7000 series.

Flow Views:  Ports  Maps

▲ Maps Maps View

Map Name	_packets	Tx Pkt/Sec (PPS)
map_SSL_forward~834	2781460927306	8225192
map_SSL_forward~833	0	0
map_SSL_forward~832	2856648743564	8447381
map_SSL_forward~831	2856649968842	8447205
map_SSL_forward~830	2856650856736	8447162

## Control Packets Statistics

Control packet statistics show information for [pfsMesh](#) and tunnel functionality (including [IP Tunnel Termination](#), [L2GRE Tunnel Origination/Termination Support](#), [VXLAN Tunnel Origination/Termination Support](#), and [pfsMesh Using pStack+](#)) on specific ports of a selected line card. To reset control packet statistics, click **Reset Counters**, and then select either **This slot only** or **All Control Packets counters**.

Slot 1

**Reset Counters** ▼ Statistics Reset Time Fri Jul 28 18:54:38 2017  
Counters Reset Time

Configured Card pre-configured  
Configured Model

▲ Control Packets Statistics

Port ID	Rx ARP Packets	Tx ARP Packets	Rx ICMP Packets	Tx ICMP Packets	Rx pfsMesh Packets	Tx pfsMesh Packets	Drop Packets
1-1	0	0	0	0	0	0	0
1-2	0	0	0	0	0	0	0



The statistics for each port on the line card include:

- **(Rx/Tx) ARP Packets:** Receive/transmit Address Resolution Protocol (ARP) packet count.
- **(Rx/Tx) ICMP Packets:** Receive/transmit Internet Control Message Protocol (ICMP) packet count.
- **(Rx/Tx) pfsMesh Packets:** Number of pfsMesh packets received/transmitted.
- **Drop Packets:** Dropped packets, either excessive or checksum failure packets.

## Tunnel Statistics

Tunnel statistics show information for GRE and VXLAN tunnel packet counts. To reset tunnel statistics, click **Reset Counters** on the GRE tunnel statistics page or the VXLAN statistics tunnel page. To reset pStack+ maps statistics, click **Reset Counters** on the VXLAN tunnel statistics page.

**Note:** Due to a hardware limitation, pStack+ tunnel statistics for PFS 704x devices are not incremented; they will display a 0 value.

**Statistics** Statistics

Network Deduplication Flow Control Packets Tunnel Port Group

Tunnel Views:  GRE  VxLAN

**Reset Counters** Statistics Reset Time Mon Sep 11 22:35:25 2023  
Counters Reset Time

GRE View

GRE Tunnel Name	Arp Req Sent	Arp Res Recv	Packet Tx	Packet Rx	Tx Pkt/Sec (PPS)	Rx Pkt/Sec (PPS)
gre_tunnel_1113	2	2	301468	301847	241	250
gre_tunnel_gateway_2222	2	2	302071	301846	257	250

Showing 1 to 2 of 2

**Statistics** Statistics

Network Deduplication Flow Control Packets Tunnel Port Group

Tunnel Views:  GRE  VxLAN

**Reset Counters** Statistics Reset Time Mon Sep 11 22:35:25 2023  
Counters Reset Time

VxLAN View

VxLAN Tunnel Name	Arp Req Sent	Arp Res Recv	Packet Tx	Packet Rx	Tx Pkt/Sec (PPS)	Rx Pkt/Sec (PPS)
vxlan_tunnel_1113	2	2	347674	7208410	282	250
vxlan_tunnel_gateway_2222	2	2	347412	347663	235	249

Showing 1 to 2 of 2



The statistics for GRE and VXLAN tunnels include:

- **(Rx/Tx) ARP Req Sent:** Receive/transmit Address Resolution Protocol (ARP) Requests count.
- **(Rx/Tx) ARP Res Recv:** Receive/transmit ARP Responses count.
- **(Rx/Tx) Packets:** Number of packets received/transmitted.
- **(Rx/Tx) Pkt/Sec (PPS):** Number of packets received/transmitted per second. **Note:** These statistics are only supported on the PFS 5000/7000 series.

## Port Group Statistics

Port Group statistics provide total bandwidth and Packets per Second (PPS) data for Network Port Groups, Load Balance Groups, and Monitor Port Groups. **Note:** These statistics are only supported on the PFS 5000/7000 series.

**Statistics** Statistics

Network Deduplication Flow Control Packets Tunnel Port Group

Port group Views:  Network  Monitor  Load Balance

▲ Network Network View

Pg Name	Rx Pkt/Sec (PPS)	Rx Bandwidth(Gbps)
NWPG_DFW	0	0.0

Showing 1 to 1 of 1

**Statistics** Statistics

Network Deduplication Flow Control Packets Tunnel Port Group

Port group Views:  Network  Monitor  Load Balance

▲ Monitor Monitor View

Pg Name	Tx Pkt/Sec (PPS)	Tx Bandwidth(Gbps)
inline_passive MPG	25328855	25.93
inline_replacement_passive MPG	0	0.0

Showing 1 to 2 of 2



Lbg Name	Tx Pkt/Sec (PPS)	Tx Bandwidth (Gbps)
inline_toochain_passive_LBG	8430690	8.63

Showing 1 to 1 of 1

The Port Group statistics include:

**Note:** These statistics are only supported on the PFS 5000/7000 series.

- **Network**
  - **Rx Pkt/Sec (PPS)**: The total number of packets received per second by the network port group.
  - **Rx Bandwidth (Gbps)**: Total Receive bandwidth (Gbps) for the network port group.
- **Monitor**
  - **Tx Pkt/Sec (PPS)**: The total number of packets transmitted per second by the monitor port group.
  - **Tx Bandwidth (Gbps)**: Total Transmit bandwidth (Gbps) for the monitor port group.
- **Load Balance**
  - **Tx Pkt/Sec (PPS)**: The total number of packets transmitted per second by the load balance group.
  - **Tx Bandwidth (Gbps)**: Total transmit bandwidth (Gbps) for the load balance group.

## Event Notifications

The Event Notifications page in the Status section displays information on Syslog notifications and alarms. Click the appropriate tab to select the desired display.

## Syslog History

This page displays up to the 200 most recent Syslog notifications. To view additional information about a single notification, click the number in the leftmost column.

**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.



### Event Notifications

Syslog History Alarms

Syslog History

ID	Facility	Severity	Timestamp	Message
200	system	notice	2017-12-13T15:11:40.260Z	SysAccCll. Logged out User public,IP:10.250.16.63,Context:snmp,AccessType:UDP
199	system	notice	2017-12-13T15:11:16.095Z	SysAccCll. Logged in User admin,IP:10.200.205.167,Context:webui,AccessType:HTTPS
198	system	notice	2017-12-13T15:11:00.244Z	SysAccCll. Logged in User public,IP:10.250.16.63,Context:snmp,AccessType:UDP
197	system	notice	2017-12-13T15:10:40.235Z	SysAccCll. Logged out User public,IP:10.250.16.63,Context:snmp,AccessType:UDP
196	system	notice	2017-12-13T15:10:00.000Z	SysAccCll. Logged in User public,IP:10.250.16.63,Context:snmp,AccessType:UDP

**199**

Facility	system	Severity	notice
Syslog Facility		Syslog Severity	
Timestamp	2017-12-13T15:12:40.239Z	Message	SysAccCll. Logged out User public,IP:10.250.16.63,Context:snmp,AccessType:UDP
			Syslog Message

## Alarms

PFOS maintains alarms for:

- Disk space usage
- The presence of core files
- Hardware elements including power supplies and fans
- Component temperatures

The actual list of hardware elements and components varies by platform.

The alarms page displays the alarm status of each alarm unit on the system. To acknowledge (or un-acknowledge) an alarm, click the checkbox of the alarm and then select Apply. PFOS records the time the alarm was raised as well as the time it was acknowledged. To view additional information about a single alarm unit, click the name in the leftmost column.

### Event Notifications

Syslog History Alarms

System Alarms

Unit	Unit Name	Fail Timestamp	Ack Timestamp	Status	Message	Acknowledge
core-file	Core file			ok		<input type="checkbox"/>
fan-01	Blower tray 1			ok		<input type="checkbox"/>
fan-02	Blower tray 2			ok		<input type="checkbox"/>
fan-03	Blower tray 3			critical		<input type="checkbox"/>

**fan-01** ×

Unit Name	Blower tray 1	Fail Timestamp	Default: Failed alarm event timestamp
Default:	System Alarms unit name	Ack Timestamp	Default: Acknowledge timestamp
Status	OK	Message	Default: System Alarms message
Default:	int		
System Alarms status			



## Hardware Information

The Hardware page displays detailed information about the capabilities of each port on the system, including port ID, configured port name, speed, acronyms for enabled applications, acronyms for disabled applications, a plain text description of each application, and the software version of each feature. When reporting issues to Technical Support, this information can be useful.

The information displayed on this page varies according to the type of hardware on which PFOS is running.

Click these tabs to display the following hardware information:

- **State:** State, module serial number, PCBA revision, SKU part number, module part number, module revision number, PCBA part number, PCBA serial number, chassis MAC address, PFS 5000/7000 total energy consumption (total estimated daily power usage in kWh based on sampling over the past 1 hour), and PFS 5000/7000 current power consumption (in Watts) of each PSU in the device.

Hardware					
		State			
	State	OK	Module Part Number	S5248F-ON	Chassis Part Number
		Default: init			
		Chassis state	Module Revision Number	N/A	Chassis Revision Number
Module Serial Number	FQ3RY03	PCBA Part Number	N/A	PCBA Part Number	
	Chassis Serial Number. Read only				
PCBA Revision	A02	PCBA Serial Number	TH0GM4RM CET00089007N	PCBA Serial Number	
	Chassis PCBA revision				
SKU Part Number	0GM4RM	Mac Address	1c:72:1d:9e:f4:f7	Chassis MAC Address	
	SKU Part Number				
Temperature (degrees-celsius)	28	Energy Consumption (KWh)	0.13	Chassis energy consumption (KWh) for an hour	
	Chassis temperature				
Power Consumption (W)	130.0				
	Chassis current power consumption (W)				

- **Slots:** State, SKU part number, module, module part number, module revision number, module serial number, PCBA serial number, PCBA revision number, PCBA part number, FPGA 1, temperature.



## Hardware

[State...](#) [Slots](#) [Fabric Module](#) [Management Module](#) [Fan Tray](#) [Power Supplies](#)

Line Cards

ID	State	SKU P/N	Model	Module P/N	Module Rev	Module S/N	PCBA P/N	PCBA Rev	PCBA S/N	FPGA 1	FPGA 2	FPGA 3	Temperature
1	empty												
2	empty												
3	empty												
4	empty												
5	OK	6000NBBGE100	6Q28std	VP_02171	01	17105420	VA_00823	0A	VMSNC-17105420	CF631011 rev 0017			35
6	empty												
7	empty												

- Fabric Module:** State, SKU part number, module part number, module revision number, module serial number, PCBA part number, PCBA revision number, PCBA serial number, Fan 1 speed, Fan 2 speed, Fan 3 speed, temperature.

## Hardware

[State...](#) [Slots](#) [Fabric Module](#) [Management Module](#) [Fan Tray](#) [Power Supplies](#)

Switch Fabric Cards

ID	State	SKU P/N	Module P/N	Module Rev	Module S/N	PCBA P/N	PCBA Rev	PCBA S/N	Fan 1 Speed	Fan 2 Speed	Fan 3 Speed	Temperature
1	OK	VA_00684	VP_01941	04	14071089	VA_00684	AF	VSSAL-14071089	15887	15665	15665	41
2	OK	VA_00684	VP_01941	04	14071094	VA_00684	AF	VSSAL-14071094		15887	16049	42
3	OK	VA_00684	VP_01941	XX	15077268	VA_00684	AF	VSSAL-14100828	15634	0	16049	43
4	empty											

Showing 1 to 4 of 4

- Management Module:** State, SKU part number, module part number, module revision number, module serial number, PCBA part number, PCBA revision number, PCBA serial number, Fan 1 speed, Fan 2 speed, Fan 3 speed, temperature.

## Hardware

[State...](#) [Slots](#) [Fabric Module](#) [Management Module](#) [Fan Tray](#) [Power Supplies](#)

CPU Cards

ID	State	SKU P/N	Module P/N	Module Rev	Module S/N	PCBA P/N	PCBA Rev	PCBA S/N	FPGA	Fan 1 Speed	Fan 2 Speed	Fan 3 Speed	Temperature
1	active	VP_02011	VP_01940	AE	VSVP1940-1620001	VA_00779	AA	VMSVSN-16050210	00007000 rev 0017	15511	16049	15450	31
2	standby	VP_00692	VP_01940	AD	1620010	VA_00779	08	VMSNC-16070736	00007000 rev 0018				

Showing 1 to 2 of 2



- **Fan Tray:** State, SKU part number, module part number, module revision number, module serial number, PCBA part number, PCBA revision number, PCBA serial number, blower speed, Fan 1 speed, Fan 2 speed.

Hardware											
<a href="#">State...</a> <a href="#">Slots</a> <a href="#">Fabric Module</a> <a href="#">Management Module</a> <a href="#">Fan Tray</a> <a href="#">Power Supplies</a>											
Fans											
ID	State	SKU P/N	Module P/N	Module Rev	Module S/N	PCBA P/N	PCBA Rev	PCBA S/N	Blower Speed	Fan 1 Speed	Fan 2 Speed
1	OK	VA_00723	VA_00723	AC	14100038	VA_00723	AF	VSSAL-14100065	2580	8438	8420
2	OK	VA_00723	VA_00723	AD	15083241	VA_00723	AF	VSSAL-14100060	2580	8474	8465

- **Power Supplies:** ID, state, model number, power type, fan direction, voltage, and power consumption.

Hardware						
<a href="#">State</a> <a href="#">Slots</a> <a href="#">Fabric Module</a> <a href="#">Management Module</a> <a href="#">Fan Tray</a> <a href="#">Power Supplies</a>						
Power Supplies						
ID	State	Model	Type	Fan Direction	Voltage In (V)	Power Consumption (W)
1	OK	CPR-4011-4M11	AC	Front-to-Back	117.5	65.0
2	OK	CPR-4011-4M11	AC	Front-to-Back	117.0	57.0

Click any slot or module ID to see more information about the individual blade. Installed applications can also be viewed per port on the System Status page and on the individual Ports Settings page.

Data on the Module Information page can be useful when contacting Technical Support to report problems.

## SNMP MIBs

PFOS currently has the following Management Information Bases (MIB) implemented, which include standard as well as product-specific (referred to in SNMP nomenclature as "enterprise extensions") MIBs. Each MIB is a conceptual database that allows visibility and control of PFOS features and settings. Most host SNMP management programs have a provision to read and process a file that defines the product-specific MIB database; these files are in a structured,



standard format called ASN.1 format (although these files commonly are referred to simply as "MIB files"). The MIB (ASN.1) files for PFOS are provided with the system. These MIB files can also be obtained by contacting NETSCOUT.

Refer to [SNMP MIB and Trap Definitions](#) for a full definition of the currently supported MIBs, which are:

- Interfaces MIB (RFCs 2863 and 3635); OID 1.3.6.1.6.3.1.1 for Traps, 1.3.6.1.2.1.2.2 for Base Stats, and 1.3.6.1.2.1.31.1 for High-speed Stats
- SNMPv2 MIB (RFC 3418); OID 1.3.6.1.6.3.1.1 for Traps, 1.3.6.1.2.1.2.2 for Stats
- Framework MIB (RFC 3411); OID 1.3.6.1.6.3.10
- Target MIB (RFC 3413); OID 1.3.6.1.6.3.12.1 for Stats
- Notification MIB (RFC 3413); OID 1.3.6.1.6.3.13.1 for Stats
- User-based Security Model MIB (RFC 3414); OID 1.3.6.1.6.3.15.1 for Stats
- View-based Access Control Model MIB (RFC 3415); OID 1.3.6.1.6.3.16.1 for Stats
- Community MIB (RFC 3584); OID 1.3.6.1.6.3.18.1 for Stats
- VSS Enterprise MIB: OID 1.3.6.1.4.1.21671.3 for Traps
- RMON MIB (RFC 2819): OID 1.3.6.1.2.1.16 for Stats
- High Capacity RMON MIB (RFC 3273); OID 1.3.6.1.2.1.16 for Stats

The standard MIBs are not viewable in the Web UI, but they are viewable using an SNMP client application (such as Network Management Map or GreatNMS) to receive and display these statistics.

PFOS supports SNMP versions 1, 2c, and 3.

## SNMP Configuration Support

By default, SNMP is disabled on PFOS. You must enable SNMP to perform any SNMP operations or receive any SNMP traps.

Commands are available in the Web UI and CLI to configure an SNMP agent, system, v1, v2c, and USM (v3), community, user, and trap receiving hosts. For details, refer to [SNMP in Configuring Notifications](#).

The following MIBs are read-only. You can view, but cannot change, the configuration of these MIBs from any MIB manager:

- SNMP-USER-BASED-SM-MIB
- SNMP-VIEW-BASED-ACM-MIB
- SNMP-COMMUNITY-MIB
- SNMP-TARGET-MIB
- SNMP-NOTIFICATION-MIB

To configure these MIBs, see refer to [SNMP in Configuring Notifications](#).

In SNMP version 3, MD5 and SHA authentication, DES and AES privacy protocols are supported. Diffie-Hellman exchange is not supported.



## nGeniusONE PFS Monitoring

nGeniusONE provides PFS monitoring modules for PFS 5000/7000 and PFS 6000 devices. These modules provide end-to-end packet acquisition assurance from tapping points to packet ingestion devices connected via PFS 5000/7000 and PFS 6000 devices. The PFS monitor is tightly integrated with and provides volumetric and vital stats for all PFS ports. These stats can be used for packet loss and oversubscription triage. You must configure the [nGeniusONE Configuration Manager \(nCM\)](#) server to which PFS will send data.

**Note:** PFS Monitor requires the following PFOS ports be open to communicate with PFOS:

- Port 8443 (HTTPS) - Port on which nGeniusONE retrieves files from the PFOS web server
- Port 395 (UDP) - Port from which PFOS sends traps to inform nGeniusONE/nCM it can retrieve stats. nGeniusONE/nCM will acknowledge the trap.

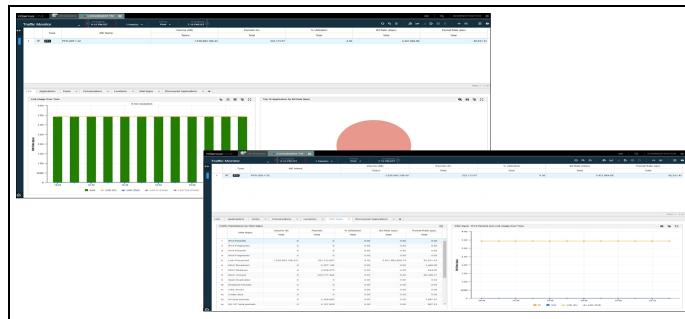
nGeniusONE PFS Monitoring modules include:

- [Consolidated Traffic Monitor](#)
- [Grid](#)
- [PFS Monitor](#)

For details about these modules, refer to the nGeniusONE online help.

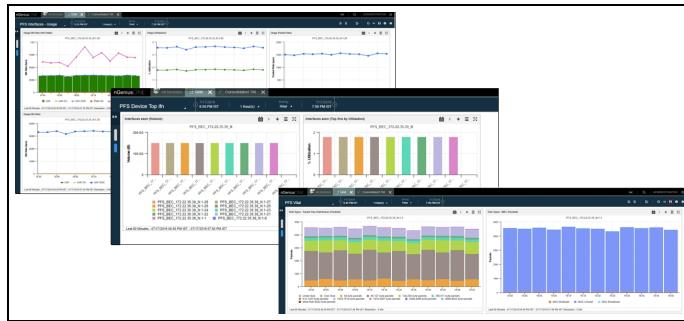
### Consolidated Traffic Monitor

The nGeniusONE Consolidated Traffic Monitor enables you to view PFS Link Usage over Time and Packet statistics such as total volume, % Utilization, Bit Rate and Packet Rate.



### Grid

The nGeniusONE Grid enables you to view PFS interface usage statistics and provides a Vital Signs template you can use to view charts of PFS packet statistics.



## PFS Monitor

The nGeniusONE PFS Monitor enables you to view packet statistics across ports and over time.



## Syslog Messages

Syslog is an industry-standard method for event reporting. If one or more Syslog (IPv4 and/or IPv6) servers are configured, the Syslog messages described in the following tables are sent to a Syslog server.

### User

Category	Sub-category Event	Event	Severity	Enum	Current Syslog String Displayed
Authentication:	access:	LOGIN	NOTICE	0	SysAccCtl. Logged in User:\$user,IP:\$IP, Context:webui,AccessType:HTTP
		LOGIN_FAILED	WARNING	1	SysAccCtl. Login failed User:\$user,IP:\$IP, Context:webui,AccessType:HTTP,reason:noauth



<b>Category</b>	<b>Sub-category Event</b>	<b>Event</b>	<b>Severity</b>	<b>Enum</b>	<b>Current Syslog String Displayed</b>
		LOGOUT	NOTICE	2	SysAccCtl. Logged out User:\$user,IP:\$IP, Context:webui,AccessType:HTTP
		LICENSE AGREEMENT ACCEPTED	NOTICE	3	SysAccCtl. License agreement accepted User:\$user IP:\$IP,context:\$context

## Configuration

<b>Category</b>	<b>Sub-category Event</b>	<b>Event</b>	<b>Severity</b>	<b>Enum</b>	<b>Current Syslog String Displayed</b>
Port:	basic:	PORT_NAME_CHANGED	NOTICE	4	PortCfgChg. (\$slot-\$port) Name Chgd from \$name to \$name by \$user
		PORT_CLASS_CHANGED	NOTICE	5	PortCfgChg. (\$slot-\$port) Class Chgd from \$class to \$class by \$user
		PORT_LINK_STATE_CHANGED	NOTICE	6	PortCfgChg. (\$slot-\$port) Link state Chgd from \$link to \$link by \$user
		PORT_SPEED_CHANGED	NOTICE	7	PortCfgChg. (\$slot-\$port) Speed Chgd from \$speed to \$speed by \$user
		PORT_STAMPING_CHANGED	NOTICE	8	PortCfgChg. (\$slot-\$port) Port stamping Chgd from \$state to \$state by \$user
		PORT_TIME_STAMPING_CHANGED	NOTICE	9	PortCfgChg. (\$slot-\$port) Time stamping Chgd from \$state to \$state by user \$user
		PORT_GEO_PROBE_TIME_FORMAT_CHANGED	NOTICE	10	PortCfgChg. (\$slot-\$port) geo probe time format Chgd from \$state to \$state by user \$user
		PORT_VN_TAG_STRIPPING_CHANGED	NOTICE	11	PortCfgChg. (\$slot-\$port) Vntag stripping Chgd from \$state to \$state by \$user
		PORT_DEDUP_SETTING_CHANGED	NOTICE	12	PortCfgChg. (\$slot-\$port) extended load balance Chgd from \$state to \$state by user \$user



Category	Sub-category Event	Event	Severity	Enum	Current Syslog String Displayed
		PORT_EXTENDED_LB_CHANGED	NOTICE	13	PortCfgChg. (\$slot-\$port) Dedup setting Chgd from \$state to \$state by user \$user
		PORT_PROTOCOL_STIPPING_CHANGED	NOTICE	14	PortCfgChg. (\$slot-\$port) protocol stripping setting Chgd from \$state to \$state by user \$user
		PORT_VLAN_TAG_STIPPING_CHANGED	NOTICE	15	PortCfgChg. (\$slot-\$port) VLAN tag stripping Chgd from \$state to \$state by user \$user
		PORT_SLICING_CHANGED	NOTICE	16	PortCfgChg. (\$slot-\$port) slicing Chgd from \$state to \$state by user \$user
		APP_MASKDEF_LIB_ADDED	NOTICE	17	AppCfgChg. Maskdef lib \$name is added by user \$user
		PORT_TUNNEL_CHANGED	WARNING	18	PortCfgChg. Appending Port: \$slot-\$port in tunnel termination Group: tt1 by \$user
System:	access-ctl:	SYS_ACC_CTL_ROLE_CHANGED	NOTICE	19	SysCfgChg. Acc Ctl role \$role is added/deleted/modified: rule \$rule added[access: \$access, context:\$context, feature:\$feature] by \$user
		SYS_ACC_CTL_USER_CHANGED	NOTICE	20	SysCfgChg. Acc Ctl user \$user is added/deleted/modified: password Set, role:\$role by \$user
		SYS_ACC_CTL_AUTH_ORDER_CHANGED	NOTICE	21	SysCfgChg. Acc Ctl authentication order Chgd to \$order_new by \$user
		SYS_ACC_CTL_RADIUS_CHANGED	NOTICE	22	SysCfgChg. Acc Ctl RADIUS server \$host is added/deleted/modified: [port:\$port, timeout:\$timeout, retransmit:\$retransmit key Set] by \$user



Category	Sub-category Event	Event	Severity	Enum	Current Syslog String Displayed
		SYS_ACC_CTL_TACACS_CHANGED	NOTICE	23	SysCfgChg. Acc Ctrl TACACS server \$host is added/deleted/modified: [port:\$port, timeout:\$timeout, retransmit:\$retransmit key Set] by \$user
	info:	SYS_INFO_NAME_CHANGED	NOTICE	24	SysCfgChg. Name Chgd from \$value1 to \$value2 by \$user.
		SYS_INFO_CONTACT_CHANGED	NOTICE	25	SysCfgChg. Contact Chgd from \$value1 to \$value2 by \$user.
		SYS_INFO_LOCATION_CHANGED	NOTICE	26	SysCfgChg. Location Chgd from \$value1 to \$value2 by \$user.
	features:	SYS_FIPS_MODE_FEATURE_CHANGED	NOTICE	28	SysCfgChg. FIPS mode setting Chgd from '\$state' to '\$state' by \$user
		SYS_ACC_MGMT_SSH_CLI_CHANGED	NOTICE	29	SysCfgChg. CLI with SSH access is \$enabled/disabled at port \$port by \$user
		SYS_ACC_MGMT_HTTP_WEBUI_CHANGED	NOTICE	31	SysCfgChg. web UI with HTTP access is \$enabled/disabled at port \$port by \$user
		SYS_ACC_MGMT_HTTP_NETCONF_CHANGED	NOTICE	32	SysCfgChg. NETCONF with HTTP access is \$enabled/disabled at port \$port by \$user
		SYS_ACC_MGMT_HTTPS_WEBUI_CHANGED	NOTICE	33	SysCfgChg. web UI with HTTPS access is \$enabled/disabled at port \$port by \$user
		SYS_ACC_MGMT_HTTPS_NETCONF_CHANGED	NOTICE	34	SysCfgChg. NETCONF with HTTPS access is \$enabled/disabled at port \$port by \$user
		SYS_ACC_MGMT_FRONT_PANEL_CHANGED	NOTICE	35	SysCfgChg. Front Panel enabled/disabled by \$user.



Category	Sub-category Event	Event	Severity	Enum	Current Syslog String Displayed
	network:	SYS_NETWORK_CHANGED	NOTICE	36	SysCfgChg. Network Settings Chgd from '\$value1' to '\$value2' by \$user.
	notifications:	SYS_SYSLOG_CHANGED	NOTICE	37	SysCfgChg. Syslog server settings Chgd from '\$state' to '\$state' by \$user.
		SYS_TRACE_LOG_CHANGED	NOTICE	38	SysCfgChg. Trace log settings of \$facility Chgd from \$state to \$state by \$user.
		SYS_LCD_CHANGED	NOTICE	39	SysCfgChg. LCD setting Chgd from '\$state' to '\$state' by \$user.
	timing-sources:	SYS_TIMING_SOURCE_TIME_CHANGED	NOTICE	40	SysCfgChg. Timing source Chgd from \$value to \$value by user \$user.
		SYS_TIMING_SOURCE_NTP_CHANGED	NOTICE	41	SysCfgChg. NTP servers Chgd from \$value to \$value by user \$user.
		SYS_TIMING_SOURCE_GPS_CHANGED	NOTICE	42	SysCfgChg. GPS cable length Chgd from \$value to \$value by user \$user.
		SYS_TIMING_SOURCE_PTP_CHANGED	NOTICE	43	SysCfgChg. PTP setting Chgd from \$value to \$value by user \$user.
	Source Port VLAN tagging:	SYS_MONITOR_PORT_VLAN_TAG_CHANGED	NOTICE	44	SysCfgChg. Monitor port VLAN tagging Chgd from '\$type' to '\$type' by \$user
Traffic:	map:	FLOWMAP_ADDED	NOTICE	45	TrfcfgChg. Map \$map filter: \$filter input ports: \$slot-\$port output ports: \$slot-\$port is added by user \$user
		FLOWMAP_DELETED	NOTICE	46	TrfcfgChg. Map \$map is deleted by user \$user
		FLOWMAP_MODIFIED	NOTICE	47	TrfcfgChg. Map \$map is modified by user \$user
	lbg:	LBG_ADDED	NOTICE	48	TrfcfgChg. LBG \$lbg ports: \$slot-\$port failover action: \$failover_action type: \$type is added by user \$user



Category	Sub-category Event	Event	Severity	Enum	Current Syslog String Displayed
		LBG_DELETED	NOTICE	49	TrfCfgChg. LBG \$lbg is deleted by user \$user
		LBG_MODIFIED	NOTICE	50	TrfCfgChg. LBG \$lbg \$item from [\$original_setting] to [\$new_setting] is modified by user \$user
	filter:	FILTER_ADDED	NOTICE	51	TrfCfgChg. Filter \$filter expression: \$expression is added by user \$user
		FILTER_DELETED	NOTICE	52	TrfCfgChg. Filter \$filter is deleted by user \$user
		FILTER_MODIFIED	NOTICE	53	TrfCfgChg. Filter \$filter expression from \$original_expression to \$new_expression is modified by user \$user
	lb-criteria:	LB_CRITERIA_ADDED	NOTICE	54	TrfCfgChg. LB criteria \$criteria is added by user \$user.
		LB_CRITERIA_DELETED	NOTICE	55	TrfCfgChg. LB criteria \$criteria is deleted by user \$user
		LB_CRITERIA_MODIFIED	NOTICE	56	TrfCfgChg. LB criteria \$criteria is modified by user \$user.
applications:	dedup:	APP_DEDUP_LIB_ADDED	NOTICE	57	AppCfgChg. Deduplication lib \$lib is added by user \$user.
		APP_DEDUP_LIB_DELETED	NOTICE	58	AppCfgChg. Application dedup lib \$lib is deleted by user \$user.
		APP_DEDUP_LIB_MODIFIED	NOTICE	59	AppCfgChg. Application dedup lib \$lib modified by user \$user.
	protocol-stripping:	APP_PROTOCOL_STRIPPING_ADDED	NOTICE	60	AppCfgChg. Application protocol stripping \$lib is added by user \$user.
		APP_PROTOCOL_STRIPPING_DELETED	NOTICE	61	AppCfgChg. Application protocol stripping \$lib is deleted by user \$user.
		APP_PROTOCOL_STRIPPING_MODIFIED	NOTICE	62	AppCfgChg. Application protocol stripping \$lib modified by user \$user.



Category	Sub-category Event	Event	Severity	Enum	Current Syslog String Displayed
	protocol:	APP_PROTOCOL_ADDED	NOTICE	63	AppCfgChg. Application protocol \$protocol is added by user \$user.
		APP_PROTOCOL_DELETED	NOTICE	64	AppCfgChg. Application protocol \$protocol is deleted by user \$user.
		APP_PROTOCOL_MODIFIED	NOTICE	65	AppCfgChg. Application protocol \$protocol modified by user \$user.
	mpls-l3:	APP_MPLS-L3_ADDED	NOTICE	66	AppCfgChg. Application mpls-l3 \$mpls-l3 is added by user \$user.
		APP_MPLS-L3_DELETED	NOTICE	67	AppCfgChg. Application mpls-l3 \$mpls-l3 is deleted by user \$user.
		APP_MPLS-L3_MODIFIED	NOTICE	68	AppCfgChg. Application mpls-l3 \$mpls-l3 modified by user \$user.
	extended lb:	APP_EXTENDED_LB_ADDED	NOTICE	69	AppCfgChg. Application extended lb \$lib is added by user \$user.
		APP_EXTENDED_LB_DELETED	NOTICE	70	AppCfgChg. Application extended lb \$lib is deleted by user \$user.
		APP_EXTENDED_LB_MODIFIED	NOTICE	71	AppCfgChg. Application extended lb \$lib is modified by user \$user.
	ELB protocol:	APP_ELB_PROTOCOL_ADDED	NOTICE	72	AppCfgChg. Application elb protocol \$protocol is added by user \$user.
		APP_ELB_PROTOCOL_DELETED	NOTICE	73	AppCfgChg. Application elb protocol \$protocol is deleted by user \$user.
		APP_ELB_PROTOCOL_MODIFIED	NOTICE	74	AppCfgChg. Application elb protocol \$protocol modified by user \$user
	VLAN-tag:	APP_VLAN_TAG_STRIP_LIB_ADDED	NOTICE	75	AppCfgChg. Application vlan tag strip lib \$lib is added by user \$user.
		APP_VLAN_TAG_STRIP_LIB_DELETED	NOTICE	76	AppCfgChg. Application vlan tag strip lib \$lib is deleted by user \$user.



<b>Category</b>	<b>Sub-category Event</b>	<b>Event</b>	<b>Severity</b>	<b>Enum</b>	<b>Current Syslog String Displayed</b>
		APP_VLAN_TAG_STRIP_LIB_MODIFIED	NOTICE	77	AppCfgChg. Application vlan tag strip lib \$lib modified by user \$user
	port-filter:	APP_PORT_FILTER_ADDED	NOTICE	78	AppCfgChg. Advanced-filter \$filter is added by user \$user.
		APP_PORT_FILTER_DELETED	NOTICE	79	AppCfgChg. Advanced-filter \$filter is deleted by user \$user.
		APP_PORT_FILTER_MODIFIED	NOTICE	80	AppCfgChg. Advanced-filter \$filter modified by user \$user.
	offset:	APP_OFFSET_LIB_ADDED	NOTICE	81	AppCfgChg. Offset lib \$lib is added by user \$user.
		APP_OFFSET_LIB_DELETED	NOTICE	82	AppCfgChg. Offset lib \$lib is deleted by user \$user.
		APP_OFFSET_LIB_MODIFIED	NOTICE	83	AppCfgChg. Offset lib \$lib modified by user \$user.
	tunnel termination:	APP_TUNNEL_TERMINATION_ADDED	NOTICE	84	AppCfgChg. Application tunnel termination \$lib is added by user \$user.
		APP_TUNNEL_TERMINATION_DELETED	NOTICE	85	AppCfgChg. Application tunnel termination \$lib is deleted by user \$user.
		APP_TUNNEL_TERMINATION_MODIFIED	NOTICE	86	AppCfgChg. Application tunnel termination \$lib is modified by user \$user.
Notifications	Events:	NOTIF_CONFIG_CHANGED	NOTICE	87	SysCfgChg. Notification settings for '\$description' chgd from '\$type' to '\$type' by \$user
	SNMP:	SNMP_CONFIG_CHANGED	NOTICE	88	SnmpCfgChg. Snmp \$description changed from \$old_change to \$new_change by \$user

## Chassis

<b>Category</b>	<b>Sub-category Event</b>	<b>Event</b>	<b>Severity</b>	<b>Enum</b>	<b>Current Syslog String Displayed</b>
Fru:	Line Card:	CARD_LC_INSERT	NOTICE	89	SysHS. Line card inserted in slot \$slot.



Category	Sub-category Event	Event	Severity	Enum	Current Syslog String Displayed
		CARD_LC_REMOVE	NOTICE	90	SysHS. Line card removed from slot \$slot.
		CARD_LC_RESET	INFORMATION	91	SysHS. Linecard \$slot has been reset. (not work when resetting from shutdown state)
		CARD_LC_SHUTDOWN	NOTICE	92	SysHS. Line card shutdown for slot \$slot
		CARD_LC_UPGRADE	NOTICE	93	SysHS, Line card firmware \$upgrade_action for slot \$slot
		CARD_LC_FAILURE	CRITICAL	94	SysHS. Line card \$slot went to a failed state
Fabric Card:	CARD_FC_INSERT	NOTICE	95		SysHS. fabric card inserted in slot \$slot.
		CARD_FC_REMOVE	NOTICE	96	SysHS. Fabric card removed from slot \$slot.
		CARD_FC_SHUTDOWN	NOTICE	97	SysHS. Fabric card shutdown for slot \$slot
		CARD_FC_FAILURE	ERROR	98	SysHS. Fabric card failure for slot \$slot
CPU Card:	CARD_CPU_INSERT	NOTICE	99		SysHS. CPU card A inserted
		CARD_CPU_REMOVE	NOTICE	100	SysHS. CPU card A removed
		CARD_CPU_UPGRADE	NOTICE	101	SysHS. CPU card firmware is upgrading
		CARD_CPU_FAILURE	ERROR	102	SysHS. CPU card A failed
Fan tray:	CARD_FAN_INSERT	NOTICE	103		SysHS. Fan Tray inserted in slot \$slot
		CARD_FAN_REMOVE	NOTICE	104	SysHS. Fan Tray removed from slot \$slot
		CARD_FAN_SPEED_READ_ERROR	ERROR	105	SysHS. Fan speed read error in tray \$tray fan:\$fan_idx_list
		CARD_FAN_ABSENT	ERROR	106	SysHS. \$device \$slot - fans are missing
Power supply:	CARD_PWR_SUPPLY_INSERT	NOTICE	107		SysHS. Power Supply Unit inserted in slot \$slot
		CARD_PWR_SUPPLY_REMOVE	NOTICE	108	SysHS. Power Supply Unit removed from slot \$slot
		CARD_PWR_SUPPLY_ERROR	ERROR	109	SysHS. Power supply \$slot is \$status



Category	Sub-category Event	Event	Severity	Enum	Current Syslog String Displayed
Mgmt:	restart:	PROCESS_RESTART	CRITICAL	110	Sys. Process \$process restarted.
		WARMSTART	NOTICE	130	Sys. Warmstart.
		REBOOT	NOTICE	111	Sys. Reboot with option:reboot is issued by \$user
		FACTORY_RESET	NOTICE	112	Sys. Reboot with option:factory reset is issued by \$user
		CLEAR_CONFIG	NOTICE	113	Sys. Reboot with option:clear configuration is issued by \$user
	core-dump:	CORE_FILES_PRESENT	NOTICE	114	Sys. Core files present
		CORE_FILE_DELETED	NOTICE	116	Sys. Core dump file \$file deleted by user \$user
	disk-space:	DISK_USAGE_WARNING	WARNING	117	Sys. Disk usage is above the warning level. Current usage: \$sda_type \$percentage%
		DISK_USAGE_ALERT	ALERT	118	Sys. Disk usage is at a critical level. Current usage: \$sda_type \$percentage%
		DISK_USAGE_NORMAL	NOTICE	240	Sys. Disk usage is normal. Current usage: %s", diskUsage
	file-mgmt:	SOFTWARE_UPLOADED	NOTICE	119	Sys. VXOS software pkg \$pkg Uploaded by user \$user
		SOFTWARE_INSTALLED	NOTICE	120	Sys. VXOS software pkg \$pkg Installed by user \$user
		SOFTWARE_DELETED	NOTICE	121	Sys. VXOS software pkg \$pkg deleted by user \$user
		FIRMWARE_UPLOADED	NOTICE	122	Sys. VXOS firmware pkg \$pkg Uploaded by user \$user
		FIRMWARE_INSTALLED	NOTICE	123	Sys. VXOS firmware pkg \$pkg Installed by user \$user
		FIRMWARE_DELETED	NOTICE	124	Sys. VXOS firmware pkg \$pkg deleted by \$user
		CONFIGURATION_FILE_UPLOADED	NOTICE	125	Sys. VXOS Configuration file \$file Uploaded by user \$user
		CONFIGURATION_FILE_DELETED	NOTICE	127	Sys. VXOS Configuration file \$file deleted by user \$user



Category	Sub-category Event	Event	Severity	Enum	Current Syslog String Displayed
		STARTUP_CONFIG_DELETED	NOTICE	128	Sys. Startup-config is deleted by user \$user
	coldstart:	COLDSTART	NOTICE	129	Cold Start (power-up)
		CHASSIS_DEFAULT_MAC_ALERT	NOTICE	132	
Port:	in-out:	XCVR_INSERT	INFORMATION	135	SysPort. XCVR inserted into (\$slot-\$port)
		XCVR_REMOVE	INFORMATION	136	SysPort. XCVR removed from (\$slot-\$port)
		XCVR_MISMATCH	WARNING	137	SysPort. XCVR mismatched in ports \$slot-\$port
	link-state:	LINK_UP	WARNING	138	SysPort. Port \$slot-\$port is now online (link up)
		LINK_DOWN	ALERT	139	SysPort. Port \$slot-\$port is offline (link down)
		TEMPERATURE_HIGH	NOTICE	147	SysEnv. Temperature ALERT: High temperature threshold reached
		CARD_TEMPERATURE_HIGH	ERROR	157	SysEnv. Temperature out-of-range ALARM: Absolute High temperature reached. System threshold varies per model/chassis: <ul style="list-style-type: none"><li>• 49 degrees for PFS 5000/7000 1RU chassis</li><li>• 53 degrees for PFS 5000/7000 2RU chassis</li><li>• 80 degrees for PFS 6000 chassis</li></ul>

# A PFOS Packet Fields in Filter Expressions

The following table shows the packet field names that can be used in a filter expression.

Two types of filter expressions are used in PFOS:

- **Type 2:** Used in conditional slicing and masking filters on the PFS 6000 Series.
- **Type 3:** Used in forwarding filters.

The syntax for Type 2 and Type 3 filter expressions is the same, minus exceptions described in [Table 1.3](#).

For Type 3 filter expressions, the number of packet fields per filter and the number of values compared against each field per expression depend on the type and combination of filter elements and logical expressions. Refer to the [Filter Resource Limits](#) section for the maximum possible filter resources available for use.

**Table A.1 - Packet Fields in Filter Expressions**

Packet field	Alternate forms	Comparison value
mac source	mac source address ethernet source address source {mac ethernet} address [bidi bidirection] (mac source address)	48-bit Ethernet address, entered as 12 hexadecimal digits, with optional embedded space, -, or : characters for readability, such as 00dd00 112233. The <code>bidi bidirection</code> keyword configures the address as either source or destination for bidirectional traffic. See <a href="#">bidi examples</a> . MAC filters can include a mask; matching is performed only on the bits of the address specified by the mask. For example: <code>mac source 01:00:5e:00:00:00 mask ff:ff:ff:00:00:00</code>
mac destination	[mac ethernet] dest [ination] address dest[ination] [mac ethernet] address [bidi bidirection] (mac dest[ination] address)	Same as mac source.

**Table A.1 - Packet Fields in Filter Expressions (continued)**

Packet field	Alternate forms	Comparison value
etype	[mac ethernet] etype value	16-bit hexadecimal value (four hexadecimal digits) matching the EtherType for untagged packet or outer VLAN TPID for tagged packet. <b>Note:</b> Filtering on EType 0x8926 does not work if VN Tag stripping is selected on PFS 5000/7000. Please use <a href="#">Custom Offset Filters</a> instead.
tag	[mac ethernet] [outer inner] tag value	16-bit hexadecimal TPID value; allowable values are 8100, 9100, or 88a8. The outer keyword (the default if neither is specified) specifies that filtering is performed on the outermost VLAN tag. The inner keyword specifies that filtering is performed on the inner (second) VLAN tag. <b>Note:</b> To filter different EtherType or outer TPID values, use the etype packet field. To filter VLANs with TPIDs other than 8100, 9100, or 88a8 please use custom offset filters. The inner keyword is not supported in Type 2 (advanced) filters nor on the PFS 5000 and 7000 series.
vlan	[mac ethernet] {outer inner} vlanid value   range [mac ethernet] {outer inner} vid value	Decimal value in the range 0-4095. On PFS 5000 and 7000 series, VLANs can also be specified as a range such as "100-2000". The outer keyword (the default if neither is specified) specifies that filtering is performed on the outermost VLAN ID. The inner keyword specifies that filtering is performed on the inner (second) VLAN id. The inner keyword is not supported in Type 2 (advanced) filters nor on the PFS 5000 and 7000 series.
extvlan	[mac ethernet] extvlanvalue	Used to isolate traffic based on PFX-assigned VLAN; refer to <a href="#">PFS+PFX Inner Filtering and Inner Load Balancing</a> . Decimal value in the range 1-4095.
priority	[mac ethernet] [outer inner] pri value [mac ethernet] [outer] qos value	Decimal value in the range 0-7. The outer keyword (the default if neither is specified) specifies that filtering is performed on the outermost VLAN ID. The inner keyword specifies that filtering is performed on the inner (second) VLAN id. The inner keyword is not supported in Type 2 (advanced) filters nor on the PFS 5000 and 7000 series.

**Table A.1 - Packet Fields in Filter Expressions (continued)**

Packet field	Alternate forms	Comparison value
ip source	ip {source src} {address range} {source src} ip {address range} [bidi bidirection] ({source src} ip {address})	To specify an IPv4 address, enter the address using standard delimited decimal notation, such as 192.168.0.250. To specify an IPv6 address, enter the address as a 128-bit address using hexadecimal digits delimited by : after every two bytes. The <b>bidi bidirection</b> keyword configures the address as either source or destination for bidirectional traffic. See <a href="#">bidi examples</a> .  Type 3 (forwarding) <b>IPv4</b> filters can include: <ul style="list-style-type: none"><li>• A netmask or prefix length; matching is performed only on the bits of the address specified by the mask or prefix length. For example: <code>ip source 192.168.1.0 mask 255.255.255.0 or ip source 192.168.1.0/24</code></li><li>• A range of IPv4 addresses specified by entering a range such as <code>ip source 192.168.1.2-192.168.2.30</code> (supported on PFS 5000 and 7000 series only)</li></ul> Type 3 (forwarding) <b>IPv6</b> filters can include a netmask or prefix length; matching is performed only on the bits of the address specified by the mask or prefix length. For example: <code>ip source 2607:f8b0:4006:807:0000:0000:0000:0000 mask ffff:ffff:ffff:ffff:0000:0000:0000:0000 or ip source 2607:f8b0:4006:807/64</code>  Type 2 (advanced) filters on the PFS 6000 series can include a range of IPv4 addresses specified by entering a range such as <code>ip source 192.168.1.2-192.168.2.30</code> . Ranges of IPv6 addresses are not supported.
ip destination	ip dest[ination] {address range} dest[ination] ip {address range} [bidi bidirection] ({dest[ination]} ip {address})	Same as ip source.

**Table A.1 - Packet Fields in Filter Expressions (continued)**

<b>Packet field</b>	<b>Alternate forms</b>	<b>Comparison value</b>
ip flags	ip flags {ipv4df   ipv4notdf   ipv4mf   ipv4notmf}	Filter packets based on various combinations of IP Fragment flags: ipv4df - Don't Fragment bit is set ipv4notdf - Don't Fragment bit is not set ipv4mf - More Fragments bit is set ipv4notmf - More Fragments bit is not set
ip dscp	ip dscp value	Differentiated Services Code Point (DSCP) value; range support decimal value 0-63. Supported in both IPv4 and IPv6.
ip ecn	ip ecn value	Explicit Congestion Notification (ECN) value; range support decimal value 0-3. Supported in both IPv4 and IPv6.
ip tos	ip tos value	Type of Service (ToS) value; 8-bit value specified as two hexadecimal digits. Supported in both IPv4 and IPv6.
ip protocol	ip prot value	IP protocol value; decimal value 0-255.
ip flow	ip flow value	20-bit value specified as five hexadecimal digits, as per RFC3232.
14 source port	{14 tcp udp sctp} {src source} port {value range odd even} {source src} {14 tcp udp sctp} port {value range odd even} [bidi bidirection] ({source src} port)	For PFS 5000/7000 series, L4/TCP ports can be specified as a range such as "20-21". The "odd" and "even" keywords filter for any odd or even port value, respectively. The <code>bidi bidirection</code> keyword configures the port as either source or destination for bidirectional traffic. See <a href="#">bidi examples</a> .
14 destination port	{14 tcp udp sctp} dest [ination] port {value range odd even} dest[ination] {14 tcp udp sctp} port {value range odd even} [bidi bidirection] (dest[ination] port)	Same as 14 source port.

**Table A.1 - Packet Fields in Filter Expressions (continued)**

Packet field	Alternate forms	Comparison value
type	type tcpflag	<p>Filter packets based on various combinations of TCP flags. Valid values for tcpflag are:</p> <ul style="list-style-type: none"><li>TCPSyn - SYN bit is set</li><li>TCPNotSyn - SYN bit is not set</li><li>TCPFIN - FIN bit is set</li><li>TCPNotFin - FIN bit is not set</li><li>TCPRST - RST bit is set</li><li>TCPNotRst - RST bit is not set</li><li>TCPPSH - PSH bit is set</li><li>TCPNotPSH - PSH bit is not set</li><li>TCPACK - ACK bit is set</li><li>TCPNotACK - ACK bit is not set</li><li>TCPURG - URG bit is set</li><li>TCPNotURG - URG bit is not set</li><li>TCPCwr - CWR bit is set</li><li>TCPNotCwr - CWR bit is not set</li><li>TCPECN - ECN bit is set</li><li>TCPNotECN - ECN bit is not set</li></ul> <p>TCP flag filter fields are not supported in Type 2 (advanced) filters.</p> <p>The TCPCwr, TCPNotCwr, TCPECN, and TCPNotECN TCP flags are not supported on the PFS 5010/7010.</p>
offset	{mac ip tcp udp} offset <offset value> <hex comparison pattern> mask <hex mask value>	<p><b>Offset Filtering for Non-503x/703x Devices</b></p> <p>The comparison pattern is entered as a hexadecimal string (1-32 hex characters), an IPv4 decimal, or IPv6 hex address with each byte optionally separated by a hyphen, colon, or space (such as 01bcd8 or 01:bc:db or 192.168.0.1). The maximum pattern length is 16 bytes.</p> <p>The maximum allowed offset value is 63 for PFS 6000 Series and 127 for PFS 5000/7000 Series. Optional alternative for ip is 13, and for tcp and udp is 14, thus not implying limitation to IP only for Layer 3 or to TCP/UDP only for Layer 4.</p> <p>A mask is a qualifier for the data pattern entered in bits. This causes the specified value to be logically ANDed with the packet data. Valid values can be a hexadecimal string (1-32 hex characters), an IPv4 decimal netmask, or IPv6 hex netmask. The example 14 offset 28 192.168.11.0 mask 255.255.255.0 filters on any IP address within the entire network 192.168.11.x as the source IP address within a tunneled protocol where the source IP address started at 28 bytes from the start of L4 (TCP or UDP) header.</p> <p>Custom offset filter fields are not supported in Type 2 (advanced) filters.</p>

**Table A.1 - Packet Fields in Filter Expressions (continued)**

Packet field	Alternate forms	Comparison value
offset	{mac ip tcp udp} offset <offset value> <hex comparison pattern> mask <hex mask value>	<p><b>Offset Filtering for PFS 503x/703x Devices</b></p> <p>In addition to standard tokens [mac/ip/tcp/udp] used for UDF filters, PFS 503x/703x devices support the following tokens to qualify based on packet types:</p> <ul style="list-style-type: none"> <li>• L2withVlan</li> <li>• KnownNonIp</li> <li>• UnknownI3</li> <li>• IPv4</li> <li>• IPv6</li> <li>• MPLSheader</li> <li>• UnknownL4</li> <li>• GRE</li> <li>• GreErspan</li> </ul> <p>Refer to <a href="#">PFS 5041/7041-32D Filter Resource Limits</a> for details.</p>
inner ip source	inner ip <source src> ipv4-address [mask ipv4-mask]	<p><b>Inner Filtering Options for PFS 503x/703x and 504x/704x Devices</b></p> <p>To qualify on inner IP4 source address in standard delimited decimal notation. Mask field is optional and also needs to be given in standard delimited decimal notation.</p>
inner ip destination	inner ip dest[ination] ipv4-address [mask ipv4-mask]	<p><b>Inner Filtering Options for PFS 503x/703x and 504x/704x Devices</b></p> <p>To qualify on inner IP4 destination address in standard delimited decimal notation. Mask field is optional and also needs to be in standard delimited decimal notation.</p>
inner ip protocol	inner ip prot value	<p><b>Inner Filtering Options for PFS 503x/703x and 504x/704x Devices</b></p> <p>Decimal value 0-255.</p>
inner 14 source port	inner {14 tcp udp} {src source} port {value odd even} {source src} {14 tcp udp} port {value odd even}	<p><b>Inner Filtering Options for PFS 503x/703x and 504x/704x Devices</b></p> <p>Decimal value 1-65535. The “odd” and “even” keywords filter for any odd or even port value, respectively.</p>
inner 14 destination port	inner {14 tcp udp} dest[ination] port {value odd even} Dest[ination] {14 tcp udp} port {value odd even}	<p><b>Inner Filtering Options for PFS 503x/703x and 504x/704x Devices</b></p> <p>Decimal value 1-65535. The “odd” and “even” keywords filter for any odd or even port value, respectively.</p>
inner payload	inner payload offset <offset value> <hex comparison pattern> mask <hex mask value>	<p><b>Inner Filtering Options for PFS 503x/703x and 504x/704x Devices</b></p> <p>Used to qualify on inner payload on user specified offset location. The comparison pattern is entered as a hexadecimal string. Max offset value is 84 bytes.</p>

## B Configuring SNMP for PFOS

Simple Network Management Protocol (SNMP) is a protocol that allows large numbers of network devices to be remotely managed in a consistent way. The SNMP Agent in PFOS supports version v1, v2c and v3, to respond to the requests from SNMP applications. The notification function in PFOS can be enabled for various events, and configured to send out SNMP v1, v2c or v3 Traps to specific target IPs. In the PFOS default configuration, the SNMP agent and all event notifications are disabled.

Explaining the principles of SNMP use is beyond the scope of this guide. This guide assumes that you already understand basic SNMP terminology and have SNMP manager software available to interface to PFOS.

Refer to the following workflows for configuring SNMP:

- [Configuring SNMPv1 or SNMPv2c](#)
- [Configuring SNMPv3](#)
- [Configuring SNMP Notification \(Traps\)](#)

**Note:** If you are sending PFS traps to nGeniusONE you must configure the Read and Write Communities (v2c) and authentication and password (v3) to those configured in PFOS. Refer to the nGeniusONE online help for details.

### Configuring SNMPv1 or SNMPv2c

The following steps summarize the tasks you must perform to configure SNMPv1 or SNMPv2c. Each step links to a procedure with more detail. Refer to the **PFOS CLI Reference Guide** for CLI command details.

Steps	Web UI	CLI
<a href="#">1 Enable SNMP and Configure SNMP Versions</a>	<a href="#">Notifications&gt;SNMP&gt;Agent</a>	snmp agent agent-options
<a href="#">2 Create a New SNMP Community (Optional)</a>	<a href="#">Notifications&gt;SNMP&gt;Community</a>	snmp community community-options
<a href="#">3 Add Security Name to View-Based Access Control Model (Optional)</a>	<a href="#">Notifications&gt;SNMP&gt;VACM</a>	snmp vacm vacm-options
<a href="#">4 Grant Access Rights to the VACM Group</a>	<a href="#">Notifications&gt;SNMP&gt;VACM</a>	snmp vacm vacm-options
<a href="#">5 Limit SNMP Access Rights</a>	<a href="#">Notifications&gt;SNMP&gt;VACM</a>	snmp vacm vacm-options



## Enable SNMP and Configure SNMP Versions

Perform the following steps:

1. On the Notifications>SNMP>Agent page, click the **Enabled** checkbox to enable the SNMP Agent.
2. Click each version checkbox that you want to enable.
3. If necessary adjust the Max Message Size that the agent can send or receive (default is 50000).

The screenshot shows the 'Agent' tab selected in the top navigation bar. Under the 'Enabled' section, the checkbox is checked. Below it, the 'Default: Unchecked' and 'Enables/Disables the SNMP agent.' descriptions are visible. In the 'Versions' section, 'V 1' and 'V 2c' have checkboxes checked, while 'V 3' is unchecked. To the right, the 'Max Message Size' field is set to '50000', with a note that the default is 50000 and the valid range is 484–214748364. A tooltip at the bottom right indicates the maximum length of an SNMP message.

## Create a New SNMP Community (Optional)

The "SNMP Community string" is like a password that allows access to SNMP agents on PFOS switches. SNMP Community strings are used only in SNMPv1 and SNMPv2c.

Perform the following steps:

1. On the Notifications>SNMP>Community page, click the **Add** button.
2. Enter a name for the SNMP Community string (1 to 32 characters), and click **Add**.

In the example below, a new community string named "SNMPRead" has been created.

The screenshot shows the 'Community' tab selected in the top navigation bar. Below it, a table lists communities with two entries: 'SNMPRead' and 'public'. At the bottom right, a note says 'Showing 1 to 2 of 2'.

## Add Security Name to View-Based Access Control Model (Optional)

The View-Based Access Control Model (VACM) enables users to define access for an SNMP group. Each group is defined by a security name, a security model (and level), and a set of views that specifies which types of MIB data that access group can read or write.

PFOS provides a default "all-rights" VACM group with "public" and "remote" default security names with predefined security models.



This procedure shows how to add SNMPRead as a new security group name to the VACM group. You can also create another group and add SNMPRead for v2c under the new group.

Perform the following steps:

1. On the Notifications>SNMP>VACM page, click **all-rights** VACM group name.
2. On the all-rights page, in the Member section, click the **Add** button to add a new member.
3. As the security name, type the name of the community string you previously added (such as "SNMPRead") and click **Add**.
4. Click the **Group = all-rights** link in the upper left of the browser to return to the all-rights page.

The screenshot shows a table with three rows: 'SNMPRead', 'public', and 'remote'. Each row has three checkboxes under 'Security Model': 'v1' (checked), 'v2c' (checked), and 'usm' (unchecked).

Security Name	Security Model
SNMPRead	<input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input type="checkbox"/> usm
public	<input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input checked="" type="checkbox"/> usm
remote	<input type="checkbox"/> v1 <input type="checkbox"/> v2c <input checked="" type="checkbox"/> usm

5. Select **v1** and **v2c** checkboxes to apply these security models to the SNMPRead security name.

## Grant Access Rights to the VACM Group

For the **all-rights** VACM group, PFOS provides a default Access Security Model named "any" which defines a "no-auth-no-priv" (no authentication no privacy exchanged) security level for MIB object "Internet" on SNMP Read, Write and Notify. To add customized security models see [Add New Security Models](#).

The screenshot shows a table with one row for 'any'. The columns are: Security Model (any), Security Level (no-auth-no-priv), Read View (internet), Write View (internet), and Notify View (internet). There are icons for search, refresh, and download at the top right.

Security Model	Security Level	Read View	Write View	Notify View
any	no-auth-no-priv	internet	internet	internet

Showing 1 to 1 of 1



The MIB view “Internet” is also pre-defined as “OID=1.3.6.1 included”. You can also define other OIDs to limit Read, Write and Notify permissions; see [Limit SNMP Access Rights](#).

The screenshot shows the NETSCOUT interface with the path Home / SNMP / VACM / View = internet. On the left, there's a sidebar with links for Status, Configuration, and Ports Settings. The main area is titled 'internet x' and shows a table under 'Subtree'. The table has two columns: 'OID' and 'Type'. One row is listed with '1.3.6.1' in the 'OID' column and 'Included' selected in the 'Type' column. There are buttons for 'Add ...' and 'Delete' at the top of the table, and icons for 'New View...', 'Edit', 'Search', and 'Delete' on the right.

## Add New Security Models

Perform the following to add new security models and apply Access Security level options.

1. On the Notifications>SNMP>VACM page, click **all-rights** VACM group name.
2. In the **Access** section, click **Add**. The Add New Access page appears.

The screenshot shows a modal dialog titled 'Add new Access' with the subtitle 'Definition of access right for groups'. The dialog has a form with two dropdown menus: 'Sec Model \*' and 'Sec Level \*'. Below each dropdown is a brief description. At the bottom are 'Add' and 'Cancel' buttons.

3. Select a security model and security level from the drop-down menus and click **Add**. The following table describes each security level and supported security models.

Security Level	Applicable Security Models	Description
auth-no-priv	Any, v3	A connection that is secured with a passphrase and authentication but no encryption.
auth-priv	Any, v3	A connection that is secured with both authentication and encryption.
no-auth-no-priv	Any, v1, v2c, v3	A connection that uses a simple passphrase (known as a shared secret) to secure the communication.

4. Select Read, Write, and Notify MIB Views.



The screenshot shows the configuration interface for a v2c context named 'no-auth-no-priv'. It displays three sections: 'Read View', 'Write View', and 'Notify View', each with a 'MIB view' dropdown set to 'internet'. Below each section is a placeholder text: 'The name of the MIB view of the SNMP context a...'. The interface has a clean, modern design with a light gray background and white text.

5. Click **Apply** in the toolbar to save the changes.

## Verify SNMP Configuration

You can verify successful SNMP configuration by using the `snmpwalk` command; it is a function provided by the SNMP protocol to get metrics of a remote system.

The first example returns metrics for the specified OID for the `SNMPRead` community.

```
snmpwalk -v 2c -c SNMPRead 10.250.176.149 iso.3.6.1.2.1.2.2.1
```

```
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpwalk -v2c -c SNMPRead 10.250.176.149 iso.3.6.1.2.1.2.2.1
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.10 = INTEGER: 10
iso.3.6.1.2.1.2.2.1.1.11 = INTEGER: 11
iso.3.6.1.2.1.2.2.1.1.12 = INTEGER: 12
iso.3.6.1.2.1.2.2.1.1.13 = INTEGER: 13
iso.3.6.1.2.1.2.2.1.1.14 = INTEGER: 14
iso.3.6.1.2.1.2.2.1.1.15 = INTEGER: 15
iso.3.6.1.2.1.2.2.1.1.16 = INTEGER: 16
iso.3.6.1.2.1.2.2.1.1.17 = INTEGER: 17
```

The second example uses `snmpget` and `snmpset` commands for the specified OID for the default public community.

```
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpget -v2c -c public 10.250.176.149 iso.3.6.1.2.1.1.4.0
iso.3.6.1.2.1.1.4.0 = STRING: "tsupport@netscout.com"
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpset -v2c -c public 10.250.176.149 iso.3.6.1.2.1.1.4.0 s "My Company Support Team"
iso.3.6.1.2.1.1.4.0 = STRING: "My Company Support Team"
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpget -v2c -c public 10.250.176.149 iso.3.6.1.2.1.1.4.0
iso.3.6.1.2.1.1.4.0 = STRING: "My Company Support Team"
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpget -v2c -c public 10.250.176.149 iso.3.6.1.2.1.31.1.1.1.18.1
iso.3.6.1.2.1.31.1.1.1.18.1 = STRING: "Port#1-1"
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpset -v2c -c public 10.250.176.149 iso.3.6.1.2.1.31.1.1.1.18.1 s "#1-1 to nG1"
iso.3.6.1.2.1.31.1.1.1.18.1 = STRING: "#1-1 to nG1"
jchang@qa-auto-01:~$ snmpget -v2c -c public 10.250.176.149 iso.3.6.1.2.1.31.1.1.1.18.1
iso.3.6.1.2.1.31.1.1.1.18.1 = STRING: "#1-1 to nG1"
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$
```



## Limit SNMP Access Rights

As shown in [Grant Access Rights to the VACM Group](#), both “Read Value” and “Write Value” are set for “Internet” as OID=1.3.6.1; meaning the full permissions have been granted to SNMP GET and SET function.

The second example in [Verify SNMP Configuration](#) shows the default community “public” gives full MIB OIDs permission to both GET and SET operation.

In general, system administrators prefer to limit SNMP access to certain MIB OIDs only.

To limit SNMP Set permission, you can configure a different OID for “Write Value”. For example, you can create a new MIB View “SystemParams” for subtree OID=1.3.6.1.2.1.1 (SNMP MIB-2 System objects). You can then use SystemParams as the Write View for security model “any”. Perform the following steps to create a new MIB View.

1. Access the Notifications>SNMP>VACM page
2. In the MIB Views area, click the **Add** button and create a new MIB View called “SystemParams”.

The screenshot shows the VACM Groups configuration page. At the top, there are tabs for Agent, VACM, USM, Target, Community, Notify, and Traps. The VACM tab is selected. Below the tabs, there is a section titled "VACM Groups" containing a table with one row. The row has a "Name" field containing "all-rights". To the right of the table are "Add ..." and "Delete" buttons. Below this section is another titled "Definition of MIB views" containing a table with one row. The row has a "Name" field containing "internet". To the right of this table is a red box highlighting the "Add ..." button, followed by "Delete".

3. Define the subtree to include OID=1.3.6.1.2.1.1 (SNMP MIB-2 System objects). Refer to [SNMP MIB and Trap Definitions](#) for OID details.

The screenshot shows the SystemParams configuration page. At the top, there is a breadcrumb navigation: Home / SNMP / VACM / View ≡ SystemParams. The title is "SystemParams". On the left, there is a sidebar with links for Status, Configuration, and others. The main area is titled "Subtree" and contains a table with one row. The row has columns for "OID" (containing "1.3.6.1.2.1.1") and "Type" (with radio buttons for "included" and "excluded", where "included" is selected). There are also "Add ...", "Delete", and other action buttons. At the bottom right, it says "Showing 1 to 1 of 1".

4. Then use SystemParams as the Write View for Security Model “any”.



Access Definition of access right for groups				
Security Model	Security Level	Read View	Write View	Notify View
any	no-auth-no-priv	internet	SystemParams	internet
Showing 1 to 1 of 1				

## Verify SNMPSet by Using the New Access Configuration

The example below shows an error when a user is attempting an SNMPSet command for an OID for which write permissions have not been set. As shown in [Limit SNMP Access Rights](#), the SNMPSet (write) permission was limited to MIB-2 system objects only (1.3.6.1.2.1.1).

**Note:** You may also leave "Write View" as empty, then it'll give no permission to set any OID.

```
jchang@qa-auto-01:~$ snmpset -v2c -c public 10.250.176.149 iso.3.6.1.2.1.31.1.1.18.2 s "#1-2 to nG1"
Error in packet.
Reason: noAccess
Failed object: iso.3.6.1.2.1.31.1.1.18.2

jchang@qa-auto-01:~$ snmpget -v2c -c public 10.250.176.149 iso.3.6.1.2.1.1.4.0
iso.3.6.1.2.1.1.4.0 = STRING: "My Company Support Team"
jchang@qa-auto-01:~$ snmpset -v2c -c public 10.250.176.149 iso.3.6.1.2.1.1.4.0 s "PFS Support Team"
iso.3.6.1.2.1.1.4.0 = STRING: "PFS Support Team"
jchang@qa-auto-01:~$ snmpget -v2c -c public 10.250.176.149 iso.3.6.1.2.1.1.4.0
iso.3.6.1.2.1.1.4.0 = STRING: "PFS Support Team"
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$
```

## Configuring SNMPv3

The following steps summarize the tasks you must perform to configure SNMPv3. Each step links to a procedure with more detail. Refer to the [PFOS CLI Reference Guide](#) for CLI command details.

Steps	Web UI	CLI
<a href="#">1 Enable SNMP and Configure SNMP Versions</a>	<a href="#">Notifications&gt;SNMP&gt;Agent</a>	snmp agent agent-options
<a href="#">2 Create a User-Based Security Model (USM) with Authentication and Privacy</a>	<a href="#">Notifications&gt;SNMP&gt;USM</a>	snmp community community-options
<a href="#">3 Add the USM User to VACM Group</a>	<a href="#">Notifications&gt;SNMP&gt;VACM</a>	snmp vacm vacm-options
<a href="#">4 Request Authentication and Privacy Password for USM</a>	<a href="#">Notifications&gt;SNMP&gt;VACM</a>	snmp usm usm-options
<a href="#">5 Limit Access Rights for SNMPSet</a>	<a href="#">Notifications&gt;SNMP&gt;VACM</a>	snmp vacm vacm-options



## Create a User-Based Security Model (USM) with Authentication and Privacy

Example below configures "v3user" as a new USM with Authentication and Privacy settings.

Perform the following steps:

1. On the Notifications>SNMP>USM page, click the **Add** button.
2. Enter a name for the USM (1 to 32 characters), and click **Add**.

In the example below, a new USM named "v3user" has been created.

The screenshot shows a browser window with the NETSCOUT logo at the top left. The URL bar indicates the user is on the 'User' page under 'SNMP' > 'USM'. The main content area is titled 'v3user'. On the left, there's a sidebar with links for Status, System Status, Statistics, Event Notifications, and pfSense Mesh. The main form contains fields for Authentication (radio buttons for md5, sha, and none, with sha selected) and Privacy (radio buttons for aes, des, and none, with aes selected). There are also two password input fields. The entire interface has a light gray background with dark blue header and sidebar elements.

3. Configure Authentication and Privacy communication algorithms and passwords for "v3user".
4. Click **Apply** in the toolbar to save the changes.

## Add the USM User to VACM Group

The VACM enables users to define access for an SNMP group. Each group is defined by a security name, a security model (and level), and a set of views that specifies which types of MIB data that access group can read or write.

PFOS provides a default "all-rights" VACM group with "public" and "remote" default security names with predefined security models.

This procedure shows how to add "v3user" as a new security group name to the VACM group.

Perform the following steps:

1. On the Notifications>SNMP>VACM page, click **all-rights** VACM group name.
2. On the all-rights page, in the Member section, click the **Add** button to add a new member.
3. As the security name, type the name of the community string you previously added (such as "v3User") and click **Add**.
4. Click the **Group = all-rights** link in the upper left of the browser to return to the all-rights page.



**all-rights ×**

Member A member of this VACM group. According to VACM, every group must have ...

Add ... Delete

Security Name	Security Model
SNMPRead	<input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input type="checkbox"/> usm
public	<input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input checked="" type="checkbox"/> usm
remote	<input type="checkbox"/> v1 <input type="checkbox"/> v2c <input checked="" type="checkbox"/> usm
v3user	<input type="checkbox"/> v1 <input type="checkbox"/> v2c <input checked="" type="checkbox"/> usm

5. Select **usm** checkboxes to apply to the v3user security name.

### Verify Using New USM User “v3user” without Password

You can run the snmpwalk command without authentication or privacy password.

```
snmpwalk -v3 -u v3user -a sha -x aes -n "" -l noAuthNoPriv 10.250.176.149
iso
```

```
2000 history
jchang@qa-auto-01:~$ snmpwalk -v3 -u v3user -a sha -x aes -n "" -l noAuthNoPriv 10.250.176.149 iso
iso.3.6.1.2.1.1.1.0 = STRING: "PFSS5010 VXOS 5.5.0"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.21671
iso.3.6.1.2.1.1.3.0 = Timeticks: (17334806) 2 days, 0:09:08.06
iso.3.6.1.2.1.1.4.0 = STRING: "tsupport@netscout.com"
iso.3.6.1.2.1.1.5.0 = STRING: "CLOUD_SZE_GM_G01-26U_NPB1-5812_1"
iso.3.6.1.2.1.1.6.0 = STRING: "San Jose, CA USA"
iso.3.6.1.2.1.1.7.0 = INTEGER: 8
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.2.1.0 = INTEGER: 54
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
```

### Request Authentication and Privacy Password for USM

For most common use cases, USM user should request authentication and privacy passwords; therefore you should create different security models for v2c and usm (v3) access.

In the example below the default "any" security model has been deleted and two new security models have been created:

- “v2c” with “no-auth-no-priv” for SNMPv2c access
- “usm” with “auth-priv” for SNMPv3 access

Refer to [Add New Security Models](#) for details.



**Member** (Showing 1 to 4 of 4)

Security Name	Security Model
SNMPRead	<input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input type="checkbox"/> usm
public	<input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2c <input checked="" type="checkbox"/> usm
remote	<input type="checkbox"/> v1 <input type="checkbox"/> v2c <input checked="" type="checkbox"/> usm
v3user	<input type="checkbox"/> v1 <input type="checkbox"/> v2c <input checked="" type="checkbox"/> usm

**Access** (Showing 1 to 2 of 2)

Security Model	Security Level	Read View	Write View	Notify View
v2c	no-auth-no-priv	internet	internet	internet
usm	auth-priv	internet	internet	internet

## Verify Using New USM User "v3user" without Password

Now that authentication and privacy password are required for "v3user", running the snmpwalk command without a password results in an error.

```
snmpwalk -v3 -u v3user -a sha -x aes -n "" -l noAuthNoPriv
10.250.176.149 iso
```

```
^C
jchang@qa-auto-01:~$ snmpwalk -v3 -u v3user -a sha -x aes -n "" -l noAuthNoPriv 10.250.176.149 iso
Error in packet.
Reason: authorizationError (access denied to that object)
Failed object: ccitt.1

jchang@qa-auto-01:~$ snmpwalk -v2c -c SNMPRead 10.250.176.149 iso.3.6.1.2.1.2.2.1
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
iso.3.6.1.2.1.2.2.1.1.9 = INTEGER: 9
iso.3.6.1.2.1.2.2.1.1.10 = INTEGER: 10
iso.3.6.1.2.1.2.2.1.1.11 = INTEGER: 11
```

Running SNMPWalk command with authentication and privacy passwords now works for "v3user" (both authentication and privacy passwords were set to "12345678" (see [Create a User-Based Security Model \(USM\) with Authentication and Privacy](#))

```
snmpwalk -v3 -u v3user -a sha -A 12345678 -x aes -X 12345678 -n "" -l authPriv
10.250.176.149 iso
```

```
jchang@qa-auto-01:~$ snmpwalk -v3 -u v3user -a sha -A 12345678 -x aes -X 12345678 -n "" -l authPriv 10.250.176.149 iso
iso.3.6.1.2.1.1.1.0 = STRING: "PFSS5010 VXOS 5.5.0"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.21671
iso.3.6.1.2.1.1.3.0 = Timeticks: (17473389) 2 days, 0:32:13.89
iso.3.6.1.2.1.1.4.0 = STRING: "tsupport@netscout.com"
iso.3.6.1.2.1.1.5.0 = STRING: "CLOUD_SZE_GM_G01-26U_NPB1-5012_1"
iso.3.6.1.2.1.1.6.0 = STRING: "San Jose, CA USA"
iso.3.6.1.2.1.1.7.0 = INTEGER: 8
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.2.1.0 = INTEGER: 54
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
iso.3.6.1.2.1.2.2.1.1.4 = INTEGER: 4
iso.3.6.1.2.1.2.2.1.1.5 = INTEGER: 5
iso.3.6.1.2.1.2.2.1.1.6 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.1.7 = INTEGER: 7
iso.3.6.1.2.1.2.2.1.1.8 = INTEGER: 8
```



## Limit Access Rights for SNMPSet

The MIB view “Internet” is pre-defined as “OID=1.3.6.1 included”, meaning the full permissions have been granted to SNMP SET function.

OID	Type
1.3.6.1	<input checked="" type="radio"/> included <input type="radio"/> excluded

You can also limit v2c users without any permission for SNMPSet by leaving the Write View empty, and limit v3 users with only “MIB-2 system objects” permission on SNMPSet.

Security Model	Security Level	Read View	Write View	Notify View
v2c	no-auth-no-priv	internet		internet
usm	auth-priv	internet	SystemParams	Internet



To remove the Write View from v2c users, select **v2c** from the Access section of the all-rights page. Click the **x** to the right of the Write View field to delete it.

## Verify SNMPSet by Using the New Access Configuration

In the example below:

- Write View permission for v3 users is configured with SystemParams, including MIB-2 system objects only (so other parameters such as MIB (1.3.6.1.2.1.31) cannot be modified).
- Write View permission for v2c users is configured as empty (no write permission is set, only permission to read an OID).

```
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpget -v3 -u v3user -a sha -A 12345678 -x aes -X 12345678 -n "" -l authPriv 10.250.176.149 iso.3.6.1.2.1.1.4.0
iso.3.6.1.2.1.1.4.0 = STRING: "PFS Support Team"
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpset -v3 -u v3user -a sha -A 12345678 -x aes -X 12345678 -n "" -l authPriv 10.250.176.149 iso.3.6.1.2.1.1.4.0 s "NetScout Support Team"
iso.3.6.1.2.1.1.4.0 = STRING: "NetScout Support Team"
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpget -v3 -u v3user -a sha -A 12345678 -x aes -X 12345678 -n "" -l authPriv 10.250.176.149 iso.3.6.1.2.1.1.4.0
iso.3.6.1.2.1.1.4.0 = STRING: "NetScout Support Team"
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpset -v3 -u v3user -a sha -A 12345678 -x aes -X 12345678 -n "" -l authPriv 10.250.176.149 iso.3.6.1.2.1.1.18.1
iso.3.6.1.2.1.1.18.1 = STRING: "#1-l to nG1"
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpset -v3 -u v3user -a sha -A 12345678 -x aes -X 12345678 -n "" -l authPriv 10.250.176.149 iso.3.6.1.2.1.31.1.1.18.1 s "Port#1-l to n
Error in packet.
Reason: noAccess
Failed object: iso.3.6.1.2.1.31.1.1.1.18.1
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpget -v3 -u v3user -a sha -A 12345678 -x aes -X 12345678 -n "" -l authPriv 10.250.176.149 iso.3.6.1.2.1.1.4.0
iso.3.6.1.2.1.1.4.0 = STRING: "NetScout Support Team"
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpset -v2c -c SNMPRead 10.250.176.149 iso.3.6.1.2.1.1.4.0
iso.3.6.1.2.1.1.4.0 = STRING: "NetScout Support Team"
jchang@qa-auto-01:~$ jchang@qa-auto-01:~$ snmpset -v2c -c SNMPRead 10.250.176.149 iso.3.6.1.2.1.1.4.0 s "PFS Support Team"
Timeout: No Response from 10.250.176.149
jchang@qa-auto-01:~$
```

## Configuring SNMP Notification (Traps)

This section describes how to configure SNMP trap notifications.

The following steps summarize the tasks you must perform to configure SNMP Notifications, also known as Traps. Each step links to a procedure with more detail. Refer to the **PFOS CLI Reference Guide** for CLI command details.

Steps	Web UI	CLI
<a href="#"><b>1 SNMP Notify Tags</b></a>	<a href="#">Notifications&gt;SNMP&gt;Notify</a>	snmp notify notify-options
<a href="#"><b>2 Add Trap Receiver IP Address to Target Table</b></a>	<a href="#">Notifications&gt;SNMP&gt;Target</a>	snmp target target-options



Steps	Web UI	CLI
<b>3 Enable SNMP Traps</b>	<a href="#">Notifications&gt;SNMP&gt;Traps</a> or <a href="#">Notifications&gt;Events</a>	snmp-server or notification event

## SNMP Notify Tags

SNMP Notify Tags specify tag values to be used by the targets that will receive SNMP notifications. PFOS provides three default tags: std\_v1\_trap, std\_v2\_trap, std\_v3\_trap. You are not required to create new tags and can use the default tags.

Name	Tag	Type
std_v1_trap	std_v1_trap	trap
std_v2_trap	std_v2_trap	trap
std_v3_trap	std_v3_trap	trap

## Add Trap Receiver IP Address to Target Table

You can create a Trap Receiver at [Notifications>SNMP>Target](#).

Name	IP	UDP Port	Tag	Security Model
127.0.0.1 v2	127.0.0.1	6000	std_v2_trap	v2c
127.0.0.1 v3	127.0.0.1	7000	std_v3_trap	usm
Trap_Receiver	10.200.130.60	162	std_v3_trap, std_v2_trap, std_v1_trap	v2c



## SNMP v2c Receiver Example

The following page shows an SNMP v2c Receiver example.

The screenshot shows the 'Trap\_Receiver' configuration page. On the left is a navigation sidebar with various settings like Ports, Port Groups, Tool Chain, Trigger Policies, and SNMP. The main area has fields for 'IP' (ip-address) and 'UDP Port' (162). A 'Tag' section lists 'std\_v3\_trap', 'std\_v2\_trap', and 'std\_v1\_trap'. Below is a 'Security Models' section with radio buttons for v1, v2c (selected), and usm. For v2c, a dropdown 'Security Name' is set to 'SNMPRead public'.

- Enter the IP address of the SNMP notification recipient.
- SNMP Notify Tags for v2c trap receiver are included.
- Select a previously-defined community name.
- Remember that the specified UDP port must not be blocked by any firewall(s) between the PFS and the trap receiver.

## SNMP v3 Receiver Example

The following page shows an SNMP v3 Receiver example.

This screenshot shows the same 'Trap\_Receiver' configuration page as the previous one, but with different security settings. In the 'Security Models' section, the 'usm' radio button is selected. It requires a 'User Name' ('v3user') and a 'Security Level' ('Auth Priv', which is highlighted in blue).

- Enter the IP address of the SNMP notification recipient.
- SNMP Notify Tags for v3 trap receiver are included.
- Select a previously-defined USM user.



- Select Security Level "No Auth No Priv", "Auth No Priv" or "Auth Priv" for Authentication and Privacy algorithm
- Remember that the specified UDP port must not be blocked by any firewall(s) between the PFS and the trap receiver.

## Enable SNMP Traps

You can enable SNMP Traps from the following two pages in PFOS.

- Notifications>SNMP>Traps
- Notifications>Events

SNMP trap options are consistent for both of these pages; either page can be used to enable SNMP traps.

### Notifications>SNMP>Traps

Select the specific traps to enable or use the All option to enable all traps.

**SNMP Configuration of the User-based Security Model**

Agent VACM USM Community Target Notify Traps

Link up Down  Enable SNMP IF-MIB LinkUpDown trap

All  Enable SNMP all traps    None  Disable SNMP all traps

**System** Enable SNMP VSS-SYSTEM-MIB Traps

Temperature <input checked="" type="checkbox"/>	Config Change <input checked="" type="checkbox"/>	Access <input checked="" type="checkbox"/>
File Mgmt <input checked="" type="checkbox"/>	Restart <input checked="" type="checkbox"/>	Fru <input checked="" type="checkbox"/>
Health Stats <input checked="" type="checkbox"/>	pfsMesh <input checked="" type="checkbox"/>	High Availability <input checked="" type="checkbox"/>
Tunnel State <input checked="" type="checkbox"/>	Health Check State <input checked="" type="checkbox"/>	Trigger Policy <input checked="" type="checkbox"/>
Enhanced Link up Down <input checked="" type="checkbox"/>	Stripping <input checked="" type="checkbox"/>	Access SNMP <input checked="" type="checkbox"/>
Enhanced Link up Down <input checked="" type="checkbox"/> Enable SNMP system LinkUpDown trap		
<b>SNMP</b> Enable SNMP SNMPv2-MIB Traps		
Coldstart <input checked="" type="checkbox"/> Enable SNMP snmp coldstart trap		

**Note:** The **Link up Down** traps ([link Down](#) and [link Up Objects](#) in standard IF-MIB) and the **Enhanced Link up Down** traps ([vsLinkUpNotif](#) and [vsLinkDownNotif](#) in proprietary VSS-SYSTEM-MIB) are similar traps, but the Enhanced Link up Down 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.



## Notifications>Events

Select different categories of event notifications by enabling Syslog, SNMP, or NETCONF for each function.

The screenshot shows the NETSCOUT Event Notification event Settings page. On the left is a navigation sidebar with links like Status, Configuration, Libraries, Notifications, Global Settings, and System Administration. The main area has tabs for Config Notification, User Notification, and Chassis Notification. Under Config Notification, there's a section for Global Notification Type with checkboxes for All, None, Syslog, SNMP, and NETCONF. Below this are two expandable sections: Port (Port configuration events) and System (System configuration events). Each section contains a table with columns for Event and Notification Type, showing checkboxes for All, None, Syslog, SNMP, and NETCONF. In the Port section, events include powersafe, advanced, and basic. In the System section, events include access-ctl, info, and features. The Syslog and SNMP checkboxes are checked for most events.

Event	Notification Type
powersafe	<input type="checkbox"/> All <input type="checkbox"/> None <input checked="" type="checkbox"/> Syslog <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> NETCONF
advanced	<input type="checkbox"/> All <input type="checkbox"/> None <input checked="" type="checkbox"/> Syslog <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> NETCONF
basic	<input type="checkbox"/> All <input type="checkbox"/> None <input checked="" type="checkbox"/> Syslog <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> NETCONF

Event	Notification Type
access-ctl	<input type="checkbox"/> All <input type="checkbox"/> None <input checked="" type="checkbox"/> Syslog <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> NETCONF
info	<input type="checkbox"/> All <input type="checkbox"/> None <input checked="" type="checkbox"/> Syslog <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> NETCONF
features	<input type="checkbox"/> All <input type="checkbox"/> None <input checked="" type="checkbox"/> Syslog <input checked="" type="checkbox"/> SNMP <input type="checkbox"/> NETCONF



## Verify SNMP v2c Trap is Received by Third-Party SNMP Trap Receiver

The following graphic shows an example third-party SNMP trap receiver. Remember that the specified UDP port must not be blocked by any firewall(s) between the PFS and the trap receiver. Refer to [SNMP MIB and Trap Definitions](#) for OID details.

Description	Source	Time	Severity
linkUp	10.250.176.150	2020-02-25 15:37:45	
linkDown	10.250.176.150	2020-02-25 15:37:45	
linkUp	10.250.176.150	2020-02-25 15:37:45	

**Source:** 10.250.176.150      **Timestamp:** 6 minutes 15 seconds      **SNMP Version:** 2  
**Trap OID:** .iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTraps.linkUp      **Community:** public

**Variable Bindings:**

**Name:** .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0  
**Value:** [TimeTicks] 6 minutes 15 seconds (37578)

**Name:** snmpTrapOID  
**Value:** [OID] linkUp

**Name:** .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifIndex.47  
**Value:** [Integer] 47

**Name:** .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifAdminStatus.47  
**Value:** [Integer] up (1)

**Name:** .iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus.47  
**Value:** [Integer] up (1)

**Description:** A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.

# C SNMP MIB and Trap Definitions

This section provides information on SNMP traps and notifications, packet and port statistics, and MIBs.

This release of PFOS supports SNMP versions 1, 2c, and 3, all of which are enabled by default.

Refer to the following sections for details:

- [Traps/Notifications](#)
- [Packet/Port Statistics](#)
- [System Information](#)
- [NTCT-PFS-HEALTH-MIB](#)
- [VSS-SYSTEM-MIB](#)

## Traps/Notifications

### Interfaces MIB Traps

The following traps from the Interfaces MIB (RFC 2863) are supported.

Object	linkDown
OID	1.3.6.1.6.3.1.1.5.3
Status	Current
MIB	IF-MIB (RFC 2863)
Trap Components	ifIndex ifAdminStatus ifOperStatus
Description	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
ClearTrap	linkUp
Object	linkUp
OID	1.3.6.1.6.3.1.1.5.4
Status	Current
MIB	IF-MIB (RFC 2863)



Trap Components	ifIndex ifAdminStatus ifOperStatus
Description	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
ClearTrap	linkDown

## VSS Enterprise MIB Traps

The following traps from VSS-SYSTEM-MIB are supported.

Object	vsTempHighNotif
OID	.1.3.6.1.4.1.21671.3.1.0.2
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsTemperatureStatusDescr vsTemperatureStatusValue
Description	A vsTempHighNotif trap is generated by the managed system when the temperature of one of its entities has reached a high state as compared to the normal operating state.
Description String	"Temperature of Line Card# %d has reached a high state" "Temperature of Fabric Module# %d has reached a high state" "Temperature of Management Module# %d has reached a high state"
ClearTrap	vsTempNormalNotif

Object	vsCfgChangeNotif
OID	.1.3.6.1.4.1.21671.3.1.0.3
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsCfgChangeTime vsCfgChangeCommandSrc vsCfgChangeCommandUser vsCfgChangeCommandSrcAddrType vsCfgChangeCommandSrcAddr vsCfgChangeNode vsCfgChangeDescr
Description	A vsCfgChangeNotif is generated by the managed system when any configuration on the system has changed.
ClearTrap	N/A

Object	vsAuthenticationNotif
OID	.1.3.6.1.4.1.21671.3.1.0.4
Status	Current
MIB	VSS-SYSTEM-MIB



Trap Components	vsAuthenticationChangeTime vsAuthenticationCommandSrc vsAuthenticationType vsAuthenticationDescr
Description	A vsAuthenticationNotif is generated by the managed system when a user attempts to access the system.
Description String	vsAuthenticationChangeTime=07:E3:0A:1B:12:17:38:00:2B:00:00 vsAuthenticationCommandSrc=2(cli) vsAuthenticationType=LOGIN_SUCCESS/LOGOUT/LOGIN_FAILED/LOGIN_BLOCKED/ LICENSE AGREEMENT ACCEPTED/ EVENT_TYPE_LICENSE AGREEMENT DECLINED . vsAuthenticationDescr=User:admin,IP:10.200.130.51,AccessType:SSH/HTTPS/UDP
ClearTrap	Self
Object	vsRestartNotif
OID	.1.3.6.1.4.1.21671.3.1.0.5
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsRestartDescr
Description	A vsRestartNotif is generated by the managed system when the system or any process is going to restart.
Description String	"Reboot with option:factory reset is issued by \$user for \$cmd_mgmt" "Reboot with option:clear configuration is issued by \$user" "Reboot is issued by \$user for \$cmd_mgmt" "Reboot is issued by \$user. It will clear configuration due to software downgrade"
ClearTrap	N/A
Object	vsFRUInsertedNotif
OID	.1.3.6.1.4.1.21671.3.1.0.6
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsFRUInsertedDescr
Description	A vsFRUInsertedNotif is generated by the managed system whenever any FRU (Field Replaceable Unit) is inserted in the system.
Description String	"Line card inserted for slot %d" "Fabric card inserted in slot %d" "Mgmt card %d inserted" "Fan Tray inserted in slot %d" "Power Supply Unit inserted in slot %d" "Powersafe Device found vendor id %X product id %X Modules: "
ClearTrap	vsFRURemovedNotif
Object	vsFRURemovedNotif
OID	.1.3.6.1.4.1.21671.3.1.0.7
Status	Current
MIB	VSS-SYSTEM-MIB



Trap Components	vsFRURemovedDescr
Description	A vsFRURemovedNotif is generated by the managed system whenever any FRU (Field Replaceable Unit) is removed from the system.
Description String	"Line card removed from slot %d" "Fabric card removed from slot %d" "CPU card removed from slot %d" "Fan Tray removed from slot %d" "Power Supply Unit removed from slot %d"
ClearTrap	vsFRUIInsertedNotif
Object	vsFileMgmtNotif
OID	.1.3.6.1.4.1.21671.3.1.0.8
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsFileMgmtDescr
Description	A vsFileMgmtNotif is generated by the managed system when a software or firmware image or configuration file is uploaded, installed, or deleted on the system.
Description String	"\$imageType software pkg \$simpleName uploaded by user \$user on \$dest_mgmt" "pfsfm-ems software pkg \$imageName installed by user \$user on \$cmd_mgmt " "VXOS software pkg \$imageName installed by user \$user on \$cmd_mgmt "VXOS firmware pkg \$firmwareName installed in slots \$cards in positions \$positions by user \$user" "VXOS firmware pkg \$simpleName uploaded by user \$user on \$dest_mgmt" "VXOS Cfg file \$simpleName uploaded by user \$user "VXOS Cfg file \$simpleName2 uploaded by user \$user. WARNING: Platform of \${simpleName2} and current system is not same." "Core dump file \$srcFileName downloaded by user \$user" "SSH public key file \$simpleName uploaded by user \$user" "VXOS Cfg file \$cmd_mgmt:\$configName applied by user \$user" "Certificate File \$simpleName uploaded by user \$user "Warning: PFOS Support license will expire in %d days" PFOS license file \$simpleName uploaded by user \$user" "Warning: PFOS %s trial license has expired. %s" "Warning: PFOS %s trial license has expired." "Warning: PFOS %s trial license will expire in %d days." "Warning: PFOS Support license has expired." "Line card firmware upgraded for slot %d "Line card firmware upgrading for slot %d" "Line card firmware upgrade canceled for slot %d" "Line card firmware cancels upgrading for slot %d" "Standby mgmt card firmware is upgrading" "Mgmt card %d firmware upgrade canceled"
ClearTrap	N/A
Object	vsPfsMeshNotif



OID	.1.3.6.1.4.1.21671.3.1.0.9
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsPfsMeshDescr
Description	A vsPfsMeshNotif is generated by the managed system when a change in pfsMesh topology is detected by the system.
Description String	"Link (%s) %s" portid online/offline "Node (%X : %s at %s:label %u:%u) %s" added/removed from pfsMesh "Node (%X : %s at %s:label %u:%u) %s" topology changed
ClearTrap	Self

Object	vsHaNotif
OID	.1.3.6.1.4.1.21671.3.1.0.11
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsHaDescr
Description	A vsHaNotif is generated by either current active redundant unit or newly active redundant unit whenever a change in the high availability occurs.
Description String	"HA is ready" "Switchover occurred to CPU %d" "Switchover initiated from CPU %d" "HA is disabled. Reason: Remote CPU is unreachable." "HA is disabled. Reason: Initializing." "HA is disabled. Reason: No active CPU."
ClearTrap	N/A

Object	vsHlthChckStateNotif
OID	.1.3.6.1.4.1.21671.3.1.0.12
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsHlthChckStateDescr
Description	A vsHlthChckStateNotif is generated by the managed system when a change in health check state on any interface is detected by the system.
Description String	"Health check status for port '%s' in inline monitor group '%s' is %s\n", portbuf, impg_name, up?"UP":"DOWN"
ClearTrap	Self

Object	vsPasswordExpirationNotif
OID	.1.3.6.1.4.1.21671.3.1.0.13
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsPasswordExpirationDescr



Description	A vsPasswordExpirationNotif is generated by the managed system when an user's password is about to expire.
Description String	"User:'%s' login password will expire in %d day(s), Please change the password" "User:'%s' login password expired , Please change the password"
ClearTrap	Self

Object	vsTriggerPolicyNotif
OID	.1.3.6.1.4.1.21671.3.1.0.14
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsTriggerPolicyDescr
Description	A vsTriggerPolicyNotif is generated by the managed system, when a trigger policy state has changed either from active to inactive or inactive to active.
Description String	"Trigger profile %s is now true/active" "Trigger profile %s is now false/inactive"
ClearTrap	Self

Object	vsFRUErrorNotif
OID	.1.3.6.1.4.1.21671.3.1.0.15
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsTriggerPolicyDescr
Description	A vsFRUErrorNotif is generated by the managed system, whenever any FRU error is detected in the system.
Description String	"ALARM: Power Supply %d failed" "Powersafe Unable to enable PFS6002 USB power" "Powersafe USB devices not found"
ClearTrap	vsFRUNormalNotif

Object	vsFRUNormalNotif
OID	.1.3.6.1.4.1.21671.3.1.0.16
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsFRUNormalDescr
Description	A vsFRUErrorNotif is generated by the managed system, whenever any FRU error is detected in the system.
Description String	"Power Supply %d is normal"
ClearTrap	vsFRUErrorNotif



Object	vsTempNormalNotif
OID	.1.3.6.1.4.1.21671.3.1.0.17
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsFRUNormalDescr
Description	A vsTempNormalNotif is generated by the managed system, when the temperature of one of its entity has come back to normal operating state from a high state.
Description String	"Line Card# %d Management Module# %d Fabric Module# %d"
ClearTrap	vsTempHighNotif
Object	vsTunnelStateNotif
OID	.1.3.6.1.4.1.21671.3.1.0.18
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsFRUNormalDescr
Description	A vsTunnelStateNotif is generated by the managed system, when a tunnel state has changed either to up, down or MAC unresolved.
Description String	"Tunnel %s state changed to " UP/Down/mac Unresolved
ClearTrap	Self
Object	vsStrippingNotif
OID	.1.3.6.1.4.1.21671.3.1.0.19
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	vsStrippingDescr
Description	A vsStrippingNotif is generated by the managed system, when stripping table entries are cleared or when stripping tables have reached a certain threshold.
Description String	" MPLS label count 75/90/95/100 percent reached" "Flushing dynamically learned MPLS Labels"
ClearTrap	Self
Object	vsLinkUpNotif
OID	.1.3.6.1.4.1.21671.3.1.0.20
Status	Current
MIB	VSS-SYSTEM-MIB



Trap Components	ifIndex ifAdminStatus ifOperStatus ifName ifAlias
Description	A vsLinkUpNotif is generated by the managed system, when an interface link state has changed to up.
ClearTrap	vsLinkDownNotif
Object	vsLinkDownNotif
OID	.1.3.6.1.4.1.21671.3.1.0.21
Status	Current
MIB	VSS-SYSTEM-MIB
Trap Components	ifIndex ifAdminStatus ifOperStatus ifName ifAlias
Description	A vsLinkDownNotif is generated by the managed system, when an interface link state has changed to down.
ClearTrap	vsLinkUpNotif

## SNMPv2-MIB Traps

The following traps from SNMPv2-MIB (RFC 3418) are supported.

Object	coldStart
OID	.1.3.6.1.6.3.1.1.5.1
Status	Current
MIB	SNMPv2-MIB (RFC 3418)
Description	A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.

## Packet/Port Statistics

### Interfaces MIB Stats

The following statistics from the Interfaces MIB (RFC 2863) are supported.

#### ifNumber

Object (if)	Type	OID	Comment
Number	Integer32	1.3.6.1.2.1.2.1	The number of network interfaces (regardless of their current state) present on this system



## ifTable

Object (if)	Type	OID	Comment
Index	Index	1.3.6.1.2.1.2.2.1.1	A unique value, greater than zero, for each interface
Descr	String	1.3.6.1.2.1.2.2.1.2	A textual string containing information about the interface
Type	Type	1.3.6.1.2.1.2.2.1.3	The type of interface
Mtu	Integer32	1.3.6.1.2.1.2.2.1.4	The size of the largest packet which can be sent/received on the interface, specified in octets
Speed	Gauge32	1.3.6.1.2.1.2.2.1.5	An estimate of the interface's current bandwidth in bits per second
PhysAddress	Address	1.3.6.1.2.1.2.2.1.6	The interface's address at its protocol sub-layer
AdminStatus	Integer	1.3.6.1.2.1.2.2.1.7	The desired state of the interface
OperStatus	Integer	1.3.6.1.2.1.2.2.1.8	The current operational state of the interface
LastChange	TimeTicks	1.3.6.1.2.1.2.2.1.9	The value of sysUpTime at the time the interface entered its current operational state
InOctets	Counter32	1.3.6.1.2.1.2.2.1.10	The total number of octets received on the interface, including framing characters
InUcastPkts	Counter32	1.3.6.1.2.1.2.2.1.11	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer
InDiscards	Counter32	1.3.6.1.2.1.2.2.1.13	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol
InErrors	Counter32	1.3.6.1.2.1.2.2.1.14	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
InUnknownProtos	Counter32	1.3.6.1.2.1.2.2.1.15	For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol
OutOctets	Counter32	1.3.6.1.2.1.2.2.1.16	The total number of octets transmitted out of the interface, including framing characters
OutUcastPkts	Counter32	1.3.6.1.2.1.2.2.1.17	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent
OutDiscards	Counter32	1.3.6.1.2.1.2.2.1.19	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted
OutErrors	Counter32	1.3.6.1.2.1.2.2.1.20	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors



## ifXTable

Object (if)	Type	OID	Comment
Name	String	1.3.6.1.2.1.31.1.1.1.1	The textual name of the interface
InMulticastPkts	Counter32	1.3.6.1.2.1.31.1.1.1.2	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer
InBroadcastPkts	Counter32	1.3.6.1.2.1.31.1.1.1.3	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer
OutMulticastPkts	Counter32	1.3.6.1.2.1.31.1.1.1.4	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent
OutBroadcastPkts	Counter32	1.3.6.1.2.1.31.1.1.1.5	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent
HCIInOctets	Counter64	1.3.6.1.2.1.31.1.1.1.6	The total number of octets received on the interface, including framing characters
HCIInUcastPkts	Counter64	1.3.6.1.2.1.31.1.1.1.7	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer
HCIInMulticastPkts	Counter64	1.3.6.1.2.1.31.1.1.1.8	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer
HCIInBroadcastPkts	Counter64	1.3.6.1.2.1.31.1.1.1.9	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer
HCOutOctets	Counter64	1.3.6.1.2.1.31.1.1.1.10	The total number of octets transmitted out of the interface, including framing characters
HCOutUcastPkts	Counter64	1.3.6.1.2.1.31.1.1.1.11	The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent



<b>Object (if)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
HCOutMulticastPkts	Counter64	1.3.6.1.2.1.31.1.1.1.12	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent
HCOutBroadcastPkts	Counter64	1.3.6.1.2.1.31.1.1.1.13	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent
LinkUpDownTrapEnable	Integer	1.3.6.1.2.1.31.1.1.1.14	Indicates whether linkUp/linkDown traps should be generated for this interface
HighSpeed	Gauge32	1.3.6.1.2.1.31.1.1.1.15	An estimate of the interface's current bandwidth in units of 1,000,000 bits per second
PromiscuousMode	TruthValue	1.3.6.1.2.1.31.1.1.1.16	This object has a value of false(2) if this interface only accepts packets/frames that are addressed to this station
ConnectorPresent	TruthValue	1.3.6.1.2.1.31.1.1.1.17	This object has the value true(1) if the interface sublayer has a physical connector and the value 'false(2)' otherwise
Alias	String	1.3.6.1.2.1.31.1.1.1.18	This object is an alias name for the interface as specified by a network manager, and provides a non-volatile handle for the interface
CounterDiscontinuityTime	TimeStamp	1.3.6.1.2.1.31.1.1.1.19	The value of sysUpTime on the most recent occasion at which any one or more of this interface's counters suffered a discontinuity

## RMON-MIB (RFC 2819)

The following statistics from the RMON-MIB (RFC 2819) are supported.

### etherStatsTable

<b>Object(etherStats)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
Index	Integer32	1.3.6.1.2.1.16.1.1.1.1	A unique value that identifies an etherStats entry.
DataSource	OBJECT IDENTIFIER	1.3.6.1.2.1.16.1.1.1.2	The source of the data that this etherStats entry is configured to analyze.
DropEvents	Counter32	1.3.6.1.2.1.16.1.1.1.3	The total number of events in which packets were dropped by the probe due to lack of resources.



Object(etherStats)	Type	OID	Comment
Octets	Counter32	1.3.6.1.2.1.16.1.1.1.4	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
Pkts	Counter32	1.3.6.1.2.1.16.1.1.1.5	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
BroadcastPkts	Counter32	1.3.6.1.2.1.16.1.1.1.6	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
MulticastPkts	Counter32	1.3.6.1.2.1.16.1.1.1.7	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
CRCAlignErrors	Counter32	1.3.6.1.2.1.16.1.1.1.8	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
UndersizePkts	Counter32	1.3.6.1.2.1.16.1.1.1.9	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
OversizePkts	Counter32	1.3.6.1.2.1.16.1.1.1.10	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	Counter32	1.3.6.1.2.1.16.1.1.1.11	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Jabbers	Counter32	1.3.6.1.2.1.16.1.1.1.12	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).



Object(etherStats)	Type	OID	Comment
Collisions	Counter32	1.3.6.1.2.1.16.1.1.1.13	The best estimate of the total number of collisions on this Ethernet segment.
Pkts64Octets	Counter32	1.3.6.1.2.1.16.1.1.1.14	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Pkts65to127Octets	Counter32	1.3.6.1.2.1.16.1.1.1.15	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Pkts128to255Octets	Counter32	1.3.6.1.2.1.16.1.1.1.16	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Pkts256to511Octets	Counter32	1.3.6.1.2.1.16.1.1.1.17	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Pkts512to1023Octets	Counter32	1.3.6.1.2.1.16.1.1.1.18	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Pkts1024to1518Octets	Counter32	1.3.6.1.2.1.16.1.1.1.19	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Owner	OwnerString	1.3.6.1.2.1.16.1.1.1.20	The entity that configured this entry and is therefore using the resources assigned to it.
Status	EntryStatus	1.3.6.1.2.1.16.1.1.1.21	The status of this etherStats entry.

## HC-RMON-MIB (RFC 3273)

The following statistics from the HC-RMON-MIB (RFC 3273) are supported.

### etherStatsHighCapacityTable

Object (etherStatsHighCapacity)	Type	OID	Comment
OverflowPkts	Counter32	1.3.6.1.2.1.16.1.7.1.1	The number of times the associated etherStatsPkts counter has overflowed.



Object (etherStatsHighCapacity)	Type	OID	Comment
Pkts	Counter64	1.3.6.1.2.1.16.1.7.1.2	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
OverflowOctets	Counter32	1.3.6.1.2.1.16.1.7.1.3	The number of times the associated etherStatsOctets counter has overflowed.
Octets	Counter64	1.3.6.1.2.1.16.1.7.1.4	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
OverflowPkts64Octets	Counter32	1.3.6.1.2.1.16.1.7.1.5	The number of times the associated etherStatsPkts-64Octets counter has overflowed.
Pkts64Octets	Counter64	1.3.6.1.2.1.16.1.7.1.6	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
OverflowPkts65to127Octets	Counter32	1.3.6.1.2.1.16.1.7.1.7	The number of times the associated etherStats-Pkts65to127Octets counter has overflowed.
Pkts65to127Octets	Counter64	1.3.6.1.2.1.16.1.7.1.8	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Pkts65to127Octets	Counter64	1.3.6.1.2.1.16.1.7.1.8	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
OverflowPkts128to255Octets	Counter32	1.3.6.1.2.1.16.1.7.1.9	The number of times the associated etherStats-Pkts128to255Octets counter has overflowed.
Pkts128to255Octets	Counter64	1.3.6.1.2.1.16.1.7.1.10	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).



<b>Object (etherStatsHighCapacity)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
OverflowPkts256to511Octets	Counter32	1.3.6.1.2.1.16.1.7.1.11	The number of times the associated etherStatsPkts256to511Octets counter has overflowed.
Pkts256to511Octets	Counter64	1.3.6.1.2.1.16.1.7.1.12	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
OverflowPkts512to1023Octets	Counter32	1.3.6.1.2.1.16.1.7.1.13	The number of times the associated etherStatsPkts512to1023Octets counter has overflowed.
Pkts512to1023Octets	Counter64	1.3.6.1.2.1.16.1.7.1.14	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
OverflowPkts1024to1518Octets	Counter32	1.3.6.1.2.1.16.1.7.1.15	The number of times the associated etherStatsPkts1024to1518Octets counter has overflowed.
Pkts1024to1518Octets	Counter64	1.3.6.1.2.1.16.1.7.1.16	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

## System Information

### Community MIB

RFC 3584

snmpCommunityTable

<b>Object (snmpCommunity)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
Index	String	1.3.6.1.6.3.18.1.1.1.1	The unique index value of a row in this table
Name	Octet String	1.3.6.1.6.3.18.1.1.1.2	The community string for which a row in this table represents a configuration
SecurityName	String	1.3.6.1.6.3.18.1.1.1.3	A human readable string representing the corresponding value of snmpCommunityName in a Security Model independent format



Object (snmpCommunity)	Type	OID	Comment
ContextEngineID	ID	1.3.6.1.6.3.18.1.1.1.4	The contextEngineID indicating the location of the context in which management information is accessed when using the community string specified by the corresponding instance of snmpCommunityName
ContextName	String	1.3.6.1.6.3.18.1.1.1.5	The context in which management information is accessed when using the community string specified by the corresponding instance of snmpCommunityName
TransportTag	Integer	1.3.6.1.6.3.18.1.1.1.6	This object specifies a set of transport endpoints from which a command responder application will accept management requests
StorageType	Integer	1.3.6.1.6.3.18.1.1.1.7	The storage type for this conceptual row in the snmpCommunityTable
Status	Status	1.3.6.1.6.3.18.1.1.1.8	The status of this conceptual row in the snmpCommunityTable

### snmpTargetAddrExtTable

Object (snmpTarget)	Type	OID	Comment
AddrTMask	String	1.3.6.1.6.3.18.1.2.1.1	The mask value associated with an entry in the snmpTargetAddrTable
AddrMMS	Integer32	1.3.6.1.6.3.18.1.2.1.2	The maximum message size value associated with an entry in the snmpTargetAddrTable

## View-based Access Control Model (VACM) MIB

RFC 3415

vacmSecurityToGroup

Object (vacm)	Type	OID	Comment
SecurityModel	Integer	1.3.6.1.6.3.16.1.2.1.1	The Security Model, by which the vacmSecurityName referenced by this entry is provided
SecurityName	String	1.3.6.1.6.3.16.1.2.1.2	The securityName for the principal, represented in a Security Model independent format, which is mapped by this entry to a groupName
GroupName	String	1.3.6.1.6.3.16.1.2.1.3	The name of the group to which this entry (such as the combination of securityModel and securityName) belongs
SecurityToGroupStorageType	Integer	1.3.6.1.6.3.16.1.2.1.4	The storage type for this conceptual row
SecurityToGroupStatus	Integer	1.3.6.1.6.3.16.1.2.1.5	The status of this conceptual row



## vacmAccessTable

<b>Object (vacmAccess)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
ContextPrefix	String	1.3.6.1.6.3.16.1.4.1.1	In order to gain the access rights allowed by this conceptual row, a contextName must match exactly (if the value of vacmAccessContextMatch is exact) or partially (if the value of vacmAccessContextMatch is prefix) to the value of the instance of this object
SecurityModel	String	1.3.6.1.6.3.16.1.4.1.2	In order to gain the access rights allowed by this conceptual row, this securityModel must be in use
SecurityLevel	Integer	1.3.6.1.6.3.16.1.4.1.3	The minimum level of security required in order to gain the access rights allowed by this conceptual row
ContextMatch	Integer	1.3.6.1.6.3.16.1.4.1.4	If the value of this object is exact(1), then all rows where the contextName exactly matches vacmAccessContextPrefix are selected
ReadViewName	String	1.3.6.1.6.3.16.1.4.1.5	The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes read access
WriteViewName	String	1.3.6.1.6.3.16.1.4.1.6	The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes write access
NotifyViewName	String	1.3.6.1.6.3.16.1.4.1.7	The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes access for notifications
Storage Type	Integer	1.3.6.1.6.3.16.1.4.1.8	The storage type for this conceptual row
Status	Integer	1.3.6.1.6.3.16.1.4.1.9	The status of this conceptual row

## vacmMIBViews

<b>Object (vacmViewTreeFamily)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
ViewName	String	1.3.6.1.6.3.16.1.5.2.1.1	The human readable name for a family of view subtrees
Subtree	ID	1.3.6.1.6.3.16.1.5.2.1.2	The MIB subtree which when combined with the corresponding instance of vacmViewTreeFamilyMask defines a family of view subtrees
Mask	Octet String	1.3.6.1.6.3.16.1.5.2.1.3	The bit mask which, in combination with the corresponding instance of vacmViewTreeFamilySubtree, defines a family of view subtrees



<b>Object (vacmViewTreeFamily)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
Type	Integer	1.3.6.1.6.3.16.1.5.2.1.4	Indicates whether the corresponding instances of vacmViewTreeFamilySubtree and vacmViewTreeFamilyMask define a family of view subtrees which is included in or excluded from the MIB view
StorageType	Type	1.3.6.1.6.3.16.1.5.2.1.5	The storage type for this conceptual row
Status	Status	1.3.6.1.6.3.16.1.5.2.1.6	The status of this conceptual row

## User-based Security Model (USM) MIB

RFC 3414

usmStats

<b>Object (usmStats)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
UnsupportedSecLevels	Counter32	1.3.6.1.6.3.15.1.1.1	The total number of packets received by the SNMP engine which were dropped because they requested a securityLevel that was unknown to the SNMP engine or otherwise unavailable
NotInTimeWindows	Counter32	1.3.6.1.6.3.15.1.1.2	The total number of packets received by the SNMP engine which were dropped because they appeared outside of the authoritative SNMP engine's window
UnknownUserNames	Counter32	1.3.6.1.6.3.15.1.1.3	The total number of packets received by the SNMP engine which were dropped because they referenced a user that was not known to the SNMP engine
UnknownEngineIDs	Counter32	1.3.6.1.6.3.15.1.1.4	The total number of packets received by the SNMP engine which were dropped because they referenced an snmpEngineID that was not known to the SNMP engine
WrongDigests	Counter32	1.3.6.1.6.3.15.1.1.5	The total number of packets received by the SNMP engine which were dropped because they did not contain the expected digest value
DecryptionErrors	Counter32	1.3.6.1.6.3.15.1.1.6	The total number of packets received by the SNMP engine which were dropped because they could not be decrypted

usmUser

<b>Object (usmUser)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
EngineID	ID	1.3.6.1.6.3.15.1.2.2.1.1	An SNMP engine's administratively-unique identifier
Name	String	1.3.6.1.6.3.15.1.2.2.1.2	A human readable string representing the name of the user



Object (usmUser)	Type	OID	Comment
SecurityName	String	1.3.6.1.6.3.15.1.2.2.1.3	A human readable string representing the user in Security Model independent format
CloneFrom	Pointer	1.3.6.1.6.3.15.1.2.2.1.4	A pointer to another conceptual row in this usmUserTable
AuthProtocol	Type	1.3.6.1.6.3.15.1.2.2.1.5	An indication of whether messages sent on behalf of this user to/from the SNMP engine identified by usmUserEngineID, can be authenticated, and if so, the type of authentication protocol which is used
AuthKeyChange	Change	1.3.6.1.6.3.15.1.2.2.1.6	An object, which when modified, causes the secret authentication key used for messages sent on behalf of this user to/from the SNMP engine identified by usmUserEngineID, to be modified via a one-way function
OwnAuthKeyChange	Change	1.3.6.1.6.3.15.1.2.2.1.7	Behaves exactly as usmUserAuthKeyChange with one notable difference: in order for the set operation to succeed, the usmUserName of the operation requester must match the usmUserName that indexes the row which is targeted by this operation
PrivProtocol	Type	1.3.6.1.6.3.15.1.2.2.1.8	An indication of whether messages sent on behalf of this user to/from the SNMP engine identified by usmUserEngineID, can be protected from disclosure, and if so, the type of privacy protocol which is used
PrivKeyChange	Change	1.3.6.1.6.3.15.1.2.2.1.9	An object, which when modified, causes the secret encryption key used for messages sent on behalf of this user to/from the SNMP engine identified by usmUserEngineID, to be modified via a one-way function
OwnPrivKeyChange	Change	1.3.6.1.6.3.15.1.2.2.1.10	Behaves exactly as usmUserPrivKeyChange, with one notable difference: in order for the Set operation to succeed, the usmUserName of the operation requester must match the usmUserName that indexes the row which is targeted by this operation
Public	Octet String	1.3.6.1.6.3.15.1.2.2.1.11	A publicly-readable value which can be written as part of the procedure for changing a user's secret authentication and/or privacy key, and later read to determine whether the change of the secret was effected
StorageType	Type	1.3.6.1.6.3.15.1.2.2.1.12	The storage type for this conceptual row
Status	Status	1.3.6.1.6.3.15.1.2.2.1.13	The status of this conceptual row



## Target MIB

RFC 3413

snmpTargetObjects

<b>Object (snmpTargetAddr)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
Name	String	1.3.6.1.6.3.12.1.2.1.1	The locally arbitrary, but unique identifier associated with this snmpTargetAddrEntry
TDomain	Domain	1.3.6.1.6.3.12.1.2.1.2	This object indicates the transport type of the address contained in the snmpTargetAddrTAddress object
TAddress	Address	1.3.6.1.6.3.12.1.2.1.3	This object contains a transport address
Timeout	Time Interval	1.3.6.1.6.3.12.1.2.1.4	This object should reflect the expected maximum round trip time for communicating with the transport address defined by this row
RetryCount	Integer32	1.3.6.1.6.3.12.1.2.1.5	This object specifies a default number of retries to be attempted when a response is not received for a generated message
TagList	List	1.3.6.1.6.3.12.1.2.1.6	This object contains a list of tag values which are used to select target addresses for a particular operation
Params	String	1.3.6.1.6.3.12.1.2.1.7	The value of this object identifies an entry in the snmpTargetParamsTable
StorageType	Type	1.3.6.1.6.3.12.1.2.1.8	The storage type for this conceptual row
RowStatus	Status	1.3.6.1.6.3.12.1.2.1.9	The status of this conceptual row

snmpTargetParams

<b>Object (snmpTargetParams)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
Name	String	1.3.6.1.6.3.12.1.3.1.1	The locally arbitrary, but unique identifier associated with this snmpTargetParamsEntry
MPModel	Model	1.3.6.1.6.3.12.1.3.1.2	The Message Processing Model to be used when generating SNMP messages using this entry
SecurityModel	Model	1.3.6.1.6.3.12.1.3.1.3	The Security Model to be used when generating SNMP messages using this entry
SecurityName	String	1.3.6.1.6.3.12.1.3.1.4	The securityName which identifies the Principal on whose behalf SNMP messages will be generated using this entry
SecurityLevel	Level	1.3.6.1.6.3.12.1.3.1.5	The Level of Security to be used when generating SNMP messages using this entry
StorageType	Type	1.3.6.1.6.3.12.1.3.1.6	The storage type for this conceptual row
RowStatus	Status	1.3.6.1.6.3.12.1.3.1.7	The status of this conceptual row



## Notification MIB

RFC 3413

snmpNotifyObjects

Object (snmpNotify)	Type	OID	Comment
Name	String	1.3.6.1.6.3.13.1.1.1.1	The locally arbitrary, but unique identifier associated with this snmpNotifyEntry
Tag	Value	1.3.6.1.6.3.13.1.1.1.2	This object contains a single tag value which is used to select entries in the snmpTargetAddrTable
Type	Integer	1.3.6.1.6.3.13.1.1.1.3	This object determines the type of notification to be generated for entries in the snmpTargetAddrTable selected by the corresponding instance of snmpNotifyTag
StorageType	Type	1.3.6.1.6.3.13.1.1.1.4	The storage type for this conceptual row
RowStatus	Status	1.3.6.1.6.3.13.1.1.1.5	The status of this conceptual row

## SNMPv2-MIB

RFC 3418

SNMPv2-MIB:system

Object	Type	OID	Comment
sysDescr	String	1.3.6.1.2.1.1.1	A textual description of the entity.
sysObjectID	OID	1.3.6.1.2.1.1.2	The vendor's authoritative identification of the network management subsystem contained in the entity.
sysUpTime	TimeTicks	1.3.6.1.2.1.1.3	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
sysContact	String	1.3.6.1.2.1.1.4	The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string.
sysName	String	1.3.6.1.2.1.1.5	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.
sysLocation	String	1.3.6.1.2.1.1.6	The physical location of this node. If the location is unknown, the value is the zero-length string.
sysServices	Integer	1.3.6.1.2.1.1.7	A value which indicates the set of services that this entity may potentially offer.



## NTCT-PFS-HEALTH-MIB

### nphCPUTable

<b>Object (nphCPU)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
Index	Unsigned32	1.3.6.1.4.1.21671.3.2.1.1.7.1.1	Indicates an arbitrary integer value which uniquely identifies an entry in nphCPUTable.
Total	Gauge32	1.3.6.1.4.1.21671.3.2.1.1.7.1.2	Indicates the total CPU utilization in percentage on this management index.

### nphPfsHlthStatus

<b>Object</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
nphDeviceId	String	1.3.6.1.4.1.21671.3.2.1.1.1	Indicates vendor-specific product ID string for the PFS.
nphDeviceSerialNumber	String	1.3.6.1.4.1.21671.3.2.1.1.4	Indicates vendor-specific serial number string for the PFS.
nphDeviceModelName	String	1.3.6.1.4.1.21671.3.2.1.1.5	Indicates vendor-specific model name identifier string for the PFS.

### nphInterfaceTable

<b>Object (nphInterface)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
ifIndex	InterfaceIndex	1.3.6.1.2.1.2.2.1.1	A unique value, greater than zero, for each interface.
Type	Integer	1.3.6.1.4.1.21671.3.2.1.1.2.1.1	Indicates that the interface is operating in one of the NphIfType modes.
Class	Integer	1.3.6.1.4.1.21671.3.2.1.1.2.1.2	Indicates the class of the interface.

### nphMemoryTable

<b>Object (nphMemory)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
Index	Unsigned32	1.3.6.1.4.1.21671.3.2.1.1.6.1.1	Indicates an arbitrary integer value which uniquely identifies an entry in nphMemoryTable.
Total	Gauge32	1.3.6.1.4.1.21671.3.2.1.1.6.1.2	Indicates the total memory in kilobytes available on this management index.
Free	Gauge32	1.3.6.1.4.1.21671.3.2.1.1.6.1.3	Indicates the unused memory in kilobytes available on this management index.



### nphFlowMapTable

<b>Object (nphFlow)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
Index	Unsigned32	1.3.6.1.4.1.21671.3.2.1.1.3.1	Indicates an arbitrary integer value which uniquely identifies a traffic flow in nphFlowMapTable
Name	String	1.3.6.1.4.1.21671.3.2.1.1.3.1.1.2	Indicates the name of the map for a given packet flow
Filter	String	1.3.6.1.4.1.21671.3.2.1.1.3.1.1.3	Indicates name of the filter for a given packet flow

### nphFlowInterfaceTable

<b>Object (nphFlowInterface)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
nphFlowMapIndex	Unsigned32	1.3.6.1.4.1.21671.3.2.1.1.3.1	Indicates an arbitrary integer value which uniquely identifies a traffic flow in nphFlowMapTable
InIf	InterfaceIndex	1.3.6.1.4.1.21671.3.2.1.1.3.2.1.1	Indicates the ifindex of the input interface for a given packet flow
Index	Unsigned32	1.3.6.1.4.1.21671.3.2.1.1.3.2.1.2	Indicates an arbitrary integer value which uniquely identifies a traffic flow entry in nphFlowInterfaceTable
OutIf	InterfaceIndex	1.3.6.1.4.1.21671.3.2.1.1.3.2.1.3	Indicates the ifindex of the output interface for a given packet flow

### nphFlowLbgTable

<b>Object (nphFlowLbg)</b>	<b>Type</b>	<b>OID</b>	<b>Comment</b>
nphFlowMapIndex	Unsigned32	1.3.6.1.4.1.21671.3.2.1.1.3.1.1.1	Indicates an arbitrary integer value which uniquely identifies a traffic flow in nphFlowMapTable
nphFlowInterfaceInIf	InterfaceIndex	1.3.6.1.4.1.21671.3.2.1.1.3.2.1.1	Indicates the ifindex of the input interface for a given packet flow
Index	Unsigned32	1.3.6.1.4.1.21671.3.2.1.1.3.3.1.1	Indicates an arbitrary integer value which uniquely identifies a traffic flow entry in nphFlowLbgTable



Object (nphFlowLbg)	Type	OID	Comment
Name	String	1.3.6.1.4.1.21671.3.2.1.1.3.3.1.2	Indicates the name of the LBG (load balance group) for a given packet flow

### nphFilterStatsTable

Object (nphFilterStats)	Type	OID	Comment
ifIndex	InterfaceIndex	1.3.6.1.2.1.2.2.1.1	A unique value, greater than zero, for each interface
Filter	String	1.3.6.1.4.1.21671.3.2.1.2.1.1.1	indicates the filter name on which traffic is monitored
Pkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.1.1.2	indicates the total number of packets received on the corresponding ifIndex and nphFilterStatsFilter

### nphIfExtTable

Object (nphIfExt)	Type	OID	Comment
ifIndex	InterfaceIndex	1.3.6.1.2.1.2.2.1.1	A unique value, greater than zero, for each interface
CRCOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.1	Total number of CRC error octets received on this interface. Shows '0' always
InMulticastOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.2	The total number of good octets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address. Shows '0' always
InUndersizeOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.3	Total number of octets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed. Shows '0' always



Object (nphIfExt)	Type	OID	Comment
InOversizeOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.4	Total number of octets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. Shows '0' always
InUcastOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.5	Number of octets received which were not addressed to a multicast or broadcast address at this sub-layer. Shows '0' always
InBroadcastOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.6	Total number of good octets received which were addressed to a broadcast address at this sub-layer. Shows '0' always
InDropPkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.7	Total number of packets received that were dropped due to buffer overflow
InDropOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.8	Total number of octets received that were dropped due to buffer overflow. Shows '0' always
InPkts1519to2047Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.9	Total number of packets (including bad packets) received that were between 1519 and 2047 octets in length inclusive (excluding framing bits but including FCS octets)
InPkts2048to4095Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.10	Total number of packets (including bad packets) received that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets)



Object (nphIfExt)	Type	OID	Comment
InPkts4096to9216Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.11	Total number of packets (including bad packets) received that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets)
InOverPkts9216Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.12	Total number of packets received that were longer than 9216 packets (excluding framing bits, but including FCS octets) and were otherwise well formed
InIPv4Pkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.13	Total number of packets received that were directed to a IPv4 address. Shows '0' always
InIPv4Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.14	Total number of octets received that were directed to a IPv4 address. Shows '0' always
InIPv4FragmentsPkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.15	Total number of fragmented packets received that were directed to a IPv4 address. Shows '0' always
InIPv4FragmentsOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.16	Total number of fragmented octets received that were directed to a IPv4 address. Shows '0' always
InIPv6Pkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.17	Total number of packets (including bad packets) received that were directed to a IPv6 address. Shows '0' always



Object (nphIfExt)	Type	OID	Comment
InIPv6Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.18	Total number of octets received that were directed to a IPv6 address. Shows '0' always
InIPv6FragmentsPkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.19	Total number of fragmented packets received that were directed to a IPv6 address. Shows '0' always
InIPv6FragmentsOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.20	Total number of fragmented octets received that were directed to a IPv6 address. Shows '0' always
OutMulticastOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.21	Total number of good octets transmitted that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address. Shows '0' always
OutUndersizeOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.22	Total number of octets transmitted that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed. Shows '0' always
OutOversizeOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.23	Total number of octets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. Shows '0' always
OutUcastOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.24	Number of octets transmitted which were not addressed to a multicast or broadcast address at this sub-layer. Shows '0' always



Object (nphIfExt)	Type	OID	Comment
OutBroadcastOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.25	Total number of good octets transmitted which were addressed to a broadcast address at this sub-layer. Shows '0' always
OutDropPkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.26	Total number of packets transmitted that were dropped due to buffer overflow.
OutDropOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.27	Total number of octets transmitted that were dropped due to buffer overflow. Shows '0' always
OutPkts1519to2047Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.28	Total number of packets (including bad packets) transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
OutPkts2048to4095Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.29	Total number of packets (including bad packets) transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
OutPkts4096to9216Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.30	Total number of packets (including bad packets) transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
OutOverPkts9216Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.31	Total number of packets transmitted that were longer than 9216 packets (excluding framing bits, but including FCS octets) and were otherwise well formed.



Object (nphIfExt)	Type	OID	Comment
OutIPv4Pkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.32	Total number of packets transmitted that were directed to a IPv4 address. Shows '0' always
Counter64	OutIPv4Octets	1.3.6.1.4.1.21671.3.2.1.2.2.1.33	The total number of octets transmitted that were directed to a IPv4 address. Shows '0' always
OutIPv4FragmentsPkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.34	Total number of fragmented packets transmitted that were directed to a IPv4 address. Shows '0' always
OutIPv4FragmentsOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.35	Total number of fragmented octets transmitted that were directed to a IPv4 address. Shows '0' always
OutIPv6Pkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.36	Total number of packets (including bad packets) transmitted that were directed to a IPv6 address. Shows '0' always
OutIPv6Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.37	Total number of octets transmitted that were directed to a IPv6 address. Shows '0' always
OutIPv6FragmentsPkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.38	Total number of fragmented packets transmitted that were directed to a IPv6 address. Shows '0' always
OutIPv6FragmentsOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.39	Total number of fragmented octets transmitted that were directed to a IPv6 address. Shows '0' always



Object (nphIfExt)	Type	OID	Comment
OutUndersizePkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.40	Total number of packets transmitted that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed. Shows '0' always
OutOversizePkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.41	Total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed
OutPkts64Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.42	Total number of packets (including bad packets) transmitted that were 64 octets in length (excluding framing bits but including FCS octets)
OutPkts65to127Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.43	Total number of packets (including bad packets) transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets)
OutPkts128to255Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.44	Total number of packets (including bad packets) transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets)
OutPkts256to511Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.45	Total number of packets (including bad packets) transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets)



Object (nphIfExt)	Type	OID	Comment
OutPkts512to1023Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.46	Total number of packets (including bad packets) transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets)
OutPkts1024to1518Octets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.47	Total number of packets (including bad packets) transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets)
PeakPkts	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.48	Indicates the peak packets count on the given interface. Shows '0' always
PeakTimePkts	DateAndTime	1.3.6.1.4.1.21671.3.2.1.2.2.1.49	Indicates the time of the most recent change in the corresponding instance value of PeakTimePkts. This object contains value 0x0000010100000000 when the corresponding instance value of PeakTimePkts is '0'. shows 0-1-1,0:0:0.0,+0:0 always
PeakOctets	Counter64	1.3.6.1.4.1.21671.3.2.1.2.2.1.50	Indicates the peak octets count on the given interface. shows '0' always
PeakTimeOctets	DateAndTime	1.3.6.1.4.1.21671.3.2.1.2.2.1.51	Indicates the time of the most recent change in the corresponding instance value of PeakOctets. This object contains value 0x0000010100000000 when the corresponding instance value of PeakOctets is '0'. shows 0-1-1,0:0:0.0,+0:0 always



Object (nphIfExt)	Type	OID	Comment
InThroughput	DisplayString	1.3.6.1.4.1.21671.3.2.1.2.2.1.52	Indicates the throughput in Mbps received on the given interface
InMaxThroughput	DisplayString	1.3.6.1.4.1.21671.3.2.1.2.2.1.53	Indicates the maximum throughput in Mbps received on the given interface
OutThroughput	DisplayString	1.3.6.1.4.1.21671.3.2.1.2.2.1.54	Indicates the throughput in Mbps transmitted from the given interface
OutMaxThroughput	DisplayString	1.3.6.1.4.1.21671.3.2.1.2.2.1.55	Indicates the maximum throughput in Mbps transmitted from the given interface
InUtilization	DisplayString	1.3.6.1.4.1.21671.3.2.1.2.2.1.56	Indicates the utilization in percentage on the given input interface
InMaxUtilization	DisplayString	1.3.6.1.4.1.21671.3.2.1.2.2.1.57	Indicates the maximum utilization in percentage on the given input interface
OutUtilization	DisplayString	1.3.6.1.4.1.21671.3.2.1.2.2.1.58	Indicates the utilization in percentage on the given output interface
OutMaxUtilization	DisplayString	1.3.6.1.4.1.21671.3.2.1.2.2.1.59	Indicates the maximum utilization in percentage on the given output interface
InPPS	DisplayString	.1.3.6.1.4.1.21671.3.2.1.2.2.1.60	Indicates the packets per second (PPS) received on the given interface.
OutPPS	DisplayString	.1.3.6.1.4.1.21671.3.2.1.2.2.1.61	Indicates the packets per second (PPS) transmitted from the given interface.



## VSS-SYSTEM-MIB

### vsTemperatureStatusTable

Object (vsTemperature Status)	Type	OID	Comment
Index	Unsigned32	1.3.6.1.4.1.21671.3.1.1.1.1.1	Indicates an arbitrary integer value which uniquely identifies an entry in vsTemperatureStatusTable
Descr	String	1.3.6.1.4.1.21671.3.1.1.1.1.2	Indicates the human-readable description of the entity with the temperature being monitored
Value	Gauge32	1.3.6.1.4.1.21671.3.1.1.1.1.3	Indicates the temperature value of the entity being monitored

### vsNotifsControl

Object (vsNotifsControl)	Type	OID	Comment
vsTempHighNotifEnable	TruthValue	1.3.6.1.4.1.21671.3.1.1.2.2	This object specifies whether the system generates the vsTempHighNotif or not. A value of 'false' will prevent vsTempHighNotif notifications from being generated by this system.
vsCfgChangeNotifEnable	TruthValue	1.3.6.1.4.1.21671.3.1.1.2.3	This object specifies whether the system generates the vsCfgChangeNotif or not. A value of 'false' will prevent vsCfgChangeNotif notifications from being generated by this system.



Object (vsNotifsControl)	Type	OID	Comment
vsAuthenticationNotifEnable	TruthValue	1.3.6.1.4.1.21671.3.1.1.2.4	This object specifies whether the system generates the vsAuthenticationNotif or not. A value of 'false' will prevent vsAuthenticationNotif notifications from being generated by this system.
vsFRUNotifEnable	TruthValue	1.3.6.1.4.1.21671.3.1.1.2.5	This object specifies whether the system generates any FRU (Field Replaceable Unit) notifications or not. A value of 'false' will prevent any FRU notifications from being generated by this system.
vsSystemNotifEnable	BITS	1.3.6.1.4.1.21671.3.1.1.2.6	This object specifies whether the system generates the specified notification or not. If a bit corresponding to a notification is set to 1, then the specified notification can be generated. restart: the vsRestartNotif notification. filemgmt: the vsFileMgmtNotif notification. highavailability: the vsHaNotif notification.
vsPfsMeshNotifEnable	TruthValue	1.3.6.1.4.1.21671.3.1.1.2.7	This object specifies whether the system generates any packet flow switch mesh (pfsMesh) notifications or not. A value of 'false' will prevent any pfsMesh notifications from being generated by this system.



Object (vsNotifsControl)	Type	OID	Comment
vsHlthChckStateNotifEnable	TruthValue	1.3.6.1.4.1.21671.3.1.1.2.8	This object specifies whether the system generates any health check state notifications or not. A value of 'false' will prevent any health check state notifications from being generated by this system.
vsTriggerPolicyNotifEnable	TruthValue	1.3.6.1.4.1.21671.3.1.1.2.9	This object specifies whether the system generates any trigger policy notifications or not. A value of 'false' will prevent any trigger policy notifications from being generated by this system.
vsTunnelStateNotifEnable	TruthValue	1.3.6.1.4.1.21671.3.1.1.2.10	This object specifies whether the system generates any tunnel state change notifications or not. A value of 'false' will prevent any tunnel state change notifications from being generated by this system.
vsStrippingNotifEnable	TruthValue	1.3.6.1.4.1.21671.3.1.1.2.11	This object specifies whether the system generates any stripping notifications or not. A value of 'false' will prevent any stripping notifications from being generated by this system.
vsSNMPAuthenticationNotifEnable	TruthValue	1.3.6.1.4.1.21671.3.1.1.2.12	This object specifies whether the system generates any SNMP authentication notifications or not. A value of 'false' will prevent any SNMP authentication notifications from being generated by this system.



Object (vsNotifsControl)	Type	OID	Comment
vsLinkUpDownNotifEnable	TruthValue	1.3.6.1.4.1.21671.3.1.1.2.13	This object specifies whether the system generates any link state change notifications for a given interface or not. A value of 'false' will prevent any link state change notifications from being generated by this system.

## D PFS+PFX Inner Filtering and Inner Load Balancing

nGenius Packet Flow eXtender (PFX) Certified appliances enable expert packet conditioning for service assurance and cyber security monitoring. The solution is built on the NETSCOUT hardware platforms and framework, leveraging patented technologies.

NETSCOUT provides a PFS+PFX solution enabling the PFS device to route traffic through the PFX, utilizing PFX's inner filtering and inner load-balancing functionality:

- PFX Inner Filtering: The Certified PFX appliance applies filters to incoming received traffic and then retransmits the packets with VLAN tags added.
- PFX Inner Load Balancing: The Certified PFX appliance load balances incoming received traffic per defined criteria, assigning unique VLAN tags to packets based on their hash value or round-robin selection, and then retransmits the packets with the added VLAN tags.

**Note:** PFX Configuration is beyond the scope of this document; refer to the ***Certified Packet Flow eXtender (PFX) Appliance Administrator Guide*** for details about PFX Inner Filtering and Inner Load Balancing.

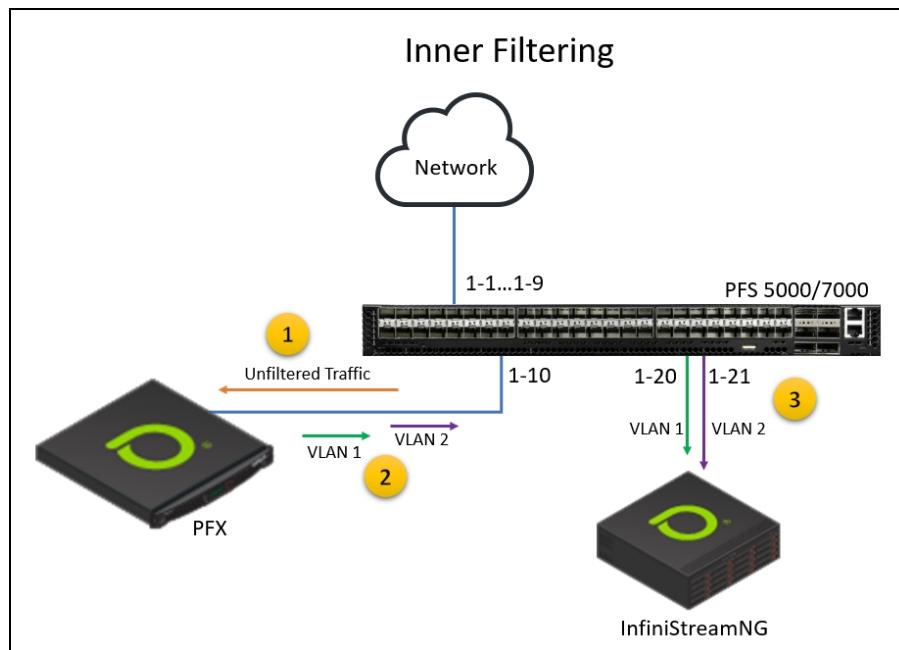
Refer to the following sections for details:

- [PFS+PFX Inner Filtering](#)
- [PFS+PFX Inner Load Balancing](#)
- [PFOS/PFX Inner Filtering and Inner Load Balancing Known Limitations](#)



## PFS+PFX Inner Filtering

The following graphic and text illustrate the PFS+PFX inner filtering process.



### Inner Filtering Process Summary:

1. PFS devices receive traffic from the network on interfaces 1-1 to 1-9. PFS forwards all traffic (unfiltered) to PFX on port 1-10.
2. PFX filters the traffic based on the inner parameters of the packet. Once filtered, PFX assigns unique VLANs (VLAN1, VLAN2, etc.) per filter (1 to 4000) and forwards the tagged packets back to PFS. (VLANs between 4001 and 4016 are reserved for load balance group purposes).
3. PFS then forwards traffic to destinations based on the outer VLAN tags the PFX added to the packets.

**Note 1:** PFX sends traffic back to the PFS using the same port on which PFOS originally forwarded it. Users can route the traffic based on their topology requirements by configuring traffic maps accordingly. The port connecting the PFX and PFS must be a SPAN-Monitor port.

**Note 2:** When utilizing PFX inner filtering, because VLAN tags are removed when the packets return to the PFS from the PFX, enabling VLAN tagging on Monitor ports will not have any effect on packets received from PFX (that is, from a Span-Monitor port with External VLAN Tagging enabled).



## PFX+PFS Inner Filtering Configuration Workflow

The following steps summarize the process for configuring PFX+PFS inner filtering. For a configuration example, refer to [PFX+PFS Inner Filtering Configuration Example](#).

### 1. Configure the PFX.

Define filters to match parameters in the inner or outer packet headers/payload, and to assign unique VLAN tags to packets based on filter matches.

**Note:** PFX Configuration is beyond the scope of this document; refer to the **Certified Packet Flow eXtender (PFX) Appliance Administrator Guide** for details about PFX Inner Filtering.

### 2. Configure PFS Port Settings.

The port connecting the PFS to the PFX appliance must be **Span-Monitor** port class and have the **External Device Tagging** option enabled. You can also enable the external-device-tagging option for the interface CLI command. When this option is enabled, PFOS does not add the port's VLAN tag during ingress processing.

**Note:** If the Span-Mon port/link connecting the PFS to the PFX does not come up, enable the FEC setting and set the FEC Type with the default value CL91.

### 3. Configure PFS filter expression **extvlan <x>**, where <x> is the vtag configured on the PFX in Step 1.

#### 4. Create traffic map from PFS to PFX:

- **Filter:** Any filter, typically Unfiltered.
- **Ingress:** Span port on which PFS is receiving traffic from network.
- **Egress:** Span-Mon port connecting the PFX to PFS (**External Device Tagging** option enabled).

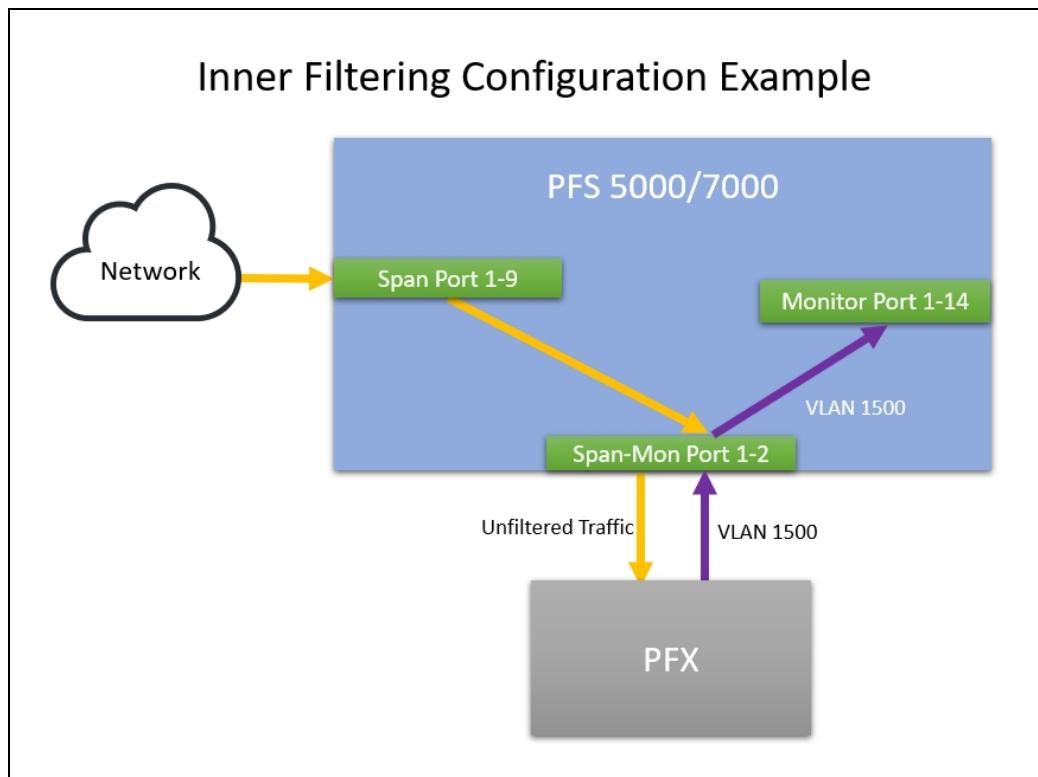
#### 5. Create traffic map for return traffic from PFX to PFS:

- **Filter:** The extvlan filter created in Step 3.
- **Ingress:** Span-Mon port connecting the PFX to PFS (**External Device Tagging** option enabled).
- **Egress:** Configure ports per desired destinations.



## PFX+PFS Inner Filtering Configuration Example

This section provides configuration details for the following PFX+PFS inner filtering example; for simplicity, the example only shows filtering traffic to a single destination.



The following steps provide configuration details for the inner filtering example.

1. Configure the PFX.

Define filters to match parameters in the inner or outer packet headers/payload, and to assign unique VLAN tags to packets based on filter matches. The vtag defined for this example is 1500.

**Note:** PFX Configuration is beyond the scope of this document; refer to the **Certified Packet Flow eXtender (PFX) Appliance Administrator Guide** for details about PFX Inner Filtering.



## 2. Configure PFS Port Settings:

Port	Port Class	Notes
Port 1-9	Span	Port on which PFS device receives traffic from the network.
Port 1-2	Span-Monitor	Enable <b>External Device Tagging</b> (interface command <code>external-device-tagging</code> option). When this option is enabled, PFOS does not add the port's VLAN tag during ingress processing. <b>Note:</b> If the Span-Mon port/link connecting the PFS to the PFX does not come up, enable the FEC setting and set the FEC Type with the default value CL91.
Port 1-14	Monitor	Destination port.

The following graphic shows the port settings for port 1-2.

### Port 1-2 Settings

Reset Port ▾

Basic Advanced References

Name: string  
A user friendly port name. Max length is 64.

Class:  Span  Monitor  Span-Monitor  Service  pStack  pStack plus  Inline Network  Inline Monitor

Link State: Auto  
Default: auto  
Port Link state

Speed: 100000  
Port Speed (Mbps/sec)

Vlan Tagging: Disable  
Default: disable  
VLAN tagging enable/disable

Port Breakout:  Default: disable  
Port Breakout into 10G

FEC:  Default:disable  
Forward error correction

FEC Type: cl91  
Default: cl91  
Forward error correction type

VLAN ID:  Default  User Defined

Link: up  
Default: down  
Port Link status

Tunnel Termination:  Default: disable  
Tunnel Termination Support

LLDP:  Rx  Tx

External Device Tagging:  Default: disable  
External Device Tagging Mode

Stripping:

Vlan Tag:  Default: disable  
Select to enable VLAN tag stripping

Vn Tag:  Default: disable  
Select to enable VN tag stripping

VxLAN:  Default: disable  
Select to enable VxLAN tag stripping

L2GRE:  Default: disable  
Select to enable L2GRE stripping



3. In PFOS Forwarding Filters, configure a filter expression for **extvlan 1500**, which matches the vtag 1500 configured on the PFX in Step 1. The following graphic shows the extvlan filter configuration.

The screenshot shows the 'ExtVLAN1500' configuration dialog. It includes fields for 'Description' (string, 1 character or more), 'Ref Map' (Map Name), 'Ref Toolgroup' (Name), and a 'Forwarding Filter Expression' (FFE) field containing 'extvlan 1500'. The 'extvlan 1500' entry is highlighted with a yellow background.

4. Create a traffic map from PFS to PFX:
  - **Filter:** Unfiltered
  - **Ingress:** Port 1-9
  - **Egress:** Port 1-2 connecting the PFX to PFS



The following graphic shows the map configuration for traffic flow from the PFS to the PFX.

### PFS\_to\_PFX\_IF ×

Description  string  
1 characters or more.  
A string description of map

Type  Monitor  
Default: Monitor  
A map type

Mode  Basic  
Default: Basic  
Map mode Basic/Extended

Filter  unfiltered    
()

Ingress  configure ×  
Selected Ingress : 1-9  
Input port(s)

Egress  configure ×  
Selected Egress: 1-2  
Output port(s)

Load Balance Criteria  ...  
Load-balance criteria

Output Load Balance Groups  Add an entry ...  
Output load-balance groups

5. Create a traffic map for return traffic from PFX to PFS:

- **Filter:** The extvlan filter created in Step 3.
- **Ingress:** Port 1-2 connecting the PFX to PFS
- **Egress:** Port 1-14



The following graphic shows the map configuration for return traffic flow from the PFX back to the PFS.

### PFXReturnTrafficPFS ×

Description  1 characters or more.  
A string description of map

Type  Default: Monitor  
A map type

Mode  Default: Basic  
Map mode Basic/Extended

Filter  ... 0

Ingress  × Selected Ingress : 1-2  
Input port(s)

Egress  × Selected Egress: 1-14  
Output port(s)

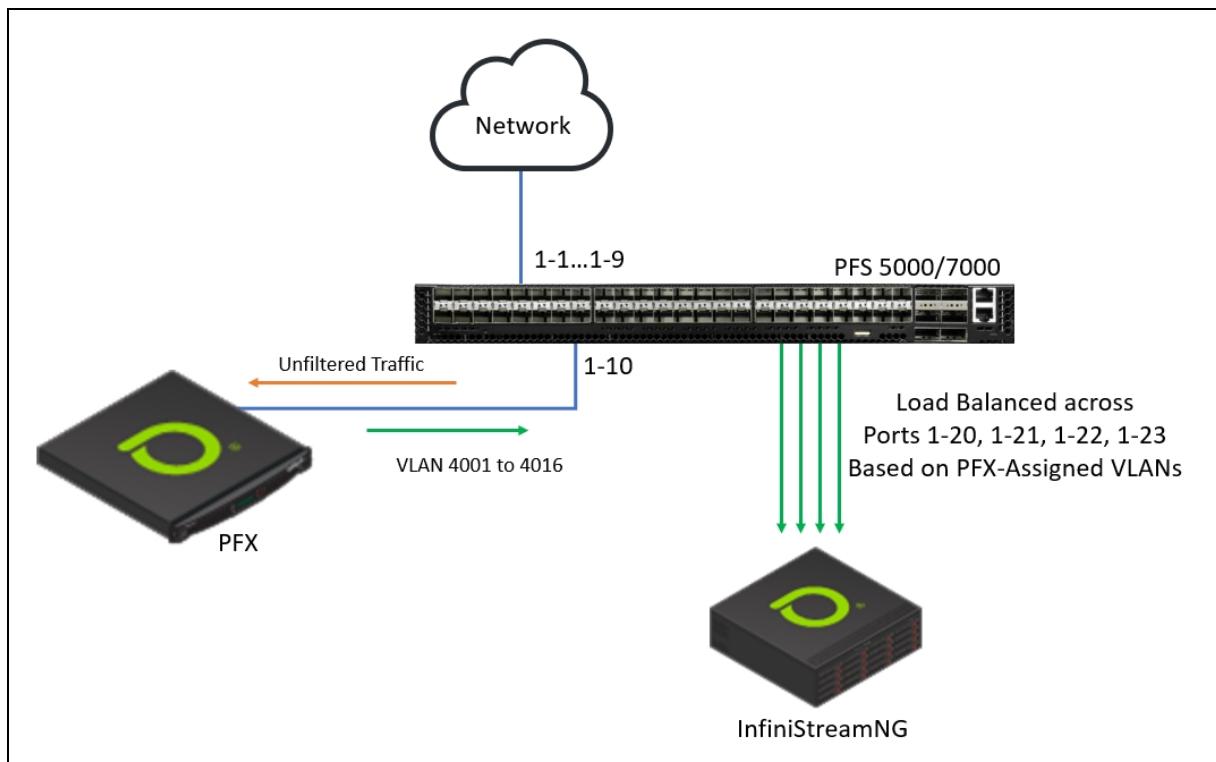
Load Balance Criteria  Load-balance criteria

Output Load Balance Groups  Output load-balance groups



## PFS+PFX Inner Load Balancing

The following graphic and text illustrate the PFS+PFX inner load balancing process.



### Inner Load Balancing Process Summary:

1. PFS devices receive traffic from the network on interfaces 1-1 to 1-9. PFS forwards all traffic (unfiltered) to PFX on port 1-10.
2. PFX load balances the traffic based on the inner parameters of the packet. Once filtered, PFX assigns a VLAN between 4001 and 4016 for load balancing purposes and forwards the tagged packets back to PFS.
3. PFS distributes the traffic to available ports in the load-balance groups using the unique PFX-assigned VLANs. When destinations become unavailable, PFOS redistributes traffic accordingly.

**Note 1:** PFX sends traffic back to the PFS using the same port on which PFOS originally forwarded it. Users can route the traffic based on their topology requirements by configuring traffic maps accordingly. The port connecting the PFX and PFS must be a SPAN-Monitor port.

**Note 2:** When utilizing PFX inner filtering, because VLAN tags are removed when the packets return to the PFS from the PFX, enabling VLAN tagging on Monitor ports will not have any effect on packets received from PFX (that is, from a Span-Monitor port with External VLAN Tagging enabled).



## PFX+PFS Inner Load Balancing Configuration Workflow

The following steps summarize the process for configuring PFX+PFS inner load balancing. For a configuration example, refer to [PFX+PFS Inner Load Balancing Configuration Example](#).

### 1. Configure the PFX.

Define load-balancing criteria based on either a hash calculation (on inner or outer packet headers/payload) or round-robin selection. Configure vtags on PFX between 4001-4016 which are the VLAN IDs PFS uses internally. The Certified PFX appliance load balances incoming received traffic per defined criteria, assigning VLAN tags 4001-4016 to packets based on their hash value or round-robin selection, and then retransmits the packets to PFS with the added VLAN tags.

**Note:** PFX Configuration is beyond the scope of this document; refer to the **Certified Packet Flow eXtender (PFX) Appliance Administrator Guide** for details about PFX Inner Filtering.

### 2. Configure PFS Port Settings.

The port connecting the PFS to the PFX appliance must be **Span-Monitor** port class and have the **External Device Tagging** option enabled. You can also enable the external-device-tagging option for the `interface` CLI command. When this option is enabled, PFOS does not add the port's VLAN tag during ingress processing.

**Note:** If the Span-Mon port/link connecting the PFS to the PFX does not come up, enable the FEC setting and set the FEC Type with the default value CL91.

### 3. Create PFS Load Balance Group.

- Add Monitor ports.
- Enable **Pfx** option. When 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).
- Select failover type (only Redistribute, Rebalance, or Drop options are supported with PFX mode).

### 4. Create traffic map from PFS to PFX:

- **Filter:** Any filter, typically Unfiltered.
- **Ingress:** Span port on which PFS is receiving traffic from network.
- **Egress:** Span-Mon port connecting the PFX to PFS (**External Device Tagging** option enabled).

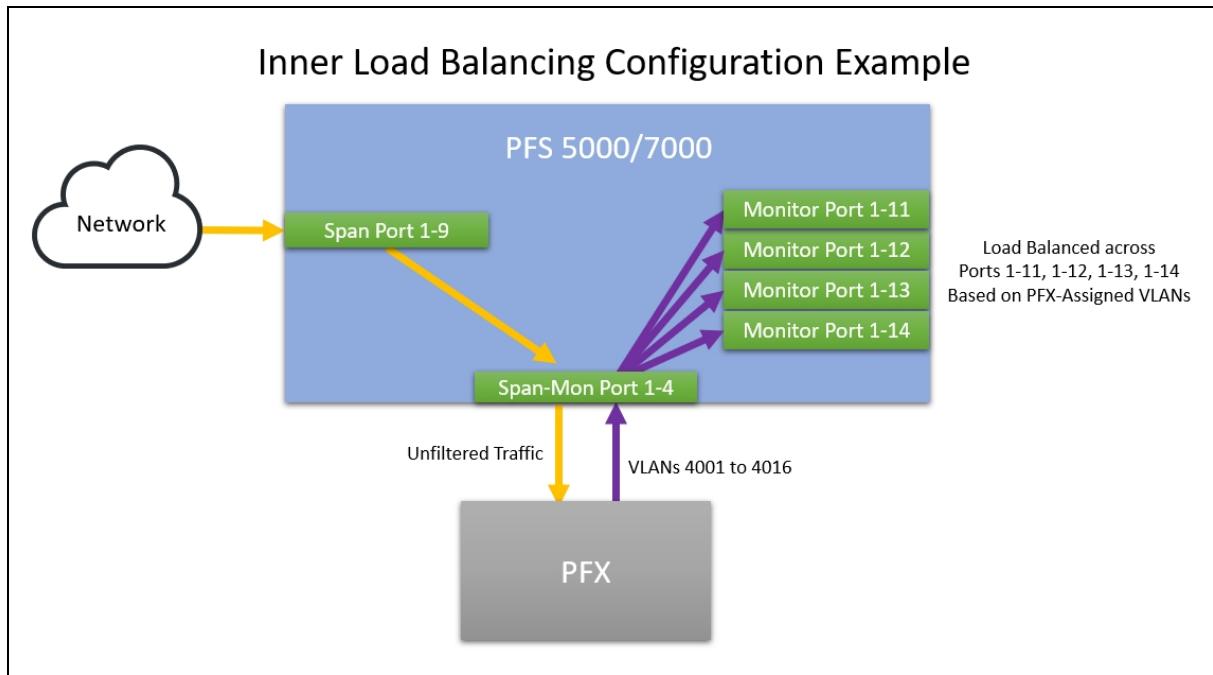
### 5. Create traffic map for load balanced return traffic from PFX to PFS:

- **Filter:** Nonmatch
- **Ingress:** Span-Mon port connecting the PFX to PFS (**External Device Tagging** option enabled).
- **Load Balance Criteria:** PFX (pre-defined criteria). This pre-defined Load Balance Criteria disables Layer 2, Layer 3, and Layer 4 fields as it is not possible to load balance on these fields.
- **Output Load Balance Group:** Load Balance Group defined in Step 3. Additional ports can be used in the traffic map; however, only one Load Balance Group can be used in the traffic map.



## PFX+PFS Inner Load Balancing Configuration Example

This section provides configuration details for the following PFX+PFS inner load balancing example.



The following steps provide configuration details for the inner filtering example.

1. Configure the PFX.

Define load-balancing criteria based on either a hash calculation (on inner or outer packet headers/payload) or round-robin selection. Configure vtags on PFX between 4001-4016 which are the VLAN IDs PFS uses internally. The Certified PFX appliance load balances incoming received traffic per defined criteria, assigning VLAN tags 4001-4016 to packets based on their hash value or round-robin selection, and then retransmits the packets to PFS with the added VLAN tags.

**Note:** PFX Configuration is beyond the scope of this document; refer to the ***Certified Packet Flow eXtender (PFX) Appliance Administrator Guide*** for details about PFX Inner Filtering.



## 2. Configure PFS Port Settings:

Port	Port Class	Notes
Port 1-9	Span	Port on which PFS device receives traffic from the network.
Port 1-4	Span-Monitor	Enable <b>External Device Tagging</b> (interface command <code>external-device-tagging</code> option). When this option is enabled, PFOS does not add the port's VLAN tag during ingress processing. <b>Note:</b> If the Span-Mon port/link connecting the PFS to the PFX does not come up, enable the FEC setting and set the FEC Type with the default value CL91.
Port 1-11	Monitor	Ports in load balancing group.
Port 1-12		
Port 1-13		
Port 1-14		

The following graphic shows the port settings for port 1-4.

### Port 1-4 Settings

Basic Advanced References

Name: string  
A user friendly port name. Max length is 64.

Class:  Span  Monitor  Span-Monitor  Service  pStack  pStack plus  Inline Network  Inline Monitor

Link State: Auto  
Default: auto  
Port Link state

Speed: 100000  
Port Speed (Mbps/sec)

Vlan Tagging: Disable  
Default: disable  
VLAN Tagging enable/disable

Port Breakout:  Default: disable  
Port Breakout into 10G

FEC:  Default: disable  
Forward error correction

FEC Type: cl91  
Default: s91  
Forward error correction type

VLAN ID:  Default  User Defined

Link: up  
Default: down  
Port Link status

Tunnel Termination:  Default: disable  
Tunnel Termination Support

LLDP:  Rx  Tx

External Device Tagging:  Default: disable  
External Device Tagging Mode

Stripping

Vlan Tag:  Default: disable  
Select to enable VLAN tag stripping

Vn Tag:  Default: disable  
Select to enable VN tag stripping

VxLAN:  Default: disable  
Select to enable VxLAN tag stripping

L2GRE:  Default: disable  
Select to enable L2GRE stripping

## 3. Create PFS Load Balance Group.

- Failover Action:** Rebalance is used for example. Redistribute, Rebalance, or Drop are only options supported with PFX mode.
- Ports:** 1-11, 1-12, 1-13, 1-14
- Pfx:** Enabled. Distribution of traffic is based on VLAN tags added by PFX appliance.



The following graphic shows the Load Balance Group configuration settings.

**PFX\_InnerLB\_LBG** × Load balancing groups

New Load Balance Group...

Basics References Ref Trigger

Description string  
1 characters or more.

Failover Action Rebalance the load among active members - traffic will be disturbed  
Default: Rebalance  
Failover action when any port in LBG goes offline

Type Monitor  
Default: Monitor  
Load-balance group type

Ports/Tunnels configure ×  
Ports selection  
Selected Ports/Tunnels: 1-11, 1-12, 1-13, 1-14

Pfx   
Enable/Disable PFX Mode in LBG

Error Code None  
Default: None

Oper Status Up  
Default: Down

4. Create a traffic map from PFS to PFX:
  - **Filter:** Unfiltered
  - **Ingress:** Port 1-9
  - **Egress:** Port 1-4 connecting the PFX to PFS



The following graphic shows the map configuration for traffic flow from the PFS to the PFX.

### PFStoPFX\_ILB ×

Description  Type  Default: Monitor

1 characters or more.  
A string description of map

Mode  Filter  ( )

Default: Basic  
Map mode Basic/Extended

Ingress  Selected Ingress: 1-9  
Input port(s)

Egress  Selected Egress: 1-4  
Output port(s)

Load Balance Criteria  Load-balance criteria

Output Load Balance Groups  Output load-balance groups

5. Create a traffic map for load balanced return traffic from PFX to PFS:
  - **Filter:** Nonmatch.
  - **Ingress:** Port 1-4 connecting the PFX to PFS
  - **Load Balance Criteria:** PFX (pre-defined criteria). This pre-defined Load Balance Criteria disables Layer 2, Layer 3, and Layer 4 fields as it is not possible to load balance on these fields.
  - **Output Load Balance Group:** Load Balance Group defined in Step 3.



The following graphic shows the map configuration for load balanced return traffic flow from the PFX back to the PFS.

**pfx-return-map** New

Description: string  
1 characters or more.  
A string description of map

Type: Monitor Monitor  
Default: Monitor  
A map type

Mode: Basic Basic  
Default: Basic  
Map mode Basic/Extended

Filter: nonmatch ... x

Ingress: configure x  
Input port(s)  
Selected Ingress : 1-4

Egress: configure  
Output port(s)  
Selected Egress:

Load Balance Criteria: PFX ... x  
Load-balance criteria

Output Load Balance Groups: PFX\_InnerLB\_LBG ... x  
Output load-balance groups

## PFOS/PFX Inner Filtering and Inner Load Balancing Known Limitations

- Only applicable on PFS 5000/7000 devices.
- PFX Load Balancing supports a maximum of 16 ports in Load Balancing Group (LBG) members.
- The PFX device that supports this feature is the Certified PFX with the installed ASI Network Interface Card (NIC).
- The filter expression keyword **extvlan** supports only individual unique IDs; PFOS does not support a range of IDs.
- Packets sent from a Span-Monitor port that has External Device Tagging enabled are not affected by the VLAN Tagging option on the Monitor or Service port(s) to which they are sent. The VLAN tags added by the PFX are always stripped; source-port VLAN tagging is not supported on Span-Monitor ports with External Device Tagging enabled.

**NETSCOUT.**

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](http://www.netscout.com)