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 2009-2021 NETSCOUT Systems, Inc. All rights reserved.
# Table of Contents

**Revision History** ................................................................. 14

**1 Introduction** ...................................................................... 17
  Audience .............................................................................. 17
  Related Documentation .......................................................... 17
  Applicable Hardware Systems .................................................. 17
    PFOS on NETSCOUT Hardware .................................................. 17
    PFOS on Certified Hardware ...................................................... 18
    PFOS on Third-party Qualified Hardware .................................... 18
  PFOS Licensing ....................................................................... 19
    Applicable Hardware Systems .................................................. 20
    License status ..................................................................... 20
    License Notifications ............................................................. 21
    Retrieving new or renewal Full License Keys ................................. 21
      PFS 5000/7000 and PFS 6000 Appliances purchased from NETSCOUT ................................................. 21
      Certified and Qualified Switches ............................................. 21
    License file format ............................................................... 22
    Installing a new license file ..................................................... 22
  Related NETSCOUT Products .................................................... 23
    Hardware Feature Cross-reference .......................................... 24
      PFS 5130-128X Limitations and Configuration Considerations ......................................................... 25
      PFS 7121-64X, PFS 7031-32X, and 7031-56X Limitations and Configuration Considerations .......................... 26

**2 Managing With PFOS** ......................................................... 28
  Configuration File Types ........................................................... 28
  Management Interfaces ............................................................. 28
  Logging in to the Web UI .......................................................... 29
    Change Default Password ...................................................... 30
  License Agreement ................................................................. 30
  Using Secure (HTTPS) Web Browser Connections ........................ 30
<table>
<thead>
<tr>
<th>Failed Login Attempts</th>
<th>Password Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the Web UI</td>
<td></td>
</tr>
<tr>
<td>Toolbar details</td>
<td></td>
</tr>
<tr>
<td>System Status</td>
<td></td>
</tr>
<tr>
<td>System Tab</td>
<td></td>
</tr>
<tr>
<td>Network Tab</td>
<td></td>
</tr>
<tr>
<td>Software Tab</td>
<td></td>
</tr>
<tr>
<td>Clocks Tab</td>
<td></td>
</tr>
<tr>
<td>Configuration Task Flow</td>
<td></td>
</tr>
</tbody>
</table>

3 Configuring the System and Ports

Configuring System Settings

System settings
- Basic Information Settings
- Network Settings
- Source Port VLAN Tagging
- Features
- Syslog
- Trace Log
- nCM
- NMS

Notifications
- Events
- SNMP

Time settings
- Manual time setting
- Port Timestamp
- NTP
- GPS
- PTP

Configuring Access Control

User Access (Roles and Users)

Password Policies
- Password expiration
- Minimum password length and character requirements
- Session Limit

User and IP Lockout Settings

Client IP Lockout

Firewall Rules

Authentication

About PFOS parameters on external AAA servers

Configuring Ports
Port classes ................................................................. 78
Span ports ................................................................... 78
Monitor ports ............................................................... 79
Span-Monitor ports .................................................... 79
Service ports .............................................................. 79
pStack ports ............................................................. 79
Inline Network ports ................................................... 79
Inline Monitor ports ................................................... 79
Using the Port Settings page ........................................ 80
Configure port settings ................................................. 81
Port Settings .............................................................. 81
Port Groups ............................................................... 90
Port group procedures ............................................... 91
Port Group Resource Limits ......................................... 96
4 Base Features and Tasks .............................................. 97
About 200G port groups .............................................. 97
Traffic Maps ............................................................ 98
Traffic Map Processing ............................................... 98
   Example 1 – Traffic Maps with Filtering on Same Input Ports ....................................................... 99
   Example 2 – Traffic Maps with Filtering on Different Input Ports ................................................ 99
Merging Traffic Maps ................................................. 100
About Traffic Maps and Service Ports ......................... 100
About Traffic Maps and Span-Monitor Ports ................ 100
Traffic Map Procedures .............................................. 100
Create a Traffic Map .................................................. 101
Change the Processing Order of Traffic Maps ............... 105
Merge Traffic Maps ................................................... 106
Delete Traffic Maps ................................................... 107
View Traffic Map Status ............................................ 107
View Remote Monitor Group Status .............................. 107
View Output pStack Ports .......................................... 108
Traffic Filtering .......................................................... 109
Forwarding Filters Library .......................................... 109
Filtering Workflow .................................................... 110
Special Filters: Unfiltered and Nonmatch ..................... 112
   Filter Precedence .................................................. 112
Constructing Filter Expressions ................................ 115
Custom Offset Filters .................................................. 116
Match Filter ................................................................ 116
Filter Masks ................................................................ 116
Custom Offset Filters for PFS 7031-32X and PFS 7031-56X .................................................. 117
PFS 7031 Custom Offset Tokens and Offsets ................ 118
PFS 7031 Custom Offset Error Handling ........................ 120
Packet Fields .................................................................................................................. 120
Filter Resource Limits ................................................................................................. 121
  PFS 6000 Series Filter Resource Limits ................................................................. 121
  PFS 5010/7010 Filter Resource Limits ................................................................. 122
  PFS 51xx/71xx Filter Resource Limits .................................................................. 123
  PFS 7031-32X and PFS 7031-56X Filter Resource Limits ..................................... 127
Filter Expression Examples ......................................................................................... 129
Traffic Load Balancing ............................................................................................... 130
 Load Balance Groups and Failover Actions ......................................................... 131
  Load Balance Weighted Calculation ..................................................................... 131
 About Load Balancing and Filtering ........................................................................ 132
 Load Balancing Workflow .......................................................................................... 132
  Define Load Balance Criteria ............................................................................... 132
  Create Load Balance Groups with Ports ............................................................. 133
  Create Load Balance Groups with Tunnels ........................................................ 135
  Delete Load Balance Groups ................................................................................ 137
 Load Balancing Considerations ................................................................................ 137
  Load Balance Criteria ............................................................................................. 137
  Load Balancing with Span-Monitor Ports ............................................................. 138
Trigger Policies ........................................................................................................... 138
 Trigger type settings ................................................................................................. 138
  Link State triggers .................................................................................................. 139
  Health Check Triggers ............................................................................................ 139
  Overflow Drop triggers .......................................................................................... 140
  Bandwidth Utilization triggers ............................................................................... 140
  Combination ("Combo") triggers ............................................................................ 141
 Trigger timer settings ............................................................................................... 141
 Port Selection ............................................................................................................... 142
  Port Selection .......................................................................................................... 142
  Port Group Selection ............................................................................................... 142
  Trigger actions ......................................................................................................... 143
 pfsMesh Option .......................................................................................................... 143
 Trigger Status and Nodes with Conflict ................................................................... 144
 Configuring Trigger Policies ..................................................................................... 145
 Source Port VLAN Tagging ........................................................................................ 146
 Override the System Default Ingress VLAN ID on an Ingress Port ....................... 147
 Configure a Port to Add VLAN Tags to Egress Packets ......................................... 148
 Change the Default TPID or Starting VLAN ID ...................................................... 148
 IP Tunnel Termination ............................................................................................... 149
 Tunnel termination considerations and limitations ............................................... 151
pStack ............................................................................................................................ 152
About pStack protocol versions .................................................. 152
Stacking with other packet flow switches .................................. 152
pfsMesh stacking topologies ................................................... 153
Integrated management interface ............................................ 154
Configuring a pfsMesh .......................................................... 154
Configuring Monitor Output with a pfsMesh .............................. 155
Using the pfsMesh page .......................................................... 160
  Topology ............................................................................. 160
  Remote Monitor Groups ...................................................... 161
  Remote Trigger .................................................................... 161
  pStackMap .......................................................................... 161
  VLAN ................................................................................... 162
About input port VLAN IDs with pfsMesh .................................. 162
Optimal path forwarding ......................................................... 163
Load spreading in a pfsMesh .................................................... 164
  Technical considerations for load spreading ......................... 164
5 Enhanced Port Features ....................................................... 165
  PFS 6000 Enhanced Port Features ........................................ 165
    Packet De-duplication ....................................................... 165
    Port and Time Stamping ................................................... 167
      Port Stamping ............................................................... 167
      Time Stamping ............................................................. 168
    About Time Stamp Synchronization Sources ....................... 170
    About Time Stamp Accuracy ............................................ 170
    Using Port Stamping and Time Stamping Together ............... 171
    Protocol De-encapsulation and Stripping ........................... 172
      ERSSPAN, GRE, GTP, MPLS-L2, and NVGRE De-encapsulation 172
      MPLS-L3, VLAN and VN Tag Stripping ............................. 172
      Generic Stripping .......................................................... 173
      Stripping and De-encapsulation Details ........................... 173
      Stripping Library and Protocol Stripping ......................... 176
    VLAN and VN Tag Stripping .............................................. 180
    Conditional Packet Slicing ................................................ 182
      About Conditional Slicing and Packet Sizes ...................... 182
    Conditional Packet Masking ............................................. 186
    Extended Load Balancing .................................................. 190
    Extended Load Balancing Workflow ................................... 190
    Extended Load Balancing Considerations ........................... 193
  PFS 5000/7000 Enhanced Port Features ................................. 194
    Standard Stripping .......................................................... 194
Standard Stripping Port Class Compatibility ............................................. 195
Configure Standard VLAN Tag Stripping ............................................. 195
Configure Standard Vn Tag Stripping ..................................................... 196
Configure Standard VXLAN Stripping ................................................... 196
Configure Standard MPLS Stripping ....................................................... 198
Configure Standard L2GRE Stripping .................................................... 203
GRE Tunnel Origination/Termination Support ....................................... 205
Configuring GRE Tunnel Origination/Termination ................................. 206
Use Case 1 - L2GRE Tunnel between Two PFS 7000 Devices ................ 206
Use Case 2 - L2GRE Tunnel from PFS to vSTREAMs ............................... 212
Use Case 3 - Building pfsMesh over L2GRE Tunnel ............................... 217
Tunnel Statistics and Status ................................................................. 221
L2GRE Origination/Termination Limitations .......................................... 224
VXLAN Tunnel Origination/Termination Support .................................... 225
Configuring VXLAN Tunnel Origination/Termination .............................. 225
VXLAN Tunnel Origination/Termination Limitations .................................. 233
Neighbor Discovery Using LLDP .......................................................... 234
LLDP Ethernet Frame Structure .......................................................... 234
Transmitted TLVs .................................................................................. 235
Enabling LLDP Packet Transmit/Receive .............................................. 236
Viewing PFS LLDP Neighbors ............................................................... 237

6 Inline Traffic ......................................................................................... 238
Tool Chain - Simple Mode vs. Advanced Mode ...................................... 239
Inline Traffic Workflow .......................................................................... 239
Simple Tool Chaining ............................................................................ 240
Simple Tool Chain Use Case .................................................................. 240
Prerequisites ......................................................................................... 241
Create a Simple Tool Chain ................................................................. 244
Advanced Tool Chaining ....................................................................... 245
Advanced Tool Chain Use Case ............................................................. 245
Prerequisites ......................................................................................... 246
Create an Advanced Tool Chain ........................................................... 248
Inline Traffic Maps ................................................................................. 252
Create an Inline Monitor Traffic Map ..................................................... 252
Tool Chain Resource Limits and Considerations .................................... 254
LinkSafe ............................................................................................... 254
About interconnected LinkSafe ports ................................................... 256
Health Check Profiles ........................................................................... 256
Health Check Configuration Parameters .............................................. 257
Transmit Rate ......................................................................................... 257
Destination MAC Address ...................................................................... 257
Payload ................................................................................................. 258
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Expression</td>
<td>258</td>
</tr>
<tr>
<td>Wait Time</td>
<td>258</td>
</tr>
<tr>
<td>Health Check Considerations</td>
<td>258</td>
</tr>
<tr>
<td>Create a Health Check</td>
<td>258</td>
</tr>
<tr>
<td>Delete Health Checks</td>
<td>259</td>
</tr>
<tr>
<td>PowerSafe</td>
<td>259</td>
</tr>
<tr>
<td>External PowerSafe TAP 3296 Components</td>
<td>260</td>
</tr>
<tr>
<td>Understanding PowerSafe</td>
<td>261</td>
</tr>
<tr>
<td>Normal Operation</td>
<td>261</td>
</tr>
<tr>
<td>Heartbeat Failure Using Poweroff Bypass Mode (Default)</td>
<td>262</td>
</tr>
<tr>
<td>Power Failure Using Poweroff Forward Mode</td>
<td>263</td>
</tr>
<tr>
<td>Heartbeat Failure Using Poweroff Block Mode</td>
<td>264</td>
</tr>
<tr>
<td>Heartbeat Failure Using Poweroff Impairdown Mode</td>
<td>264</td>
</tr>
<tr>
<td>Enabling the PowerSafe Feature</td>
<td>265</td>
</tr>
<tr>
<td>Viewing PowerSafe Hardware Details</td>
<td>265</td>
</tr>
<tr>
<td>Configuring PowerSafe Settings</td>
<td>266</td>
</tr>
<tr>
<td>Poweroff Mode</td>
<td>266</td>
</tr>
<tr>
<td>PowerSafe Manual Mode</td>
<td>267</td>
</tr>
<tr>
<td>PowerSafe Inline Network Port Group Settings</td>
<td>267</td>
</tr>
<tr>
<td>7 Maintenance</td>
<td>268</td>
</tr>
<tr>
<td>Uploading Files</td>
<td>268</td>
</tr>
<tr>
<td>Downloading Files</td>
<td>269</td>
</tr>
<tr>
<td>Saving and Loading Configurations</td>
<td>271</td>
</tr>
<tr>
<td>Maintaining Core Files</td>
<td>273</td>
</tr>
<tr>
<td>Maintaining Log Files</td>
<td>273</td>
</tr>
<tr>
<td>Maintaining Certificate Files</td>
<td>275</td>
</tr>
<tr>
<td>Installing Certificate Files</td>
<td>275</td>
</tr>
<tr>
<td>Upload a Certificate File</td>
<td>275</td>
</tr>
<tr>
<td>View, Install, or Delete Certificate Files</td>
<td>276</td>
</tr>
<tr>
<td>Maintaining SSH Public Key Files</td>
<td>277</td>
</tr>
<tr>
<td>Maintaining NTP Key Files</td>
<td>278</td>
</tr>
<tr>
<td>NTP Key File Format</td>
<td>278</td>
</tr>
<tr>
<td>Upload an NTP Key File</td>
<td>278</td>
</tr>
<tr>
<td>Upgrading PFOS</td>
<td>279</td>
</tr>
<tr>
<td>Reboots PFOS</td>
<td>279</td>
</tr>
<tr>
<td>Managing Redundancy</td>
<td>280</td>
</tr>
<tr>
<td>Configure management IP addresses</td>
<td>280</td>
</tr>
<tr>
<td>Switch current management module</td>
<td>281</td>
</tr>
<tr>
<td>Uploading files to each management module</td>
<td>281</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>View management module status</td>
<td>282</td>
</tr>
<tr>
<td>On the front panel</td>
<td>282</td>
</tr>
<tr>
<td>On the rear of the chassis</td>
<td>283</td>
</tr>
<tr>
<td>In the Web UI</td>
<td>284</td>
</tr>
<tr>
<td>About licensing and redundancy</td>
<td>284</td>
</tr>
<tr>
<td>Redundancy considerations and limitations</td>
<td>285</td>
</tr>
<tr>
<td><strong>8 Diagnostics</strong></td>
<td>286</td>
</tr>
<tr>
<td>System Status</td>
<td>286</td>
</tr>
<tr>
<td>Statistics</td>
<td>287</td>
</tr>
<tr>
<td>Network statistics</td>
<td>287</td>
</tr>
<tr>
<td>Deduplication statistics</td>
<td>288</td>
</tr>
<tr>
<td>Flow statistics</td>
<td>289</td>
</tr>
<tr>
<td>Control packets statistics</td>
<td>290</td>
</tr>
<tr>
<td>Event Notifications</td>
<td>291</td>
</tr>
<tr>
<td>Syslog history</td>
<td>291</td>
</tr>
<tr>
<td>Alarms</td>
<td>292</td>
</tr>
<tr>
<td>Hardware Information</td>
<td>293</td>
</tr>
<tr>
<td>SNMP MIBs</td>
<td>295</td>
</tr>
<tr>
<td>SNMP configuration support</td>
<td>296</td>
</tr>
<tr>
<td>nGeniusONE PFS Monitoring</td>
<td>296</td>
</tr>
<tr>
<td>Consolidated Traffic Monitor</td>
<td>297</td>
</tr>
<tr>
<td>Grid</td>
<td>297</td>
</tr>
<tr>
<td>PFS Monitor</td>
<td>298</td>
</tr>
<tr>
<td>Syslog Messages</td>
<td>298</td>
</tr>
<tr>
<td>User</td>
<td>298</td>
</tr>
<tr>
<td>Configuration</td>
<td>299</td>
</tr>
<tr>
<td>Chassis</td>
<td>305</td>
</tr>
<tr>
<td><strong>9 Frequently Asked Questions</strong></td>
<td>309</td>
</tr>
<tr>
<td>A Packet Fields in Filter Expressions</td>
<td>311</td>
</tr>
<tr>
<td>B Configuring SNMP</td>
<td>316</td>
</tr>
<tr>
<td>Configuring SNMPv1 or SNMPv2c</td>
<td>316</td>
</tr>
<tr>
<td>Enable SNMP and Configure SNMP Versions</td>
<td>317</td>
</tr>
<tr>
<td>Create a New SNMP Community (Optional)</td>
<td>317</td>
</tr>
<tr>
<td>Add Security Name to View-Based Access Control Model (Optional)</td>
<td>317</td>
</tr>
<tr>
<td>Grant Access Rights to the VACM Group</td>
<td>318</td>
</tr>
<tr>
<td>Add New Security Models</td>
<td>319</td>
</tr>
<tr>
<td>Verify SNMP Configuration</td>
<td>320</td>
</tr>
<tr>
<td>Limit SNMP Access Rights</td>
<td>321</td>
</tr>
</tbody>
</table>
Verify SNMPSet by Using the New Access Configuration ........................................ 322
Configuring SNMPv3  ........................................................................................... 322
Create a User-Based Security Model (USM) with Authentication and Privacy .......................... 323
Add the USM User to VACM Group .......................................................................... 323
Verify Using New USM User “v3user” without Password ............................................. 324
Request Authentication and Privacy Password for USM ................................................. 324
Verify Using New USM User “v3user” without Password ............................................. 325
Limit Access Rights for SNMPSet .............................................................................. 326
Verify SNMPSet by Using the New Access Configuration ............................................ 327
Configuring SNMP Notification (Traps) .................................................................... 327
SNMP Notify Tags ..................................................................................................... 328
Add Trap Receiver IP Address to Target Table ............................................................. 328
SNMP v2c Receiver Example ..................................................................................... 329
SNMP v3 Receiver Example ....................................................................................... 329
Enable SNMP Traps .................................................................................................... 330
Notifications>SNMP>Traps ......................................................................................... 330
Notifications>Events ................................................................................................. 331
Verify SNMP v2c Trap is Received by Third-Party SNMP Trap Receiver ....................... 332

C SNMP MIB and Trap Definitions ........................................................................ 333
Traps/Notifications .................................................................................................... 333
Interfaces MIB Traps ................................................................................................. 333
VSS Enterprise MIB Traps ......................................................................................... 334
SNMPv2-MIB Traps .................................................................................................... 339
Packet/Port Statistics ............................................................................................... 339
Interfaces MIB Stats .................................................................................................. 339
 iNumber .................................................................................................................... 340
 iTable ....................................................................................................................... 340
 ifXTable .................................................................................................................... 341
 RMON-MIB (RFC 2819) ............................................................................................ 343
 etherStatsTable ....................................................................................................... 343
 HC-RMON-MIB (RFC 3273) ..................................................................................... 345
 etherStatsHighCapacityTable ................................................................................... 345
System Information .................................................................................................... 347
Community MIB ....................................................................................................... 347
 RFC 3584 ................................................................................................................. 347
View-based Access Control Model (VACM) MIB ...................................................... 348
 RFC 3415 ................................................................................................................. 348
User-based Security Model (USM) MIB ..................................................................... 349
 RFC 3414 ................................................................................................................. 349
Target MIB .................................................................................................................. 351
 RFC 3413 ................................................................................................................. 351
<table>
<thead>
<tr>
<th>MIB</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification MIB</td>
<td>352</td>
</tr>
<tr>
<td>RFC 3413</td>
<td>352</td>
</tr>
<tr>
<td>NTCT-PFS-HEALTH-MIB</td>
<td>352</td>
</tr>
<tr>
<td>nphPfsHlthStatus</td>
<td>352</td>
</tr>
<tr>
<td>nphInterfaceTable</td>
<td>353</td>
</tr>
<tr>
<td>nphFlowMapTable</td>
<td>353</td>
</tr>
<tr>
<td>nphFlowInterfaceTable</td>
<td>353</td>
</tr>
<tr>
<td>nphFlowLbgTable</td>
<td>354</td>
</tr>
<tr>
<td>nphFilterStatsTable</td>
<td>354</td>
</tr>
<tr>
<td>nphlfExtTable</td>
<td>354</td>
</tr>
<tr>
<td>VSS-SYSTEM-MIB</td>
<td>363</td>
</tr>
<tr>
<td>vsTemperatureStatusTable</td>
<td>363</td>
</tr>
<tr>
<td>vsNotifsControl</td>
<td>363</td>
</tr>
</tbody>
</table>
## Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2021</td>
<td>B</td>
<td>PFOS 6.0.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated <a href="#">User and IP Lockout Settings</a> to clarify User Lockout Disable and IP Lockout Disable options.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated <a href="#">PFS 51xx/71xx Filter Resource Limits</a></td>
</tr>
<tr>
<td>April 2021</td>
<td>A</td>
<td>PFOS 6.0.3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- VLAN filter ranges are now supported in PFOS. Refer to <a href="#">vlan</a> in Packet Fields in Filter Expressions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- PFOS now supports two new third-party Qualified hardware models PFS 7031-32X (Dell S5232F-ON) and PFS 7031-56X (Dell S5248F-ON). Refer to the following sections for details about these new models:</td>
</tr>
<tr>
<td>March 2021</td>
<td>A</td>
<td>PFOS 6.0.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- PFOS now supports a new third-party <a href="#">Qualified hardware</a> model PFS 7121-64X (Dell Z9264F-ON).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- You can disable the User Lockout and IP Lockout features so there are no limits to the number of failed login attempts. See <a href="#">User and IP Lockout Settings</a> for details.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- You can now configure the number of failed user login attempts and the number of failed IP address login attempts that PFOS allows before a user account is locked out. See <a href="#">User and IP Lockout Settings</a> for details.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- PFOS now supports <a href="#">sending system logs to a remote server over an encrypted SSH tunnel</a>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- PFOS now supports uploading certificate authority files. Refer to <a href="#">Maintaining Certificate Files</a>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Other Documentation Updates for 6.0.2</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Clarified and updated <a href="#">L2GRE Origination/Termination Limitations</a> and <a href="#">VXLAN Tunnel Origination/Termination Limitations</a></td>
</tr>
<tr>
<td>Month</td>
<td>Version</td>
<td>Changes</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>January 2021</td>
<td>B</td>
<td><strong>PFOS 6.0.1</strong>&lt;br&gt;  - Updated Traffic Filtering <a href="#">TCP-UDP Port Range support statement</a>:&lt;br&gt;    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.&lt;br&gt;  - Corrected <a href="#">bi-directional filter examples</a>, replacing &quot;dst&quot; with &quot;dest&quot;</td>
</tr>
</tbody>
</table>
| December 2020 | A       | **PFOS 6.0.1**<br>  - NS-76604 - Updated PFOS per California law mandating software must prompt user to change initial (factory) password. See [Change Default Password](#) for details.<br>**PFOS 6.0.0**<br>  - PFOS 6.0 and later will not support the PFS Fabric Manager EMS. The PFOS Web UI will be the only Web UI available on the PFS. PFS Fabric Manager 6.0 and later no longer includes the EMS component.<br>  - You can now configure [Idle Timeouts](#) for the Web UI and CLI sessions.<br>  - PFOS has enhanced support of certificates:<br>    - Added support for Certificate Revocation List (CRL)<br>    - Added support for generating Certificate Signing Requests (CSRs)
<table>
<thead>
<tr>
<th>December 2020</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PFOS 6.0.0 (Continued)</strong></td>
<td></td>
</tr>
<tr>
<td>• New <a href="#">Common Criteria Mode</a> for PFS 5000/7000s</td>
<td></td>
</tr>
<tr>
<td>• On PFS 7000s, PFOS supports <a href="#">neighbor discovery using Link Layer Discovery Protocol (LLDP)</a>. Neighbor discovery allows devices to advertise device information to their directly connected peers/neighbors.</td>
<td></td>
</tr>
<tr>
<td>• PFOS now supports firewall rules which control how the PFOS firewall protects your PFS from malicious programs and unauthorized access. The <a href="#">Firewall Rules</a> feature enables you to control system access to/from certain IPs.</td>
<td></td>
</tr>
<tr>
<td>• Powersafe enhancements include:</td>
<td></td>
</tr>
<tr>
<td>• PFOS supports <a href="#">USB hot swap</a> for the External PowerSafe TAP 3296.</td>
<td></td>
</tr>
<tr>
<td>• New <a href="#">Manual Mode</a> options</td>
<td></td>
</tr>
<tr>
<td>• New <a href="#">Poweroff Mode</a> options</td>
<td></td>
</tr>
<tr>
<td>• New <a href="#">Inline Network Ports</a> option</td>
<td></td>
</tr>
<tr>
<td>• Traffic Filtering has been enhanced to support:</td>
<td></td>
</tr>
<tr>
<td>• Configuring MAC, IP (v4 and v6) and L4 port filters as bidirectional.</td>
<td></td>
</tr>
<tr>
<td>• Entering IPv4 and IPv6 addresses and masks in IP/prefix length format</td>
<td></td>
</tr>
<tr>
<td>• Total configurable TCP-UDP port ranges is no longer limited to 32 for PFS 5000/7000s</td>
<td></td>
</tr>
<tr>
<td>• The maximum number of supported Monitor and Network Port Groups has increased from 16 to 64. See <a href="#">Port Group Resource Limits</a> for details.</td>
<td></td>
</tr>
<tr>
<td>• New <a href="#">System&gt;NMS</a> tab.</td>
<td></td>
</tr>
<tr>
<td>• PFOS supports new SSH key authentication commands, including SSH key generation. Refer to the <a href="#">PFOS 6.X CLI Reference Guide</a>.</td>
<td></td>
</tr>
</tbody>
</table>

**Other Documentation Updates for 6.0.0**

- Updated [Source Port VLAN Tagging](#) to clarify procedures.
- Added clarification to [Client IP Lockout](#)
1 Introduction

This document describes the system software and graphical user interface of the NETSCOUT SYSTEMS, INC. (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

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.

- **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).

For product warranty information, go to 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.

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 for PFOS Licensing licensing details.

<table>
<thead>
<tr>
<th>Vendor Model</th>
<th>NETSCOUT Model Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PFS 5000 Series</td>
</tr>
<tr>
<td>Edgecore Networks AS5812-54X</td>
<td>PFS 5010</td>
</tr>
<tr>
<td>Edgecore Networks AS7712-32X</td>
<td>PFS 5100</td>
</tr>
<tr>
<td>Edgecore Networks AS7312-54XS</td>
<td>PFS 5110</td>
</tr>
<tr>
<td>Edgecore Networks AS7816-64X</td>
<td>PFS 5120</td>
</tr>
<tr>
<td>Edgecore Networks Minipack AS8000</td>
<td>PFS 5130-128X</td>
</tr>
<tr>
<td>Dell S5048-ON</td>
<td>PFS 5111</td>
</tr>
<tr>
<td>Dell Z9100-ON</td>
<td>PFS 5101</td>
</tr>
<tr>
<td>Dell Z9264F-ON</td>
<td>N/A</td>
</tr>
<tr>
<td>Dell S5232F-ON</td>
<td>N/A</td>
</tr>
<tr>
<td>Dell S5248F-ON</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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 limitations and configuration considerations for the PFS 5130-128X and the PFS 7121-64X, PFS 7031-56X, and PFS 7031-32X.
PFOS Licensing

The following table describes available licensing.

<table>
<thead>
<tr>
<th>License</th>
<th>License Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Support License</strong></td>
<td><strong>Full</strong></td>
<td>Enables full PFOS 5000 base feature 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. <strong>Note:</strong> The PFS 5010 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.</td>
</tr>
<tr>
<td><strong>Trial</strong></td>
<td></td>
<td>Enables PFOS base feature functionality for 90 days. Upon expiration, <strong>PFOS automatically clears its configuration</strong> and no further configuration or software upgrades can be performed until a Full Support License is installed. PFS 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.</td>
</tr>
</tbody>
</table>
| **PFS 7000 License**     | **Full**        | Enables full PFOS 7000 functionality including:  
- MPLS Stripping  
- L2GRE Stripping  
- Inline tool chain  
- External PowerSafe TAP configuration  
- GRE Tunnel Origination/Termination Support  
- VXLAN Tunnel Origination/Termination Support  
- Timestamping (PFS 7120, PFS 7031-56X, PFS 7031-32X)  
- Tunnel Load Balancing  
- Neighbor Discovery Using LLDP  
PFOS 7000 functionality is subject to the normal constraints of the hardware on which it is running, until the license expiration date. |
| **Trial**                |                 | Enables advanced PFOS functionality for 90 days. Upon expiration, **PFOS automatically clears any advanced feature configuration**; standard configuration is not cleared. No further configuration of advanced features can be performed until a Full Advanced license is installed. PFS 7000 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. |

The following table lists the type and expiration of licenses that come with (or are automatically installed on) various NETSCOUT PFS.
<table>
<thead>
<tr>
<th>Applicable Hardware Systems</th>
<th>License</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PFOS pre-installed?</td>
</tr>
<tr>
<td>PFS 6000-series Appliances purchased from NETSCOUT</td>
<td>5.5 or later</td>
</tr>
<tr>
<td></td>
<td>5.3 or earlier</td>
</tr>
<tr>
<td>PFS 5000-series Appliances purchased from NETSCOUT</td>
<td>5.5 or later</td>
</tr>
<tr>
<td></td>
<td>5.3 or earlier</td>
</tr>
<tr>
<td>PFS 7000-series Appliances purchased from NETSCOUT</td>
<td>5.5 or later</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Certified switches</td>
<td>Yes</td>
<td>Trial(1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>90 days</td>
</tr>
<tr>
<td>Qualified switches</td>
<td>No</td>
<td>Trial(2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>90 days</td>
</tr>
</tbody>
</table>

**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. For PFS 7121-64X, PFS 7031-56X, PFS 7031-56X, the 7000 license is mandatory.

**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.
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):

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

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, email NETSCOUT Technical Support at support@netscout.com 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, email NETSCOUT Technical Support at support@netscout.com 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 0229dd8b85f4af37b8a9bdbc65a40e6174f48dfc2661ea87e51e4fc74ccf53
cc:37:ab:bd:46:67 ed7d215ba04df4a38340d92daf9d5f4a626d7a1cfdf8320a56e88769320dee

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. Prior to upload, verify your system time is accurate, or your license upload will fail. For a more accurate and reliable time, ensure that an NTP server is defined correctly.

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.
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.

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>
<thead>
<tr>
<th>Feature</th>
<th>PFS 5000 Series</th>
<th>PFS 7000 Series</th>
<th>PFS 6000 Series</th>
<th>COTS hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management interfaces</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web UI</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CLI</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SNMP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NETCONF</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Syslog</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Load balancing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flow-aware L2-L4 load balancing</td>
<td>Yes²</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Encapsulated (inner L2-L4) load balancing</td>
<td>No</td>
<td>No</td>
<td>Yes¹</td>
<td>No</td>
</tr>
<tr>
<td>Failover actions: Rebalance, redistribute, drop</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Failover actions: Weighted</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Tunnel</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Traffic filtering</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L2-L4 filters</td>
<td>Yes²</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Custom offset/user-defined filters</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Filter service ports</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Extended microburst protection (HDBB)</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Deduplication</td>
<td>Yes³</td>
<td>Yes³</td>
<td>Yes¹</td>
<td>Yes³</td>
</tr>
<tr>
<td>IP tunnel termination¹⁴</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NetFlow generation</td>
<td>Yes³</td>
<td>Yes³</td>
<td>Yes³</td>
<td>Yes³</td>
</tr>
<tr>
<td>Packet modification</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protocol stripping / de-encapsulation</td>
<td>Yes⁵</td>
<td>Yes⁵</td>
<td>Yes¹</td>
<td>Yes⁵</td>
</tr>
<tr>
<td>Payload modification: Conditional slicing, Conditional masking</td>
<td>Yes³</td>
<td>Yes³</td>
<td>Yes¹</td>
<td>Yes³</td>
</tr>
<tr>
<td>Port stamping</td>
<td>No</td>
<td>No</td>
<td>Yes¹</td>
<td>No</td>
</tr>
<tr>
<td>Time stamping</td>
<td>No</td>
<td>Yes</td>
<td>Yes¹</td>
<td>Yes</td>
</tr>
<tr>
<td>VLAN tag, VN-tag, and VXLAN stripping</td>
<td>Yes²</td>
<td>Yes⁷</td>
<td>Yes¹</td>
<td>Yes</td>
</tr>
<tr>
<td>MPLS stripping</td>
<td>No</td>
<td>Yes</td>
<td>Yes¹</td>
<td>Yes</td>
</tr>
<tr>
<td>L2GRE stripping</td>
<td>No</td>
<td>Yes</td>
<td>Yes¹</td>
<td>Yes</td>
</tr>
<tr>
<td>VLAN Tagging</td>
<td>Yes²</td>
<td>Yes</td>
<td>Yes¹</td>
<td>Yes</td>
</tr>
<tr>
<td>Inline traffic and tool chains</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>External PowerSafe TAP (EPT)</td>
<td>No</td>
<td>Yes</td>
<td>No⁸</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 1.1 - PFOS 6.x Hardware Feature Cross-Reference (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>PFS 5000 Series</th>
<th>PFS 7000 Series</th>
<th>PFS 6000 Series</th>
<th>COTS hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Discovery Using LLDP</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>GRE Encapsulation/ Decapsulation (Tunnel origination/termination)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>VXLAN Encapsulation/ Decapsulation (Tunnel origination/termination)</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Clock Sources</td>
<td>Local clock</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>NTP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>GPS</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>PTP</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>1PPS</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Locator LED</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>LCD display</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>pfsMesh</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Notes:

1. Available on systems with one or more 40SadvR line cards.
2. The PFS 5130-128X provides limited support; see PFS 5130-128X Limitations and Configuration Considerations for details.
3. Available with the use of PFX.
4. 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.
5. Available with the use of PFX; refer to PFX documentation for information on supported protocols.
6. Only available on PFS 7120, PFS 7031-56X, and the PFS 7031-32X.
7. The PFS 7031-56X and PFS 7031-32X do not support VN Tag Stripping; see PFS 7121-64X, PFS 7031-32X, and 7031-56X Limitations and Configuration Considerations.
8. Not supported on PFS 6010 or original revision of PFS 6002. Is supported on new revision of PFS 6002 only.

PFS 5130-128X Limitations and Configuration Considerations

- **FEC** is disabled by default (except PFS 5130-128X), which offers the lowest latency delay. FEC is typically disabled with single mode (LR) connections. FEC at PFS 5130-128X is not configurable, it is always enabled. Therefore, PFS 5130-128X does not support 100G BiDi because it requires FEC to be disabled.
- PFS 5130-128X can support **FEC RS-FEC mode (CL91)** only.
**VLAN Tagging** is not configurable but always enabled at PFS 5130-128X; packets egressing the PFS 5130-128X device will always be tagged with the Default or “User-Defined” VID configured at Source port VLAN. However, if packets are from a remote device over pfsMesh and they egress at the PFS 5130-128X, they will always be tagged with the default VID of the remote source port.

- The PFS 5130-128X device does not support the following stripping functions:
  - **Vn Tag stripping**
  - **VLAN Tag Stripping**
  - **VXLAN Tag stripping**

- PFS 5130-128X supports QSFP+, 40G BiDi Tx/Rx, 40G BiDi Rx and QSFP28 in all ports. These ports may be configured for operation at 40G and 100G, however the port speed is a common setting for each group of four sequential ports, starting at the first port of each line card (for example, ports 1-1 to 1-4 must all have the same speed regardless of port class even if service port). 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 enforce all 4 ports to be the same speed).

- When replacing transceivers on the PFS 5130-128X, PFOS can require up to 20 seconds to detect removal. To avoid error, wait until the UI confirms removal prior to inserting a new transceiver.

- **Map profile** is not configurable at PFS 5130-128X devices as only the Legacy mode can be supported (No SIP or DIP mode).

- The PFS 5130-128X does not support filter expressions that include VLAN ID, TPID, and priority field in the VLAN Tag.

- The PFS 5130-128X supports a maximum of 510 traffic maps.

- PFS 5130-128X does not support any encapsulation, so load balance can only be based on L2 or L3 or MPLS label at outer header of the ingress encapsulated packets.

- PFS 5130-128X does not support line card hot swap.

**PFS 7121-64X, PFS 7031-32X, and 7031-56X Limitations and Configuration Considerations**

- The PFS 7031-32X and 7121-64X systems require 26 seconds to initialize each transceiver while the PFS 7031-56X requires 12 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:

<table>
<thead>
<tr>
<th>Model</th>
<th>Calculation</th>
<th>Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7031-32X</td>
<td>26 seconds * 32 = 832 seconds = 14 minutes</td>
<td></td>
</tr>
<tr>
<td>7031-56X</td>
<td>12 seconds * 56 = 672 seconds = 11 minutes</td>
<td></td>
</tr>
<tr>
<td>7121-64X</td>
<td>26 seconds * 64 = 1,664 seconds = 28 minutes</td>
<td></td>
</tr>
</tbody>
</table>

- For PFS 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.
The PFS 7031-32X and PFS 7031-56X devices do not support Vn Tag stripping.

PFS 7031-32X and PFS 7031-56X devices require specific Custom Offset Filter configurations that are only compatible with PFS 7031 devices.

PFS 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).
Managing With PFOS

This chapter provides information about managing PFOS.

Contents

Configuration File Types
Management Interfaces
Logging in to the Web UI
Using the Web UI
Configuration Task Flow

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 interfaces are available to manage PFOS:

- **CLI**: Command-based user interface. You can use the CLI to read and write most configuration and status parameters. See the PFOS 6.x CLI Reference Guide.
- **Web UI**: Web user interface, described in this guide.

**Note**: The nGenius Performance Manager currently cannot be used to manage PFOS devices.
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 or TACACS+, 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 “System-wide features” in Configuring System Settings.

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 login attempts.
PFOS manages failed login attempts as described below:

- **User tries to log in with a 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.

- **User tries to log in with a username that does not exist.** 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 interface. A user can continue to login successfully using a non-compliant password.

- Imported users. User information imported through File Management that contains non-compliant passwords is not checked. When the imported users attempt to login to the CLI or Web UI, they will be prompted to update their passwords.
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” (next section).
- **Side menu:** Access the status, configuration, and administration pages.
- **Main panel:** View and configure content.

**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, all changes after those in the rollback file are removed from the system.

**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:** On systems that support this feature, turns on the LOC indicator on the front of the system.

**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.

**Logout:** Logs you 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.
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.

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 Audience), management module status, data and system disk usage, temperature, system status, redundancy status, and platform.
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.

**Software Tab**

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

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

<table>
<thead>
<tr>
<th>System</th>
<th>Date/Time</th>
<th>Boot Time</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Fri, 03 Feb 2019 16:17:09 GMT</td>
<td>Fri, 03 Feb 2019 20:40:45 GMT</td>
<td>6 days, 19 hours, 33 mins and 4 seconds</td>
</tr>
<tr>
<td></td>
<td>Fri, 03 Feb 2019 20:40:45 GMT</td>
<td>Fri, 03 Feb 2019 23:39:40 GMT</td>
<td>6 days, 19 hours, 55 mins and 4 seconds</td>
</tr>
</tbody>
</table>

Configuration Task Flow

Follow this task flow to set up and configure PFOS:

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 System Settings.
4. Configure filtering, as needed. See Traffic Filtering.
5. Configure load balancing, as needed. See Traffic Load Balancing.

After these steps are complete, traffic is automatically forwarded through the system according to the specified conditions.
This chapter describes how to configure PFOS and the physical ports on your system. Before you continue, review Configuration Task Flow.

Contents

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

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

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

- Basic Information Settings
- Network Settings
- Source Port VLAN Tagging
- 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 email address.
- Location - define the chassis location (such as city, state)
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/netmask 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.
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.

DHCP on PFS 5000/7000 Series

On a PFS 5000/7000 Series system, you can use this page to enable 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.

By default, DHCP is disabled.
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.
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**
- **MPLS**
- **MPLS Max Labels**
- **MPLS Cleanup Mode**
- **Common Criteria Mode**
- **Access Management**

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

**FIPS mode**

This feature is available on PFS 5000/7000 and 6000 Series. To enable or disable FIPS mode, either select or deselect the **FIPS Mode** checkbox. When operating in FIPS mode, PFOS uses only
cryptographic algorithms that comply with the Federal Information Processing Standard. 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 a 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Normalization</th>
<th>Normalization</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCM_HASH_FIELD_CONFIG_CRC16XOR8</td>
<td>Upper 8 bits of BISYNC CRC16 and 8 bit XOR8</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>BCM_HASH_FIELD_CONFIG_CRC16XOR4</td>
<td>Upper 8 bits of BISYNC CRC16 and 8 bit XOR4</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>BCM_HASH_FIELD_CONFIG_CRC16XOR2</td>
<td>Upper 8 bits of BISYNC CRC16 and 8 bit XOR2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>BCM_HASH_FIELD_CONFIG_CRC16XOR1</td>
<td>Upper 8 bits of BISYNC CRC16 and 8 bit XOR1</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>BCM_HASH_FIELD_CONFIG_CRC16</td>
<td>16 bit CRC16</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>BCM_HASH_FIELD_CONFIG_XOR16</td>
<td>16 bit XOR (Default)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>BCM_HASH_FIELD_CONFIG_CRC16CCITT</td>
<td>16 bit CRC16 calculated using CCITT polynomial</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>BCM_HASH_FIELD_CONFIG_CRC32LO</td>
<td>Lower 16 bit of computed CRC32</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>BCM_HASH_FIELD_CONFIG_CRC32HI</td>
<td>Higher 16 bit of computed CRC32</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>BCM_HASH_FIELD_CONFIG_CRC32_ETH_LO</td>
<td>Lower 16 bit of Ethernet CRC32</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>BCM_HASH_FIELD_CONFIG_CRC32_ETH_HI</td>
<td>Higher 16 bit of Ethernet CRC32</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>BCM_HASH_FIELD_CONFIG_CRC32 KOOPMAN_LO</td>
<td>Lower 16 bit of Koopman CRC32</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
### Tunnel

This Tunnel option enables/disables tunnel features and functionality (such as [IP tunnel termination](https://example.com) and [GRE Tunnel Origination/Termination Support](https://example.com)).

- 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.

In the default Auto mode, PFOS automatically adjusts the mode depending on the configured forwarding filters.

**Note:** Map profile is not configurable at PFS 5130-128X devices as only the Legacy mode can be supported (No SIP or DIP mode).

<table>
<thead>
<tr>
<th>SIP mode</th>
<th>The default mode, used when the number of source IP address filters is less than 1025.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIP mode</td>
<td>Used when the number of source IP address filters is greater than 1024 and the number of destination IP address filters is less than 1025.</td>
</tr>
<tr>
<td>Legacy mode</td>
<td>Used when the number of source and destination IP address filters are both greater than 1025.</td>
</tr>
</tbody>
</table>

SIP and DIP mode allow the maximum number of filter resources (as described in [Filter resource limits](https://example.com)) but suffer from incorrect matching when two or more source or destination IP address filters, respectively, have overlapping ranges.

Consider the following traffic map configuration:

<table>
<thead>
<tr>
<th>Map</th>
<th>Filter</th>
<th>Egress port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.1.0.0/16 and TCP port 80</td>
<td>1-10</td>
</tr>
<tr>
<td>2</td>
<td>10.1.1.0/24 and TCP port 443</td>
<td>1-11</td>
</tr>
</tbody>
</table>
With these traffic maps in SIP or DIP mode a packet with IP source or destination address (respectively) 10.1.1.2 and TCP port 443 will mistakenly be dropped, even if the traffic maps use different ingress ports. This happens because in SIP or DIP mode the IP address portion of the filter is evaluated first, matching traffic map 1; since TCP port 443 does not match the second clause of map 1’s filter, the packet is dropped. To prevent this the filters can be changed so there is no overlap or the Map Profile mode can be changed to Legacy. Note that traffic map ordering does not affect this behavior.

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.

**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. The Common Criteria mode enables SSH session rekeying functionality. An SSH session will rekey after an hour or 1 G of data transferred if Common Criteria mode is enabled. When enabled, you cannot log in to PFOS CLI using TACACS or RADIUS.

![Common Criteria Mode](image)

**Warning!!!** All the active CLI sessions will be cleared automatically upon confirmation for common criteria mode change to take effect.

### Access Management

Access Management enables you to control the following settings:

- **Management Interfaces**
- **Front Panel**
- **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 830 for NETCONF over TCP (which is non-standardized) and 832 for NETCONF over SSH.

#### Front Panel

This option is only available on the PFS 6000 Series. It enables or disables the LCD panel on the front of the system.
**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.
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 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.
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, a TLS certificate to identify the PFS (as a syslog client – mutual authentication is used) and the corresponding key file must be uploaded through the File Management page. PFOS supports only a single TLS certificate which is used both for the web UI (as a server certificate) and for syslog (as a client certificate). Refer to [Maintaining Certificate Files](#) for details. Additionally, TLS protocol is not supported when common criteria mode is enabled.

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

![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.]

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

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

7. 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.

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

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.

<table>
<thead>
<tr>
<th>Severity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
</tr>
<tr>
<td>Alert</td>
</tr>
<tr>
<td>Critical</td>
</tr>
<tr>
<td>Error</td>
</tr>
<tr>
<td>Warning</td>
</tr>
<tr>
<td>Notification</td>
</tr>
<tr>
<td>Info</td>
</tr>
<tr>
<td>Debug</td>
</tr>
</tbody>
</table>

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).
nCM

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

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.
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:

![Config Notifications tab](image)

### Event Notification Settings

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Notification Type</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>All</td>
<td>all</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>none</td>
</tr>
</tbody>
</table>

**Note:**
- Action: Configure the notification type for different events.
- Notification Types: All, None, SNMP, NETCONF.
Select the **User Notification** tab to configure notifications related to user access:

![Event Notification event Settings](image)

**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:

SNMP

Use the SNMP page to set SNMP agent, community, target, and user-related configuration. See [Configuring SNMPv1 or SNMPv2c](#) 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.

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.

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 SNMPv1 or SNMPv2c for SNMP configuration workflows.
USM

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

Target

Select the Target tab to specify SNMP target addresses and security model(s) to use.
Community
Select the **Community** tab to configure the list of SNMP communities.

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

Select the **Traps** tab to specify which SNMP traps will be enabled.

Time settings

Use the **Timing Sources** page to set the system time manually or by specifying one to three NTP servers. 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

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.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>server-not-reachable</strong></td>
<td>No NTP server is reachable.</td>
</tr>
<tr>
<td><strong>syncing</strong></td>
<td>The system time is synchronized to one of the NTP servers.</td>
</tr>
<tr>
<td><strong>running</strong></td>
<td>NTP is running but has not started to synchronize to any NTP server.</td>
</tr>
<tr>
<td><strong>not-running</strong></td>
<td>No NTP server is configured.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ok</strong></td>
<td>Authentication is successful. The &quot;ok&quot; status only displays while the status is &quot;syncing.&quot;</td>
</tr>
<tr>
<td><strong>bad</strong></td>
<td>Authentication failed.</td>
</tr>
<tr>
<td><strong>None</strong></td>
<td>No authentication is configured for this NTP server.</td>
</tr>
</tbody>
</table>

| 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.
5. 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**

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.

**PTP**

Select the **PTP** tab to configure settings for Precision Time Protocol.
The following table shows the settings. After specifying the configuration, click **Apply** in the Toolbar to save the changes to the running configuration.

**Table 3.1 - PTP settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable PTP</td>
<td>Enables PTP for time setting (default is disable). When you select Enable, the additional fields are shown.</td>
</tr>
<tr>
<td>IP Address</td>
<td>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.</td>
</tr>
<tr>
<td>Domain</td>
<td>Specifies the PTP domain (1-255, default 0).</td>
</tr>
<tr>
<td>Announce Msg Interval</td>
<td>Configures the interval between PTP announcement messages (-4 to 5, default 1).</td>
</tr>
<tr>
<td>Announce Recv Timeout</td>
<td>Configures the number of attempts before timeout of receive messages (2 to 10, default 3).</td>
</tr>
<tr>
<td>Sync Interval</td>
<td>Configures the synchronization interval (-8 to 2, default 0).</td>
</tr>
<tr>
<td>DHCP</td>
<td>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.</td>
</tr>
<tr>
<td>Transport</td>
<td>Specifies the transport type for PTP messages (Ethernet or UDP, default UDP).</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the port as Ethernet or PTP (default PTP).</td>
</tr>
<tr>
<td>Delay Mechanism</td>
<td>Configures either end-to-end or peer-to-peer for PTP delay messages (default is end-end).</td>
</tr>
<tr>
<td>PPS Source</td>
<td>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).</td>
</tr>
<tr>
<td>Telecom Profile</td>
<td>Enable or disable the telecom profile.</td>
</tr>
</tbody>
</table>

### Configuring Access Control

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

- **User Access (Roles and Users)**
- **Password Policies**
- **Session Limit**
- **User and IP Lockout Settings**
- **Client IP Lockout**
- **Firewall Rules**
- **Authentication**

#### 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.

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

7. Click **OK**.
8. 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.
9. Click **Apply** to save the settings and **OK** to confirm.
10. Click the **Role** breadcrumb near the top of the page to return to the role definition page.

### 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**.
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.

### 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.
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.

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.

Password expiration limits apply only to local authentication. This feature has no effect on external authentication through RADIUS or TACACS.

Configure password expiration

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.
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.

Password length and character limits apply only to local authentication. This feature has no effect on external authentication through RADIUS or TACACS.

Configure password length and character requirements


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).
   - **Lowercase**: minimum number of lowercase letters 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.
   - **Uppercase**: minimum number of uppercase letters required (default is 0).
   - **Numerical**: minimum number of numerical characters required (default is 0).

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.

**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

**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).

![Login Session Limit Settings](image)

**User and IP Lockout Settings**

You can configure the number of failed login attempts that PFOS allows before a user account or IP address is locked out. These settings are enabled by default with a value of 5. You can also disable the lockout features:

- **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.

  The Lockout Disable options are disabled (unchecked) as a default; therefore, PFOS will lock user accounts and IP addresses based on the configured maximum failed attempts.

To 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 login attempts, check either of the following 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. 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.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Invalid Login Attempts Count</th>
<th>First Invalid Login Time</th>
<th>IP Lock Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.3.4</td>
<td>1</td>
<td>2019-10-16T07:52:21:00:00</td>
<td></td>
</tr>
<tr>
<td>4.3.2.1</td>
<td>5</td>
<td>2019-10-16T07:53:19:00:00</td>
<td>2019-10-16T07:54:26:00:00</td>
</tr>
</tbody>
</table>
“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.

**Configure Firewall Rules**

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

- **IP**: Network IP address and netmask prefix length. Both IPv4 and IPv6 addresses are supported.

- **Action**: Permit or Deny traffic on specified IP.

  **Note**: To prevent user from inadvertently locking themselves out, the Deny command will fail if:
  - The user client IP is in Usable Host IP range. For example, if user defines firewall rule 216.130.207.9/22 deny ingress, and the user client IP is within 216.130.204.1 - 216.130.207.254 IP range, the deny command will fail.
  - The Switch Gateway IP is in usable host IP range.
  - The Input IP is 127.0.0.0/8 (or ::1 for IPv6).

- **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.

**Authentication**

When a user logs in, PFOS attempts each configured remote authentication server. If the server that is next in line is reached but fails to authenticate, a response is returned to the client that authentication failed, 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.

You can specify which authentication types (Local, RADIUS, and TACACS) are active and the order in which they are used.

**To configure authentication order**
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**.

To add a **RADIUS** server

1. Open the **Radius 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**.
3. Specify the following settings based on the configuration of your RADIUS server:
   - **Host**: IP address of the RADIUS server.
   - **Port**: Port for access to the server (default 0).
   - **Key**: AES encrypted string to authenticate to the server.
   - **Timeout**: Time after which requests to the server time out (default 30 seconds)
   - **Retransmit**: Number of times PFOS attempts to contact the server (default 3).
4. Click **Apply** in the toolbar to save the changes to the running configuration.

To add a **TACACS** 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**.
3. Specify the following settings based on the configuration of your TACACS server:
   - **Port**: Port for access to the server (default 49).
   - **Key**: AES encrypted string to authenticate to the server.
   - **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.

### About PFOS parameters on external AAA servers

When you configure PFOS 6.x to perform authentication and authorization on an external RADIUS or TACACS server:

- For authentication, user credentials must be configured at the external RADIUS or TACACS server.
- Authorization role details must be configured on PFOS. On the external AAA server, specify the role name (just a name). The role details must be configured in PFOS. An authentication request is sent to the external server, and a response contains the role name. PFOS takes that role, and all permissions of that role apply.

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

---

### Configuring Ports

This section describes how to configure ports. Topics include:

- **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, 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 ports
A pStack port is a bidirectional class of port that is used to interconnect systems for providing an auto-sensing, self-healing, topologically pfsMesh architecture for traffic capture. For more information on pfsMesh and pStack ports, refer to pStack.

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 be disabled for Inline Network ports. 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 with 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.

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:** For PFS 5010s with limited 16-port capacity licensing, only ports 1-16 can be configured; ports 17 and greater have a "Locked" state. To control column display settings in the Port Settings page, click the Wrench \( \text{icon} \).

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

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.
Table 3.2 provides descriptions for the Basic port settings.

**Table 3.2 - Basic tab settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Assign a name for the port to help identify the devices or network segments that are connected to the unit.</td>
</tr>
</tbody>
</table>
| Class   | Specify the type of port:  
- Monitor  
- Service  
- Span-Monitor  
- Span (default)  
- pStack  
- Inline Network  
- Inline Monitor |
Table 3.2 - Basic tab settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Features Direction</td>
<td>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.</td>
</tr>
<tr>
<td>Link State</td>
<td>Specify the link state for the port:</td>
</tr>
<tr>
<td></td>
<td>- Auto: Normal operation.</td>
</tr>
<tr>
<td></td>
<td>- Force Down: Force the link down.</td>
</tr>
<tr>
<td></td>
<td>- Force Up: Force the link up.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Speed</td>
<td>Select the port speed, if the inserted transceiver supports more than one speed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> PFS 5110s and PFS 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).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> PFS 5130-128X supports QSFP+, 40G BiDi Tx/Rx, 40G BiDi Rx and QSFP28 in all ports. These ports may be configured for operation at 40G and 100G, however the port speed is a common setting for each group of four sequential ports, starting at the first port of each line card (for example, ports 1-1 to 1-4 must all have the same speed regardless of port class even if service port). 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 enforce all 4 ports to be the same speed).</td>
</tr>
<tr>
<td>Port Breakout</td>
<td>Available on 40G and 100G ports. Select this checkbox to divide this port into multiple subports. Select a breakout option from the drop-down list that displays: 4x10G, 2x50G, or 4x25G. When port breakout is enabled, the subports have identifiers of the form <code>slot-port.num</code>, where <code>slot</code> is the slot number, <code>port</code> is the main port number, and <code>num</code> is an ascending number for each breakout. <strong>Note:</strong> Only certain ports on the PFS 5120/7120 and PFS 7121-64x have breakout capability; refer to PFS 5120/7120 Port Breakout Limitations and PFS 7121-64X Port Breakout Limitations for details.</td>
</tr>
</tbody>
</table>
Table 3.2 - Basic tab settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
Forward Error Correction (FEC) is an error correction technique that adds redundant information to a data transmission, enabling a receiver to identify and correct errors without the need for retransmission. However, there is a latency penalty when using FEC.  
FEC is disabled by default (except PFS 5130-128X), which offers the lowest latency delay. FEC is typically disabled with single mode (LR) connections. FEC at PFS 5130-128X is not configurable, it is always enabled. Therefore, PFS 5130-128X does not support 100G BiDi because it requires FEC to be disabled. |
| FEC Type     | FEC should be enabled when the peer (or tapped network) has FEC enabled. Once enabled, FEC can be operated in one of two modes: FC-FEC mode (CL74) or RS-FEC mode (CL91), depending on the network peer FEC setting and the PFS 51xx/71xx model. Support of the FEC modes varies depending on PFS 51xx/71xx model; refer to PFS 51xx/71xx Support of FEC. RS-FEC mode (CL91) is default.  
**Note:** PFS 5130-128X can support FEC RS-FEC mode (CL91) only. |
| 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 | Enable or disable VLAN tagging on this port. VLAN tagging is disabled by default.  
**Note:** VLAN tagging on the PFS 5130-128X is not configurable; packets egressing the PFS 5130-128X device will always be tagged with the Default or “User-Defined” VID configured at Source port VLAN. However, if packets are from a remote device over pfsMesh and they egress at the PFS 5130-128X, they will always be tagged with the default VID of the remote source port. |
Table 3.2 - Basic tab settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| VLAN ID                | Choose from the following options:<br>  
  - **Default:** PFOS assigns a default VLAN ID based on the Starting VLAN ID configured on the System page; for details, refer to [Source Port VLAN Tagging](https://example.com).<br>  
  - **User-Defined:** You can assign a custom VLAN ID to the port; valid values range 1-4094. PFOS derives VLAN IDs based on following:<br>  
    - If pStack is **disabled** (that is, PFS has no ports with Class = pStack), 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.<br>  
    - If pStack is **enabled** (that is, PFS has a port with Class = pStack), incoming packets will be tagged with port's user-defined VLAN. If a user-defined VLAN is not set then it will use the VLAN assigned by the pStack protocol. **Note:** One exception to this rule is when ports are part of a Consolidated network group. User-defined VLANs for all the member ports of a Consolidated network group will be ignored. Incoming packets from the member ports are tagged with a Common VLAN ID value from the Consolidated network port group. If a Common VLAN ID is not set, then it is tagged with a VLAN ID assigned by the pStack protocol.<br>  
    - See also the `vlan-translation-table` command in the [PFOS CLI Reference Guide](https://example.com).
| Tunnel Termination     | Enable tunnel termination on this port. Tunnel termination is disabled by default. **Note:** Time stamping 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 [IP Tunnel Termination](https://example.com) for details. |
| Timestamp              | (Visible only for PFS 7120, PFS 7031-56X, PFS 7031-32X devices) 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 [Time stamping](https://example.com) for details. **Note:** Time stamping and Tunnel Termination cannot be enabled on the same port. |
| Stripping              | Enable VLAN tag, VN tag, VxLAN, and MPLS stripping. Available only on PFS 5000/7000 Series. Refer to [PFS 5000/7000 Enhanced Port Features](https://example.com) for details. |

**PFS 51xx/71xx Support of FEC**

Support of the [FEC modes](https://example.com) varies depending on the PFS 51xx/71xx model (see following tables). RS-FEC mode (CL91) is default.

**PFS 5100/7100**
### PFS 5100/7100

<table>
<thead>
<tr>
<th></th>
<th>100G</th>
<th>100G Breakout</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>25G</td>
<td>50G</td>
</tr>
<tr>
<td>CL74 (FC-FEC)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CL91 (RS-FEC)</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### PFS 5110/7110

<table>
<thead>
<tr>
<th></th>
<th>25G</th>
<th>100G</th>
<th>100G Breakout</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>25G</td>
<td>50G</td>
<td></td>
</tr>
<tr>
<td>CL74 (FC-FEC)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CL91 (RS-FEC)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### PFS 5120/7120/7121-64X

<table>
<thead>
<tr>
<th></th>
<th>25G</th>
<th>100G</th>
<th>100G Breakout</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>25G</td>
<td>50G</td>
<td></td>
</tr>
<tr>
<td>CL74 (FC-FEC)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CL91 (RS-FEC)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### PFS 5130-128X

<table>
<thead>
<tr>
<th></th>
<th>100G</th>
</tr>
</thead>
<tbody>
<tr>
<td>CL74 (FC-FEC)</td>
<td>No</td>
</tr>
<tr>
<td>CL91 (RS-FEC)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Timestamping

**Note:** This feature is only available on PFS 7120, PFS 7031-32X, and PFS 7031-56X devices.

For the PFS 7120, PFS 7031-32X, and PFS 7031-56X 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 Tunnel Termination cannot be enabled on the same port.
Table 3.3 - Supported Time Stamp Directions

<table>
<thead>
<tr>
<th>Class-type</th>
<th>Direction</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RX</td>
<td>TX</td>
<td></td>
</tr>
<tr>
<td>Span</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Monitor</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Span-Monitor</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Time Stamp Details**

- Timestamps are added to the end of a frame; the timestamp consists of the low-order bits of the time of day in Universal Time Coordinated (UTC). See below for details.
- 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>1 Bit Pos</th>
<th>Width</th>
<th>Position</th>
</tr>
</thead>
<tbody>
<tr>
<td>time_0_47</td>
<td>0</td>
<td>48b</td>
<td>48-bit UTC timestamp (18b sec + 30b nanosecond)</td>
</tr>
<tr>
<td>reserved_0</td>
<td>48</td>
<td>8b</td>
<td>Unused byte</td>
</tr>
<tr>
<td>origin_id</td>
<td>56</td>
<td>23b</td>
<td>Origin ID (configured by user on port - see Step 3 in Enable Time Stamping)</td>
</tr>
<tr>
<td>rx_tx</td>
<td>79</td>
<td>1b</td>
<td>Direction (0=Rx, 1=Tx)</td>
</tr>
<tr>
<td>reserved_1</td>
<td>80</td>
<td>32b</td>
<td>Place holder for FCS if last SHIM else unused</td>
</tr>
</tbody>
</table>

**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 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.

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.

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

- Shaded numbers indicate ports that can have port breakout enabled

PFS 7121-64X Port Breakout Limitations

The PFS 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.

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

- 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.
Table 3.4 provides descriptions for the Advanced port settings.

### Table 3.4 - Advanced tab settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Output Timestamping</td>
<td>Assigns a time stamp when traffic leaves a monitor port. See Time Stamping for details.</td>
</tr>
<tr>
<td>Monitor Output Portstamping</td>
<td>Assigns a port stamp when traffic leaves a monitor port. In the Portstamping Option drop-down list that displays, select One Byte Flat or Two Byte Flat as the portstamping option (Two Byte Flat is the default). See Port Stamping for details.</td>
</tr>
</tbody>
</table>
| GeoProbe Time Format           | This option is only used for Monitor ports when the PFS is used in GeoProbe G10 deployments.  
  • Strip TS/PS (Strip timestamp/portstamp): Egress packets have no timestamp and port tag (egress packets are the same as received at ingress port)  
  • Include TS/PS (Include VSS timestamp/portstamp): Egress packets have timestamp and/or port tag appended to end of packet  
  • GeoProbe TS/PS (Encapsulate using GeoProbe-format timestamp/portstamp): Egress packets have GeoProbe metadata header containing timestamp, port tag, and other information                                                                 |
| 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 Protocol De-encapsulation and Stripping.                                                                                                                                                                                                                   |
Table 3.4 - Advanced tab settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>De-Duplication</td>
<td>Enables or disables deduplication on the port. For more information, refer to Packet De-duplication.</td>
</tr>
<tr>
<td>Slicing</td>
<td>Select this checkbox to enable conditional packet slicing and masking. For more information, refer to Conditional Packet Slicing and Conditional Packet Masking.</td>
</tr>
<tr>
<td>Extended Load Balancing</td>
<td>Select this checkbox to enable extended load balancing. For more information, refer to Extended Load Balancing. In the drop-down list that displays, select the extended load balancing library (pre-configured or user-defined) to use.</td>
</tr>
</tbody>
</table>

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.

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 Tool Chain - Simple Mode vs. Advanced Mode.

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.

Create 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.

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 Configuring Monitor Output with a pfsMesh for details.
5. To select the ports that will be in this port group, click **Configure** in the Ports section.

![Configure Port Group](image1)

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

![Select Ports](image2)

7. Enter the port group details. These details vary according to the type of port group being created:
a. For a network port group:

- **Consolidation (Only Available on PFS 6000 Series):** Select **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.

- **Common VLAN ID (Only Available on PFS 6000 Series):** Optionally specify a value from 1 to 4094. This VLAN ID must be the same as the user-defined VLAN ID of all member ports.

---

a. For a monitor port group:

- **Load Balance Groups:** Optionally select a load balance group. *Tunnel load balance groups are not supported in monitor port groups.*

- **Lb Criteria:** If a load balance group is selected and you are using pStack, then select load balancing criteria. These criteria are used only by pStack maps created by the pStack protocol.

- If the monitor group is used locally in a map, specify load balancing criteria in the map itself.

- **pfsMesh:** Select **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 Configuring Monitor Output with a pfsMesh for details.
a. For an inline network port group:

- **VLAN Tag**: 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.

- **Power Safe**: This option must be set when the Inline Network port is connected to the External PowerSafe TAP 3296.

- **A Port**: Specify the A-side port in this group.

- **B Port**: Specify the B-side port in this group.
b. For an inline monitor port group:
   - In the Port Pair section, click Add to specify the A-side port in this group.
   - In the B Port section, select the B-side port in this group.
   - 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.
   - In the LinkSafe section, enable or disable LinkSafe for this group.
   - 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.
   - 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.

1. 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 Group Resource Limits

<table>
<thead>
<tr>
<th>Port Group Type</th>
<th>Maximum Groups per chassis</th>
<th>Max Members per Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>PFS 5000/7000: 64</td>
<td>Up to 64 ports</td>
</tr>
<tr>
<td></td>
<td>PFS 6000:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Consolidated: 16</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Non-consolidated: 48-64</td>
<td></td>
</tr>
<tr>
<td>Monitor</td>
<td>64</td>
<td>No port limitation, up to 128 Load Balance Groups</td>
</tr>
<tr>
<td>Inline Network</td>
<td>32</td>
<td>Up to 128 ports</td>
</tr>
<tr>
<td>Inline Monitor</td>
<td>32</td>
<td>Up to 64 ports</td>
</tr>
</tbody>
</table>
4 Base Features and Tasks

This chapter 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.

Contents

Traffic Maps
Traffic Filtering
Traffic Load Balancing
Trigger Policies
Source Port VLAN Tagging
IP Tunnel Termination
pStack

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:
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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type</th>
<th>Mode</th>
<th>Filter</th>
<th>Input Ports</th>
<th>Network Port Groups</th>
<th>Monitor Port Groups</th>
<th>Output Ports</th>
<th>Output LBGs</th>
<th>Load Balance Criteria</th>
<th>Map Status - Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAP-1</td>
<td>Monitor</td>
<td>Basic</td>
<td>AAA</td>
<td></td>
<td>1-11</td>
<td>NPQ-1</td>
<td>NPQ-1</td>
<td>1-29</td>
<td>LBQ-1</td>
<td>LDQ_Dest_Src</td>
<td>enable</td>
</tr>
<tr>
<td>MAP-1A</td>
<td>Monitor</td>
<td>Basic</td>
<td>SUP</td>
<td></td>
<td>1-11</td>
<td>NPQ-1</td>
<td></td>
<td></td>
<td>LBQ-1</td>
<td>LDQ_Dest_Src</td>
<td>enable</td>
</tr>
<tr>
<td>MAP-1C</td>
<td>Monitor</td>
<td>Basic</td>
<td>nonmatch</td>
<td></td>
<td>1-23</td>
<td></td>
<td></td>
<td></td>
<td>LBQ-1</td>
<td>LDQ_Dest_Src</td>
<td>enable</td>
</tr>
<tr>
<td>MAP-2</td>
<td>Monitor</td>
<td>Basic</td>
<td>AAA</td>
<td></td>
<td>1-12</td>
<td>NPQ-2</td>
<td>NPQ-2</td>
<td>1-21</td>
<td>LBQ-1</td>
<td>LDQ_Dest_Src</td>
<td>enable</td>
</tr>
<tr>
<td>MAP-2A</td>
<td>Monitor</td>
<td>Basic</td>
<td>unfiltered</td>
<td></td>
<td>1-12</td>
<td>NPQ-2</td>
<td></td>
<td></td>
<td>LBQ-1</td>
<td>LDQ_Dest_Src</td>
<td>enable</td>
</tr>
</tbody>
</table>

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 TCP (with specific IP addresses) applied in Map-1, and a second filter called HTTP 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Mode</th>
<th>Filter</th>
<th>Input Ports</th>
<th>Output Ports</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map-1</td>
<td>Monitor</td>
<td>• Raw unfiltered traffic from input port 1-1 is processed against TCP filter.</td>
<td>Basic</td>
<td>TCP</td>
<td>1-1</td>
<td>1-7</td>
<td>Forward</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Packets matching TCP filter are forwarded to Port 1-7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Packets not matching TCP filter are processed by Map-2 (HTTP filter)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Map-2</td>
<td>Monitor</td>
<td>• Traffic not matching TCP filter from input port 1-1 is processed against HTTP filter.</td>
<td>Basic</td>
<td>HTTP</td>
<td>1-1</td>
<td>1-8</td>
<td>Forward</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Packets matching HTTP filter are forwarded to Port 1-8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Packets not matching HTTP filter are passed through to the next maps with the same input ports/groups.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example 2 – Traffic Maps with Filtering on Different Input Ports

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
<th>Mode</th>
<th>Filter</th>
<th>Input Ports</th>
<th>Output Ports</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map-1</td>
<td>Monitor</td>
<td>• Raw unfiltered traffic from input port 1-1 is processed against TCP filter.</td>
<td>Basic</td>
<td>TCP</td>
<td>1-1</td>
<td>1-7</td>
<td>Forward</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Packets matching TCP filter are forwarded to Port 1-7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Packets not matching TCP filter are passed through to the next maps with the same input ports/groups.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
<td>Mode</td>
<td>Filter</td>
<td>Input Ports</td>
<td>Output Ports</td>
<td>Action</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
<td>--------</td>
<td>-------------</td>
<td>--------------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| Map-2 | Monitor| • Raw unfiltered traffic from input port 1-2 is processed against HTTP filter.  
• Packets matching HTTP filter are forwarded to Port 1-8  
• Packets not matching HTTP filter are passed through to the next maps with the same input ports/groups. | Basic | HTTP   | 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

**Note:** The PFS 5130-128X supports a maximum of 510 maps.

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.
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.
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 groups and criteria:
   a. Click **Add an entry** in the Output Load Balance Group area.
   b. Select the load balance group and click **Add**. Click **Update** to update an existing entry.
   c. 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.
   d. After you add a load balance group, the page displays an additional area for load balance criteria.
   e. To add criteria, click **Add an entry**.
   f. Select the criterion, and click **Add**. Click **Update** to update an existing entry.
   g. To add another entry, click **Add**. To remove an entry, 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 Policy. To enable the traffic map based on the outcome of a trigger policy, perform the following:
   a. Select Trigger Policy.
   b. Select the Name of the trigger policy to be monitored for this map.
   c. Select the State of the trigger policy you want to enable the map (active/inactive).

![Trigger Policy State](image)

14. 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 Drag-and-Drop](image)

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.

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.

---

**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**.
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.

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.

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.
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 Ports**

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 ports**.

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.
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.
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).

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.

![Filter Expression Page](image)

**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.

![Forwarding Filters](image)

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.

**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 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.

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

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.
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.

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

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.

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

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

\[
\text{packet-field value}
\]

Multiple comparisons can be joined using the keywords \text{AND} or \text{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:

\[
(\text{mac source 00AA00112233 or Ethernet source 00AA00112234 or Ethernet destination 00AA00112235}) \text{ and (destination IP address 1.2.3.4 or source IP address 1.2.3.4) and IP protocol 6}
\]

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

\textbf{Note:} The PFS 5130-128X does not support filter expressions that include VLAN ID, TPID, and Priority field in the VLAN Tag.

\textbf{Table 4.2 - Fields Available to Define Filter Expressions}

<table>
<thead>
<tr>
<th>Packet field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC source address</td>
<td>Ethernet (IEEE 802.3 - Layer 2) source and destination address. You can use the following keywords:</td>
</tr>
<tr>
<td>MAC destination address</td>
<td>• AND/OR to combine source and destination conditions.</td>
</tr>
<tr>
<td>IP source address</td>
<td>• bidirectional to configure address as bidirectional</td>
</tr>
<tr>
<td>IP destination address</td>
<td>IP (Layer 3) source and destination address (if an IP packet). You can use the following keywords:</td>
</tr>
<tr>
<td>Source port</td>
<td>• AND/OR to combine source and destination conditions.</td>
</tr>
<tr>
<td>Destination port</td>
<td>• bidirectional to configure address as bidirectional</td>
</tr>
<tr>
<td>EType</td>
<td>Layer 4 source and destination ports. You can use the following keywords:</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>• AND/OR to combine source and destination conditions.</td>
</tr>
<tr>
<td>Tag Priority</td>
<td>• bidirectional to configure address as bidirectional</td>
</tr>
<tr>
<td>Layer 3 TOS/Class</td>
<td>Ethernet Type. Use the Shortcuts pull-down list to restrict the EType settings to a particular protocol.</td>
</tr>
<tr>
<td>IPv6 flow</td>
<td>Enter the IEEE 802.1q VLAN ID (if a tagged packet).</td>
</tr>
<tr>
<td>Using Protocols</td>
<td>Enter the IEEE 802.1p/q priority (if a tagged packet).</td>
</tr>
<tr>
<td>Specify other IP Protocol (IPv4)/Next Header (IPv6)</td>
<td>Enter the type of service (TOS) class for the filter.</td>
</tr>
<tr>
<td>TCP flag type</td>
<td>Enter the IP Flow field (if an IPv6 packet).</td>
</tr>
<tr>
<td>Include custom offset</td>
<td>Select a protocol.</td>
</tr>
<tr>
<td></td>
<td>If the desired protocol is not listed, enter the IP protocol number of the desired protocol.</td>
</tr>
<tr>
<td></td>
<td>Filter packets based on various combinations of TCP flags.</td>
</tr>
<tr>
<td></td>
<td>See Custom Offset Filters</td>
</tr>
</tbody>
</table>
Custom Offset Filters

**Note:** This section provides information about custom offset filters for PFS 6000 Series and PFS 5000/7000 Series, excluding PFS 7031-32X and PFS 7031-56X. For the PFS 7031 devices, refer to Custom Offset Filters for PFS 7031-32X and PFS 7031-56X.

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.

![Custom Offset Filters Interface](image)

**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:

<table>
<thead>
<tr>
<th>offset</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip offset 15 02</td>
<td>Matches the single byte pattern 02 against the last byte of the IPv4 source address (15 bytes past the start of the IPv4 header).</td>
</tr>
<tr>
<td>l4 offset 28 10.20.30.1</td>
<td>Matches the specified IPv4 source address inside a GTP-U header (28 bytes past the start of the UDP header).</td>
</tr>
<tr>
<td>l4 offset 28 2001:0db8:85a3:0000:0000:8a2e:0370:7334</td>
<td>Matches the specified IPv6 source address inside a GTP-U header (28 bytes past the start of the UDP header).</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>ip offset 15 01 mask 01</th>
<th>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).</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 offset 28 10.20.30.0 mask 255.255.255.0</td>
<td>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).</td>
</tr>
<tr>
<td>14 offset 28 2001:0db8:85a3:0000:0000:0000:0000:0000 mask</td>
<td>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).</td>
</tr>
</tbody>
</table>

Custom Offset Filters for PFS 7031-32X and PFS 7031-56X

**Note:** While some MAC and L4 custom offset filter configurations for other 5000/7000 devices are still valid for PFS 7031-32X and PFS 7031-56X 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 7031 devices.

Custom offset filtering for PFS 7031-32X and PFS 7031-56X devices is different from other PFS devices due to the 7031 internal switch design. This design supports more granularity on different packet types such as VxLAN, GRE, etc.; therefore, PFS 7031-32X and PFS 7031-56X devices support custom offset filters based on the actual header of the application protocol.

The PFS 7031 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 7031 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 7031 Custom Offset Tokens and Offsets.

In addition to standard tokens [mac(l2)/ip(l3)/tcp or udp(l4)] used for UDF filters, PFS 7031 devices support the following tokens to qualify based on packet type. The Filter Resource page shows the UDF bytes utilized and maximum bytes available per packet type.

- L2withVlan
- KnownNonIp
- UnknownI3
- IPv4
- IPv6
- MPLSHeader
- UnknownL4
- GRE
PFS 7031 Custom Offset Tokens and Offsets

**Note:** PFS 7031 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.

<table>
<thead>
<tr>
<th>Config Order</th>
<th>Token</th>
<th>Start Offset</th>
<th>Offset and Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>L2</td>
<td>Start of first byte of L2 header</td>
<td>Offset: 0-63 (decimal)</td>
<td>“L2 offset 12 0x88a8&quot; is used to qualify on outer TPID value from start of the packet.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maximum of 4 bytes</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>L2withvlan</td>
<td>Single Outer Tag/Inner Tag (SOT/IT) packets: 14 bytes from Start of L2 header.</td>
<td>Offset: 0-126 (decimal)</td>
<td>“L2withvlan offset 0 64&quot; is used to qualify on outervlan =100 for SOT/IT packets and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Double Tag (DT) packets: 18 bytes from Start of L2 header.</td>
<td>Maximum of 12 bytes</td>
<td>Innervlan=100 for DT packets</td>
</tr>
<tr>
<td>3</td>
<td>UnknownL3</td>
<td>Start of inner header’s first byte after unknown Ethertype. Valid only for</td>
<td>Offset: 0-108 (decimal)</td>
<td>“unknownL3 offset 16 10.1.2.3&quot; is used to qualify on SrcIP for double tagged packet with</td>
</tr>
<tr>
<td></td>
<td></td>
<td>unknown L3 protocols ETHERTYPE != ( IPv4</td>
<td>IPv6</td>
<td>MIM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maximum of 30 bytes</td>
<td>“unknownL3 offset 18 10.1.2.3&quot; is used to qualify on SrcIP for VNTag (eth type 8926)</td>
</tr>
<tr>
<td>4</td>
<td>KnownNonip</td>
<td>Start of first byte after Known non-ip EtherType (other than Known IPv4/6</td>
<td>Offset: 0-108 (decimal)</td>
<td>“knownNonip offset 14 10.1.2.3&quot; is used to qualify on ARP packet sender ip address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and FCoE/Mim/MPLS tunnels).</td>
<td>Maximum of 26 bytes</td>
<td></td>
</tr>
<tr>
<td>Config Order</td>
<td>Token</td>
<td>Start Offset</td>
<td>Offset and Value</td>
<td>Example</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
<td>--------------</td>
<td>------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 5            | UnknownL4   | Start of first byte of unknown L4 header. works when PROTOCOL != ( TCP | Offset: 0-102 (decimal)  
|              |             |              | Maximum of 16 bytes
|              |             |              | "unknownL4 offset 4 00112233" is used to qualify on custom packet L4 header. |
| 6            | IPv4        | Start of first byte of L3 header for IPv4. | Offset: 0-108 (decimal)  
|              |             |              | Maximum of 12 bytes  
|              |             |              | "ipv4 offset 32 10.1.2.3" is used to qualify on SrcIP of Inner IPv4 header |
|              |             |              | Maximum of 8 bytes  
|              |             |              | "ipv6 offset 56 20.1.2.3" is used to qualify on DstIP of Inner IPv4 header |
| 8            | 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 12 10.1.2.3" is used to qualify on SrcIP of IPv4 header encapsulated in 1-5 MPLS labels. |
| 9            | GRE         | Start of first byte of payload after 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. Internal offset adjustment is done when following bits are set in GRE header |

<table>
<thead>
<tr>
<th>Checksum (C)</th>
<th>Key (K)</th>
<th>Routing (R)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

When all the control bits (C, K, R) are set in packet, user needs to add 4 bytes to get the start of payload. For example, the above expression needs to be modified to "gre offset 30 10.1.2.3" to qualify on SrcIP. In case of "Unknown GRE type" packets, packet offset starts from first byte of L4 header (that is, at the GRE header).
<table>
<thead>
<tr>
<th>Config Order</th>
<th>Token</th>
<th>Start Offset</th>
<th>Offset and Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>L4</td>
<td>Start of first byte of L4 header. Valid only for TCP/UDP packets.</td>
<td>Offset: 0-127 (decimal) Maximum of 16 bytes</td>
<td>&quot;I4 offset 20 30&quot; is used to qualify on GTP protocol type present in TCP packet. &quot;I4 offset 14 64&quot; is used to qualify on VNID present in VxLAN packet.</td>
</tr>
</tbody>
</table>

PFS 7031 Custom Offset Error Handling

The following table describes the error messages PFOS may encounter when processing PFS 7031 custom offsets.

<table>
<thead>
<tr>
<th>Error String</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxUserDefinedFilterLimitReached</td>
<td>UDF bytes allocated count reached the max limit per system.</td>
</tr>
<tr>
<td>PktFmtMaxUserDefinedFilterLimitReached</td>
<td>UDF bytes allocated count reached the max limit per packet format type.</td>
</tr>
<tr>
<td>UserDefinedFilterInvalid</td>
<td>Error during allocation of UDF:</td>
</tr>
<tr>
<td></td>
<td>• UDF create error</td>
</tr>
<tr>
<td></td>
<td>• UDF chunk bitmap allocation failure due to conflict with unavailable chunk bitmap</td>
</tr>
<tr>
<td></td>
<td>• UDF chunk requested exceeds the maximum available chunks per packet format.</td>
</tr>
<tr>
<td>Input offset : 110 exceeds max_offset 102 supported for packet</td>
<td>When the start offset for a specific token/packet type exceeds the maximum offset limit.</td>
</tr>
</tbody>
</table>

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
```

Packet Fields

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

Standard filter expression resource limits vary by platform. Refer to the following sections for filter resource limit details:

- **PFS 6000 Series Filter Resource Limits**
- **PFS 5010/7010 Filter Resource Limits**
- **PFS 51xx/71xx Filter Resource Limits**
- **PFS 7031-32X and PFS 7031-56X Filter Resource Limits**

**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 **Traffic Maps** page.

For the PFOS 6010, 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).
  o A total of up to 30 UDF bytes may be defined.
  o Each UDF may contain up to 16 bytes.
  o Maximum offset value is 63; match up to the 64th byte from the start of a packet.

• “Filter Pool” displays the maximum filter entries with current running configuration. The maximum capability depends on the complexity of the filter expression:
  o 12,544 filter entries if filters use Group-2 only; without IPv6 (Group-1) or Control Group-10.
  o 10,496 filter entries if filters use Group-2 and Control Group-10; without IPv6 (Group-1).
  o 6,272 filter entries if filters contain IPv6 (Group-1) but no Control Group-10.
  o 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

Note:
  o Group-1 is used for IPv6 filter setting only
  o Group-2 is used for all non-IPv6 filter settings
  o Control Group-10 is for system control packets when either pfsMesh or Tunnel Termination is enabled.

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 Traffic Maps page.

```
+---------------------------------+-------------------+
+ UDF Bytes Occupied:  0 / 32     |
+ Ranges Used/Supported:  0 / 32  |
+ TCAM Information:          +
  + Group | Priority | TCAM Total | TCAM Used | TCAM Free | Bits Used +
  +--------+----------+------------+-----------+-----------+-----------+
  + 10 | 7ff5 | 6144 | 0 | 6144 | 228 +
  + 20 | 7ffeb | 12288 | 1 | 12287 | 82 +
+---------------------------------+
MODE: src-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 Termination is enabled (default is enabled).
  - 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)=0x0B00.

- **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 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.
    - 6144 or 4096 entries if filter expression is more complicated and uses multiple Field Selectors.
    - A new group is created when total match condition bits (Qset bits) is more than 380 bites.

“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 Traffic Maps page.

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 5100/7100 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 Termination is enabled (default is enabled).
  - 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)=0x0B00.

- **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 display the usage for SIP or DIP mode.
- 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, 30, 40, and 50 are used for user’s filters at each pipe:
  - 2560 entries if total match condition bits (Qset bits) is less than 160 bits
  - 768 entries if total match condition bits (Qset bits) is between 160 to 320 bits
  - 540 entries if total match condition bits (Qset bits) is more than 320 bits (less than 480)
  - A new group is created at each pipe when total match condition bits (Qset bits) is more than 480 bits.

“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:

<table>
<thead>
<tr>
<th>PFS</th>
<th>Pipe</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>5100/7100</td>
<td>1</td>
<td>1-21 to 1-24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-29 to 1-32</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1-1 to 1-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-9 to 1-12</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>1-5 to 1-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-13 to 1-16</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>1-17 to 1-20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-25 to 1-28</td>
</tr>
<tr>
<td>5110/7110</td>
<td>1</td>
<td>1-49 to 1-50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-52 to 1-53</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1-1 to 1-12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-17 to 1-24</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>1-13 to 1-16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-25 to 1-36</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>1-37 to 1-48</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-51</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-54</td>
</tr>
<tr>
<td>PFS</td>
<td>Pipe</td>
<td>Ports</td>
</tr>
<tr>
<td>--------------</td>
<td>------</td>
<td>------------------------</td>
</tr>
<tr>
<td>5120/7120</td>
<td>1</td>
<td>1-9 to 1-12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-21 to 1-24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-41 to 1-44</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-53 to 1-56</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1-1 to 1-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-33 to 1-40</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>1-13 to 1-20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-45 to 1-52</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>1-25 to 1-32</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-57 to 1-64</td>
</tr>
<tr>
<td>7121-64X</td>
<td>1</td>
<td>1-1 to 1-2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-9 to 1-14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-33 to 1-34</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-41 to 1-46</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1-3 to 1-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-15 to 1-16</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-35 to 1-40</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-47 to 1-48</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>1-17 to 1-18</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-25 to 1-30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-49 to 1-50</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-57 to 1-62</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>1-19 to 1-24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-31 to 1-32</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-51 to 1-56</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-63 to 1-64</td>
</tr>
</tbody>
</table>

**PFS 5130-128X Pipes**

PFS 5130-128X filter resources are divided into eight 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 PFS 5130-128X devices:
<table>
<thead>
<tr>
<th>Pipe</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>5130-128x</td>
<td></td>
</tr>
</tbody>
</table>
| 1      | 1-1 to 1-4
         | 2-1 to 2-4
         | 3-1 to 3-4
         | 4-1 to 4-4 |
| 2      | 1-5 to 1-8
         | 2-5 to 2-8
         | 3-5 to 3-8
         | 4-5 to 4-8 |
| 3      | 1-9 to 1-12
         | 2-9 to 2-12
         | 3-9 to 3-12
         | 4-9 to 4-12 |
| 4      | 1-13 to 1-16
        | 2-13 to 2-16
        | 3-13 to 3-16
        | 4-13 to 4-16 |
| 5      | 5-1 to 5-4
         | 6-1 to 6-4
         | 7-1 to 7-4
         | 8-1 to 8-4 |
| 6      | 5-5 to 5-8
         | 6-5 to 6-8
         | 7-5 to 7-8
         | 8-5 to 8-8 |
| 7      | 5-9 to 5-12
         | 6-9 to 6-12
         | 7-9 to 7-12
         | 8-9 to 8-12 |
| 8      | 5-13 to 5-16
        | 6-13 to 6-16
        | 7-13 to 7-16
        | 8-13 to 8-16 |

PFS 7031-32X and PFS 7031-56X Filter Resource Limits

The following graphic shows the PFS 7031 current filter resource usage report. To access the report, click Filter Resources at the top of the Traffic Maps page.

The Filter Resources page includes the following information:

- UDF bytes utilized and maximum bytes available per packet type
- TCP ranges used
- Filter groups
PFS 7031 filter resources are divided into two pipes; refer to **PFS 7031 Pipes**. The following Filter Groups are supported per pipe:

- One VFP group per pipe: VFP groups 0 and 1
- One Control group per pipe: Control groups 10 and 11
- A maximum of 10 IFP groups per pipe: IFP groups 20-29 for Pipe 1, IFP groups 30-39 for Pipe 2

For the PFS 7031 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.
- 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.

“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 7031 Custom Offset Error Handling.

PFS 7031 Pipes

PFS 7031-56X and PFS 7031-32X filter resources are divided into two 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 PFS 7031 devices:

<table>
<thead>
<tr>
<th>PFS</th>
<th>Pipe</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>7031-32X</td>
<td>1</td>
<td>1-1 to 1-16</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1-17 to 1-32</td>
</tr>
<tr>
<td>7031-56X</td>
<td>1</td>
<td>1-1 to 1-12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-25 to 1-36</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-53 to 1-56</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1-13 to 1-24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1-37 to 1-52</td>
</tr>
</tbody>
</table>

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:

```
inert 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)
```

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

<table>
<thead>
<tr>
<th>Filter for bi-directional traffic</th>
<th>Simplified expression by using <code>bidi</code> command</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>(src ip 10.10.10.1 and src port 80) or (dest ip 10.10.10.1 and dest port 80)</code></td>
<td><code>bidi (src ip 10.10.10.1 and src port 80)</code></td>
</tr>
<tr>
<td><code>(src ip 10.10.10.1 and dest port 80) or (dest ip 10.10.10.1 and src port 80)</code></td>
<td><code>bidi (src ip 10.10.10.1 and dest port 80)</code></td>
</tr>
<tr>
<td><code>(src ip 10.10.10.1 or dest port 80) or (dest ip 10.10.10.1 or src port 80)</code></td>
<td><code>bidirection (src ip 10.10.10.1 or dest port 80)</code></td>
</tr>
<tr>
<td><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></td>
<td><code>bidirection (src mac 00:00:00:00:00:11 and dest ip 10.1.1.1)</code></td>
</tr>
<tr>
<td><code>(src ip 10.10.10.1 or dest ip 10.10.10.1) and (src port 80 or dest port 80)</code></td>
<td><code>bidi (src ip 10.10.10.1 and dest ip 10.10.10.1) and bidi (src port 80 or dest port 80)</code></td>
</tr>
</tbody>
</table>

**Traffic Load Balancing**

The session-based, flow-aware load balancing feature distributes traffic across multiple output ports or tunnels. You can configure up to 64 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.

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. Different flows are distributed to different ports/tunnels within the group, effectively balancing the traffic across all ports/tunnels of the group.
Flow association is done by examining selected fields within each packet and applying a hashing algorithm to consistently separate and distribute traffic to specific ports or tunnels. Selected Layer 2, MPLS, 3 and 4 headers and their associated elements determine which header information will be used for traffic maps that have that load balance group as an output.

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 systems with one or more advanced line cards. For more information, refer to [Extended Load Balancing](#).

**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** - rebalance the load among the remaining active group members - traffic will be disturbed. (Default)
- **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.

- **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

**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.
Port Percentage ($P_i$) = \( \frac{W_i}{\Sigma W} \times 100 \)

- $W_i$ is the user-defined weight
- $\Sigma W$ is the sum of all the port weights in the group.

For example, a user configures a group with ports and weights:

<table>
<thead>
<tr>
<th>Port</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>20</td>
</tr>
<tr>
<td>1-2</td>
<td>30</td>
</tr>
<tr>
<td>1-3</td>
<td>0</td>
</tr>
</tbody>
</table>

Using the calculation for each weighted port we find the percentage traffic for each port:

- **Port 1-1**: ($P_i$) = \( \frac{20}{20+30} \times 100 = 40\% \)
- **Port 1-2**: ($P_i$) = \( \frac{30}{20+30} \times 100 = 60\% \)
- **Port 1-3**: ($P_i$) = \( \frac{0}{20+30} \times 100 = 0\% \)

**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 Balancing Workflow**

Follow this process to set up load balancing. After completing these tasks, load balancing is applied automatically.

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**

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.
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. 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.
5. 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.

**Note:** By default, the type is set to Monitor, which is the only port class supported for load balancing.

6. 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.

   ![Port Weight Option](image1)

   b. Click Add to display the Add a New Port Weight page. Select a port and click Add.

   ![Add New Port Weight](image2)

   c. Define a weight for this port. Configure additional port weights as needed.

   ![Define Weight](image3)

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.

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.

**Note:** Weighted Load Balance is not supported for load-balanced tunnels.

By default, the Type is set to Monitor, which is the only port class supported for load balancing.

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 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.
Load balancing can include values of 1 to 3 MPLS labels. 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.

- PFS 5130-128X does not support any encapsulation, so load balance can only be based on L2 or L3 or MPLS label at outer header of the ingress encapsulated packets.

### 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.

### 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, to send notifications based on events, and/or to automatically place the network access into a failsafe state based on trigger policy outcomes. The system continuously monitors these conditions and manages actions based on the outcome of these conditions.

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**

**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.

**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**
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**

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% to disable the minimum level threshold.
- The maximum level threshold, above which the trigger is activated. Enter 100% to disable the maximum level threshold.

- **Trigger timer settings**
- **Port Selection**
- **Trigger actions**
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

### 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 Clear Time](image)

**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)](image)

**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.
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 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.

pfsMesh Option

You can configure whether the trigger is visible to all nodes in pfsMesh (remote node).
**pfsMesh**

- **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 | Displays the current status of this trigger:  
|--------|-----------------------------------------------|  
| Active | indicates the condition defined in the trigger **has** occurred.  
| Inactive | indicates the condition defined in the trigger **has not yet** occurred.  

- **pfsMesh Status**: Trigger name resolution status as updated by pStack protocol.
  - **TriggerNameConflicts**: a conflict occurred with current trigger name and another trigger within pfsMesh.
  - **TriggerNameResolved**: no conflict exists with current trigger name and another trigger within pfsMesh.

<table>
<thead>
<tr>
<th>Conflicting Node ID</th>
<th>If pfsMesh status is TriggerNameConflicts, then this field reflects the node ID with which the conflict exists.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conflicting Node Name</td>
<td>If pfsMesh status is TriggerNameConflicts, then this field reflects the node name with which the conflict exists.</td>
</tr>
</tbody>
</table>
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 policy 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.

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](#)

4. If you enabled notifications in the trigger policy, configure the type of notification you want to send using the following **Notifications** settings (All, None, Syslog, SNMP, NETCONF):
   - Use the **Notifications > Events > Config Notification > Applications** triggers 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).

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. 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. Source port VLAN tagging allows you to configure whether to keep this VLAN tag when the packet exits the system. This lets you identify the PFOS port through which traffic entered the system.

The following figure shows the general format of a VLAN tag:

The VLAN tag contains the following fields:

<table>
<thead>
<tr>
<th>Bits</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-16</td>
<td>TPID</td>
<td>Tag Protocol Identifier</td>
</tr>
<tr>
<td>17-19</td>
<td>PCP</td>
<td>Priority Code Point: IEEE 802.1p priority level</td>
</tr>
<tr>
<td>20</td>
<td>CFI</td>
<td>Canonical Format Identifier: 0 = canonical MAC; 1 = non-canonical MAC</td>
</tr>
<tr>
<td>21-32</td>
<td>VID</td>
<td>VLAN Identifier: combination of the ingress system ID and port ID, or user-specified value</td>
</tr>
</tbody>
</table>

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.
The default VID value is determined by the starting VID and the ingress port identifier value (Port ID) based on its physical location. The starting VID is 1 by default.

You can optionally assign a specific VID to any port, overriding the default VID 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. On the Global Settings page, VIDs can be configured between 1 and 4094.

If a port is using the default VLAN ID and it is used as source in any traffic map, then the pStack protocol assigns it a unique VLAN ID in the range of 1 to 4000.

Source port VLAN tagging is enabled on a per-port basis on the Port Settings page for each Monitor port.

VLAN ID assignment is enabled on a per-port basis on the Port Settings page for each port of any class.

The following diagram describes how and where to configure source port VLAN tagging.

Refer to the following sections for details:

- Override the System Default Ingress VLAN ID on an Ingress Port
- Configure a Port to Add VLAN Tags to Egress Packets
- Change the Default TPID or Starting VLAN ID

Override the System Default Ingress VLAN ID on an Ingress Port

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.
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

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**.

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** (1-4094). 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**.

### 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 such as encapsulated remote port analyzer (ERSPAN), generic routing encapsulation (GRE), or network virtualization GRE (NVGRE). 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.

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.

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.

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.
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.

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 packets (larger than 8,500 bytes) are not supported.

**pStack**

pStack lets you 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, pStack technology is available on all devices that use PFOS.

pStack is the proprietary technology that allows the interconnection of multiple systems into a pfsMesh.

With a pfsMesh, you can tap into your network in one location using a system 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 also allows an administrator to log into any system, which is interconnected with a number of other systems, and see all other systems in that pfsMesh. Each system is then accessible from that same Web UI instance. 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.

With a pfsMesh, monitor output can occur 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.

**About pStack protocol versions**

NETSCOUT occasionally releases new versions of the pStack protocol that are internally incompatible with previous versions. All systems in a pfsMesh must run the same version of the pStack protocol.

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.

**Stacking with other packet flow switches**

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 stacking topologies

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.

Single-link connection

Multi-link connection

Complex mesh

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 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 be built over L2GRE; refer to Use Case 3 - Building pfsMesh over L2GRE Tunnel for details.

Technical considerations include:

- Stack links can be 1G, 10G, 25G, 40G, 50G, or 100G, copper or fiber, 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.
- 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).
Integrated management interface

All nodes within a pfsMesh can be viewed and managed from any of the nodes. To view stacking status, use a web browser to connect to any node in the topology, and then go to the Topology tab of the pfsMesh page.

Points worth noting include:

- This is a distributed management architecture, which means that there is no single point of failure; if one node fails, then all other nodes continue to be fully manageable.
- No proprietary or special software is needed to manage the stacking topology – just a standard web browser.
- The physical management interface to each node remains the management Ethernet ports on the back of 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.

Configuring a pfsMesh

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.

![Port 1-17 Settings](#)

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.
Configuring Monitor Output with a pfsMesh

In a pfsMesh, monitor output can be directed to either one or more Monitor ports on the local node (the same node as the network port input), a group of one or more Monitor ports on a remote node (any other node in the pfsMesh), or a combination of these. Configuring remote monitor output groups is different than configuring individual local output Monitor ports.

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.

All mappings are configured only on the input node, the one on which traffic originally arrives in the pfsMesh. Remote monitor port groups are configured on the appropriate destination node.

**Configure remote monitor port 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.

```
1. In the Ports section, click configure.
2. 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.
3. Click OK.
```
4. Optionally, to add a load balance group:
   a. Click **Add an entry** in the Load Balance Groups section.
   b. 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.
   c. In the Lb Criteria section, select pre-defined or user-defined load balancing criteria.
   d. Click **Update**.
5. 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.)

6. Click **Apply**. Refer to the **Remote Monitor Groups** tab on the pfsMesh page to view a list of currently available remote monitor port groups.

7. View the following status information for a monitor group.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
</table>
| Monitor group name resolution status as updated by pStack protocol. | PortGroupNameConflicts: a conflict occurred with the current monitor group name and another monitor group name within pfsMesh  
PortGroupNameResolved: no conflict exists with the current monitor group name and another monitor group within pfsMesh |

| 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**

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**.
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.
9. 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 the status of remote monitor groups that are used in a traffic map**

1. Go to the Traffic Maps page, and select the desired traffic map.
2. Click **Remote Monitor Group Status** at the bottom of the page.
Using the pfsMesh page

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.
Remote Monitor Groups

The Remote Monitor Groups tab displays the remote monitor port groups that are currently available on connected nodes in this mesh.

Remote Trigger

The Remote Trigger tab displays a list of remote triggers that are currently available on connected nodes in this mesh.

pStackMap

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.
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.

About input port VLAN IDs with pfsMesh

If any port on the system is set to a class of pStack, then VLAN allocation is done dynamically via the pStack protocol.

A unique VLAN ID is assigned to each ingress port from which you have created a traffic map.
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 intermediate 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.

**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.
Enhanced Port Features

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

- PFS 6000 Enhanced Port Features
- PFS 6000 Enhanced Port Features

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 6000 enhanced port features, refer to PFS 5000/7000 Enhanced Port Features.

- Packet De-duplication
- Port and Time Stamping
- Protocol De-encapsulation and Stripping
- Conditional Packet Slicing
- Conditional Packet Masking
- Extended Load Balancing

Packet De-duplication

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.

De-duplication 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.

![Deduplication Tab](image)

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**

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.

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>
<thead>
<tr>
<th>Bits</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-31</td>
<td>Time in seconds since Epoch (00:00:00 GMT January 1, 1970)</td>
</tr>
<tr>
<td>32-61</td>
<td>Subsecond time in nanoseconds, in 20nsec increments</td>
</tr>
<tr>
<td>62-63</td>
<td>Time synchronization source:</td>
</tr>
<tr>
<td></td>
<td>00: Uncalibrated; internal clock only</td>
</tr>
<tr>
<td></td>
<td>01: NTP synchronization</td>
</tr>
<tr>
<td></td>
<td>10: GPS (1PPS with TSIP) or 1PPS-only synchronization</td>
</tr>
<tr>
<td></td>
<td>11: PTP synchronization</td>
</tr>
</tbody>
</table>

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
0912: C9 40 02 86 D7 52
0928: 00 00 00 00 00 00 00 20
```

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 5.2 - Time Stamp Accuracy**

<table>
<thead>
<tr>
<th>Timing/sync source</th>
<th>Time stamp accuracy</th>
<th>Possible variation between ports</th>
<th>Possible variation between systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncalibrated; internal clock only</td>
<td>Indeterminate</td>
<td>16nsec for 1G ports</td>
<td>Indeterminate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13nsec for 10G ports</td>
<td></td>
</tr>
<tr>
<td>NTP server</td>
<td>≤ 10msec</td>
<td>16nsec for 1G ports</td>
<td>≤ 10msec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13nsec for 10G ports</td>
<td></td>
</tr>
<tr>
<td>GPS (1PPS with TSIP)</td>
<td>≤ 200nsec</td>
<td>16nsec for 1G ports</td>
<td>≤ 200nsec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13nsec for 10G ports</td>
<td></td>
</tr>
<tr>
<td>PTP master</td>
<td>≤ 1µsec</td>
<td>16nsec for 1G ports</td>
<td>≤ 1µsec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13nsec for 10G ports</td>
<td></td>
</tr>
<tr>
<td>1PPS only</td>
<td>Depends on 1PPS timing source</td>
<td>16nsec for 1G ports</td>
<td>Depends on 1PPS timing source</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13nsec for 10G ports</td>
<td></td>
</tr>
</tbody>
</table>

**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 stripping options in this section are available only on PFS 6000 Series systems. For information about stripping on PFS 5000/7000 Series systems, refer to PFS 5000/7000 Enhanced Port Features.

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.

**Generic 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 generic stripping feature supports pre-defined protocols that make use of the generic 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 generic 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 | TPID₀ | VLAN Tag₀ | TPID₁ | VLAN Tag₁ | Etype | Payload | Old CRC |

to, with TPIDs and tag(s) removed and CRC recalculated:

| MAC header | Etype | Payload | New CRC |

Stripping Library and Protocol Stripping

**Add a New protocol to the Stripping Library**

1. From the Applications page, click Protocol. The list of currently defined protocols (both user-defined and pre-defined) displays. Up to 20 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 Protocol Matching Field drop-down list, select Etype (the default), IP Protocol, UDP Dest Port, TCP Dest Port, or SCTP Dest Port.
5. 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.
6. In the Strip Headers drop-down list, select L2 Header (the default), L2 L3 Header, or L2 L3 L4 Header.
7. In the Strip Reference Point drop-down list, select Start L2 (the default), End L2, End L3, or End L4.
8. In the Strip Offset field, enter the number of bytes to offset from the strip reference point.
9. 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.

![Protocol Stripping Configuration](image)

**Add a New MPLS-L3 Protocol to the Stripping Library**

1. From the Applications page, click **MPLS-L3**. The list of currently defined MPLS-L3 protocols displays. 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.
7. Click **Apply** in the toolbar to save the settings to the running configuration.

**Configure Protocol Stripping**

1. From the Applications page, click **Protocol Stripping**. The list of currently defined protocol stripping configurations displays.
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 section, optionally select a protocol from the MPLS-L3 protocol library.
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.
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.
Conditional 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.

![IP Slicing Diagram](image)

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 [Packet Fields in Filter Expressions](#).

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.
     - 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 Configuration](image)

   - 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.
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.

7. Click Apply.
Conditional Packet Masking

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:
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**

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 **Packet Fields in Filter Expressions**.

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.
     - 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](image)

- 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 Configuration](image)
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.

7. Click **Apply**.
Extended 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 available on the PFS 6000 Series with the 40SadvR line card.

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.

---

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.

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.

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.

![Traffic Map Configuration](image)

**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.
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.

- **PFS 5000/7000 Enhanced Port Features** (PFS 5000 and PFS 7000 Series)
- **GRE Tunnel Origination/Termination Support** (PFS 7000 Series)
- **VXLAN Tunnel Origination/Termination Support** (PFS 7000 Series)
- **Neighbor Discovery Using LLDP** (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. PFSOS provides the following stripping options:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Tag</td>
<td>You can enable or disable 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 port. Refer to Configure Standard VLAN Tag Stripping for configuration details. <strong>Note:</strong> The PFS 5130-128X device does not support VLAN Tag Stripping.</td>
<td>PFS 5000 Series (except PFS 5130-128X) PFS 7000 Series</td>
</tr>
<tr>
<td>Vn Tag</td>
<td>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 Configure Standard Vn Tag Stripping for configuration details. <strong>Note:</strong> The PFS 5130-128X, PFS 7031-56X, and the PFS 7031-32X devices do not support Vn Tag stripping.</td>
<td>PFS 5000 Series (except PFS 5130-128X) PFS 7000 Series (except PFS 7031-56X and PFS 7031-32X)</td>
</tr>
<tr>
<td>VXLAN</td>
<td><strong>This feature requires the PFS 7000 functionality license.</strong> 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 Configure Standard VXLAN Stripping for configuration details. <strong>Note:</strong> The PFS 5130-128X device does not support Vn Tag stripping.</td>
<td>PFS 5000 Series (except PFS 5130-128X) PFS 7000 Series</td>
</tr>
</tbody>
</table>
### Feature

**MPLS**

This feature requires the PFS 7000 functionality license. You must enable the Features MPLS option in Global Settings before you can use this feature.

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 Configure Standard MPLS Stripping for configuration details.

**Note:** VXLAN and MPLS stripping cannot be enabled at the same time.

<table>
<thead>
<tr>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFS 7000 Series</td>
</tr>
</tbody>
</table>

**L2GRE**

This feature requires the PFS 7000 functionality license. 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 Configure Standard L2GRE Stripping for configuration details.

<table>
<thead>
<tr>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>PFS 7000 Series</td>
</tr>
</tbody>
</table>

### Standard Stripping Port Class Compatibility

The following table shows the availability of each stripping option on various port classes:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Span</th>
<th>Monitor</th>
<th>Service</th>
<th>pStack</th>
<th>Span-Monitor</th>
<th>Inline Network</th>
<th>Inline Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN tag stripping</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Vn tag stripping</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>VXLAN stripping</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>MPLS</td>
<td>Yes[1]</td>
<td>No</td>
<td>Yes[2]</td>
<td>No</td>
<td>Yes[1]</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>L2GRE</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

[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.

### Configure Standard VLAN Tag Stripping

**Note:** The PFS 5130-128X device does not support VLAN Tag Stripping.

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.)
1. Go to the Port Settings page for the 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.

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

**Configure Standard Vn Tag Stripping**

**Note:** The PFS 5130-128X, PFS 7031-56X and the PFS 7031-32X devices do not support Vn Tag stripping.

1. Go to the Port Settings page for the port on which you want to configure Vn tag stripping.
2. Scroll down to the Stripping section.
3. Select or deselect **Vn Tag** as desired.
4. Click **Apply** in the toolbar to save the settings to the running configuration.

**Configure Standard VXLAN Stripping**

**Note:** The PFS 5130-128X device does not support VXLAN Tag stripping.

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.
   - **UDP Port**: UDP port number to use, usually either 4789 or 8472.
   - **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.

   ![Applications](image)

   **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.

![VLAN Tag Stripping Settings](image)

**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.
- VXLAN and MPLS stripping cannot be both enabled at the same time.
- Up to 1024 VNID values (input either as individual values or in a range) can be configured per PFS
- The PFS 5130-128X device does not support VXLAN stripping.

**Configure Standard MPLS Stripping**

*Note: This feature requires the PFS 7000 functionality license. You must enable the **Features MPLS option in Global Settings** before you can use this feature.*

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 Page](image)

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 **Unstrippable MPLS Destination**.
   c. Click **Add**.

![MPLS Page](image)
4. If configuring L2 (Ethernet over MPLS) stripping, configure L2 MPLS labels:
   a. Click the Add button.

   ![Add button](image)

   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 Unstrippable MPLS Destination.

   ![Add new L2 MPLS Labels](image)

   **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.

![Pwc Configuration](image)

**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.

![MPLS Label Counts](image)

**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.
PFOS can be configured to automatically clear the programmed MPLS labels when they reach their maximum allocated limit; see Configuring System Settings 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.
- The Unstrippable MPLS destination is always a port and not a Load-balancing Group (LBG).
- VXLAN and MPLS stripping cannot be both enabled at the same time.
- 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).

Configure Standard L2GRE Stripping

**Note:** This feature requires the PFS 7000 functionality license.

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.

   ![L2GRE Stripping Application Library](image)

   **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](image)
Standard L2GRE Stripping Limitations and Considerations

- For L2GRE-striped 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.

GRE 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 tunnelled 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:

- Use Case 1 - L2GRE Tunnel between Two PFS 7000 Devices
- Use Case 2 - L2GRE Tunnel from PFS to vSTREAMs
- Use Case 3 - Building pfsMesh over L2GRE Tunnel

Refer to [Configuring GRE Tunnel Origination/Termination](#) for workflow details.

**Note:** There is a maximum of 1024 GRE tunnels per chassis.
Configuring GRE 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 GRE Tunnel Origination/Termination. Refer to the **PFOS CLI Reference Guide** for CLI command details.

<table>
<thead>
<tr>
<th>Step</th>
<th>Web UI</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Configure Ports</td>
<td>Port Settings Page</td>
<td>interface command</td>
</tr>
<tr>
<td>Configure a port that is connected to the IP network as Span-Monitor.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 Configure IP Interface</td>
<td>Tunnel Settings&gt;IP Interface Page</td>
<td>interface ip command</td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 Configure GRE Interface</td>
<td>Tunnel Settings&gt;GRE Interface Page</td>
<td>interface gre command</td>
</tr>
<tr>
<td>Configure the Destination IP address for the tunnel, the IP Interface configured in Step 2, GRE Tunnel Key, and Gateway.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 Configure Traffic Map for the Tunnel</td>
<td>Traffic Maps</td>
<td>Refer to Map Commands for GRE Tunnel Origination/Termination</td>
</tr>
<tr>
<td><strong>Note:</strong> PFOS does not support both input tunnels and output tunnels in the same map.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 Tunnel Statistics and Status for status details.

**Configure Ports**

Configure port 1-40 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.

![Port 1-40 Settings](image)

**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_2222) 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 2.2.2.2).
4. In the **Interface** area, click the **Select Port** drop down menu and select the previously configured Span-Monitor port (Port 1-40 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.

![Image of Select Port dropdown menu]

**CLI Configuration**

```
PFS7120(config)# interface ip IP_interface_2222 address 2.2.2.2 port 1-40
```

**Show IP interface on chosen L2GRE tunnel ports**

View IP Interface Settings on the Configuration > Tunnel Settings > IP Interface page.

![Image of Tunnel Settings page]

**CLI show command:**

```
PFS7120# show running-config interface ip IP_interface_2222
table ip IP_interface_2222
address 2.2.2.2
port 1-40
```

**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_3333`) 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_2222` in **Configure IP Interface**).
4. In the **Address** field, enter the Destination IP address for the tunnel (example shows `3.3.3.3`).
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 `1533`).
6. Configure 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 GRE interface.
7. Click **Apply** in the Toolbar to save the changes to the running configuration.

**CLI Configuration (Local)**

```
PFS7120(config)# interface gre gre_tunnel_3333 source IP_interface_2222 destination 3.3.3.3 key 1533
```

**CLI Configuration (Remote)**

```
PFS7120(config)# interface gre gre_tunnel_1111_gateway source IP_interface_2222 destination 4.4.4.4 key 1531 gateway 1.1.1.1
```

**Show GRE Interface on IP Interfaces**

View GRE Interface Settings on the Configuration > Tunnel Settings > GRE page.

![Tunnel Settings](image)

**CLI show command:**

```
PFS7120# show running-config interface gre gre_tunnel_3333
interface gre gre_tunnel_3333
source IP_interface_2222
destination 3.3.3.3
key 1533
```

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**

```bash
PFS7120(config)# map map_tunnels_to_port input-tunnels gre_tunnel_3333
   filter unfiltered output_ports 1-40
```

**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**.

![Select ports to use (drag-n-drop):](image)

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**

```bash
PFS7120(config)# map map_port_to_tunnel_3333 input_ports 1-40 filter
   IP333 output-tunnels gre_tunnel_3333
```

**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 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 1-62.2) 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 (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 1-62.2 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.

**CLI Configuration**

PFS7120(config)# interface ip IP_interface_1112 address 1.1.1.2
port 1-62.2

**Show IP interface on chosen L2GRE tunnel ports**

View IP Interface Settings on the Configuration > Tunnel Settings > IP Interface page.

**CLI show command:**

PFS7120# show running-config interface ip IP_interface_1112
interface ip IP_interface_1112
address 1.1.1.2
port 1-62.2
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).
6. Configure 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 GRE interface.
7. Click **Apply** in the Toolbar to save the changes to the running configuration.

**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_tunnel_1111_gateway source IP_interface_1112 destination 2.2.2.2 key 1231 gateway 1.1.1.1
```

**Show GRE Interface on IP Interfaces**

View GRE Interface Settings on the Configuration > Tunnel Settings > GRE page.

**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.

Use Case 3 - Building pfsMesh over L2GRE Tunnel
In this scenario, two PFS 7000 devices cannot be directly connected (no physical pStack connection can be made between Device A port 1-1 and Device B port 1-1). These devices can be virtually connected over an L2GRE Tunnel via a public/private IP network both running pStack.

Requirements on Both PFS 7000 Devices
Three ports are required to run pStack over L2GRE:
- One port for pStack (1-1)
- One interim Span-Monitor port (1-2) which is physically cabled to the pStack port to bridge pStack traffic.
- One Span-Monitor port (1-10) for the GRE Tunnel

Two traffic maps are required for bi-directional pStack traffic:
- One map to forward traffic from the tunnel to the pStack interim port.
- One map to forward traffic from the pStack interim port to the tunnel.

Perform the following procedures to configure pStack over GRE Tunnel for this scenario:
• **Configure Ports**
• **Configure IP Interfaces**
• **Configure GRE Interfaces**
• **Configure Traffic Maps**
• **Confirm pfsMesh over L2GRE**

Once configured, see [Tunnel Statistics and Status](#) for status details.

### Configure Ports

Configure port 1-10 on both Device A and Device B that will be used to connect to the IP network.

1. On the Configuration > Port Settings page, click Port 1-10 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.

![Port 1-10 Settings](image)

### Configure IP Interfaces

Configure an IP Interface for both Device A and Device B.

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_11`) 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 6.6.6.100 for Device A and 7.7.7.100 Device B, respectively).
4. In the **Interface** area, click the **Select Port** drop down menu and select the previously configured Span-Monitor port (Port 1-10 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.

**Device A Settings**
Configure GRE Interfaces

Configure a GRE Interface for both Device A and Device B.

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_11) 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_11 in Configure IP Interfaces).
4. In the Address field, enter the Destination IP address for the tunnel (example shows 7.7.7.100 for Device A and 6.6.6.100 for Device B, respectively).
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 1122, needs to match on both Device A and Device B).

CLI Configuration on PFS 7000 A

```
PFS(config)# interface ip IP_interface_11 address 6.6.6.100 port 1-10
```

CLI Configuration on PFS 7000 B

```
PFS(config)# interface ip IP_interface_11 address 7.7.7.100 port 1-10
```
6. Configure 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 GRE interface.

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

**Device A Settings**

**Device B Settings**

**CLI Configuration on PFS 7000 A**

```
PFS(config)# interface gre GRE_tunnel_11 source IP_interface_11 destination 7.7.7.100 key 1122 gateway 6.6.6.1
```

**CLI Configuration on PFS 7000 B**

```
PFS(config)# interface gre GRE_tunnel_11 source IP_interface_11 destination 6.6.6.100 key 1122 gateway 7.7.7.1
```

**Configure Traffic Maps**

Configure two maps for both Device A and Device B:
   - One is from the tunnel port to the interim port
   - One is from the interim port to the tunnel port.
CLI Configuration on PFS 7000 A

PFS(config)# map map_from_pstack input_ports 1-2 output-tunnels GRE_tunnel_11 filter unfiltered
PFS(config)# map map_to_pstack input-tunnels GRE_tunnel_11 output_ports 1-2 filter unfiltered

CLI Configuration on PFS 7000 B

PFS(config)# map map_from_pstack input_ports 1-2 output-tunnels GRE_tunnel_11 filter unfiltered
PFS(config)# map map_to_pstack input-tunnels GRE_tunnel_11 output_ports 1-2 filter unfiltered

Confirm pfsMesh over L2GRE

To confirm pfsMesh is up with the pStack/L2GRE connection, access the Status>pfsMesh>Topology page.

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.

```
PFS5120# statistics reset l2gre-stats
PFS5120# show statistics tunnel gre gre-tunnel-name to_vStream
       KEEP       KEEP
GRE TUNNEL  ALIVE  ALIVE  PACKET  PACKET
    NAME  SENT  RECEIVED  TX   RX
----------------------------------------
oto_vStream  0     0     216    0
```

**WebUI:** Access the Status>Statistics>Tunnel GUI.

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).
Display Tunnel Status at IP interface
To view IP interface tunnel status (state directly reflects the physical port state).

**CLI:** Use the `show interface ip` command.

```
PFS5120# show interface ip IP_interface_1112
NAME       STATE       GRE NAME
-------------------------------------
IP_interface_1112 up      gre_tunnel_1111_gateway
```

**WebUI:** Access the Configuration>Tunnel Settings>IP Interface GUI.
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.

```
PFS5120# show interface gre_tunnel_1111_gateway
NAME            STATE          MAP NAME
-----------------------------------------------------
gre_tunnel_1111_gateway   up    map_tunnels_to_port map_port_to_tunnel_1111
```

**WebUI:** Access the Configuration>Tunnel Settings>GRE GUI.

L2GRE Origination/Termination Limitations

- 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)
  - L2GRE keys must be unique per chassis (the same key cannot be used by more than one tunnel).
- Maximum one L2GRE tunnel per remote (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)
- 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:
  o Be used as regular input or output ports in traffic maps/load balance groups
  o Enable monitor port VLAN tagging
  o Have any stripping function enabled
  o Have tunnel termination function enabled

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. This provides up to up to 16 million unique IDs compared to normal VLANs that are 12-bit and have a 4094 VLAN limit.

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.

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.

Note: There is a maximum of 1024 VXLAN tunnels per chassis.

<table>
<thead>
<tr>
<th>Step</th>
<th>Web UI</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Configure Ports</td>
<td>Port Settings Page</td>
<td>interface command</td>
</tr>
<tr>
<td>Step</td>
<td>Web UI</td>
<td>CLI</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>-----</td>
</tr>
<tr>
<td><strong>2 Configure IP Interface</strong></td>
<td>Tunnel Settings&gt;IP Interface Page</td>
<td><code>interface ip command</code></td>
</tr>
<tr>
<td>Configure the Source IP address for the tunnel and select the Span-Monitor port to connect to the public/private IP network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3 Configure VXLAN Interface</strong></td>
<td>Tunnel Settings&gt;VXLAN Interface Page</td>
<td><code>interface vxlan command</code></td>
</tr>
<tr>
<td>Configure the Destination IP address for the tunnel, the IP Interface, VXLAN Tunnel Key, UDP Source Port, and Gateway.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>4 Configure Traffic Map for the Tunnel</strong></td>
<td>Traffic Maps</td>
<td>Refer to Map Commands for VXLAN Tunnel Origination/Termination</td>
</tr>
<tr>
<td><strong>Note:</strong> PFOS does not support both input tunnels and output tunnels in the same map.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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.

![Port 1-10 Settings](image)

### 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.

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.
6. Enter the **UDP L4 Source Port** for encapsulated traffic; valid values range from 1 to 65535.
7. 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.
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.

![Select ports to use (drag-n-drop):](image)

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.

```
PFS5120# statistics reset l2gre-stats
PFS5120# show statistics tunnel vxlan vxlan-tunnel-name to_node1
          KEEP      KEEP
VXLAN TUNNEL ALIVE ALIVE PACKET PACKET
```
To display the Tunnel Status at Event Notifications:

**WebUI:** Access the Status>Statistics>Tunnel GUI.

![Tunnel GUI](image)

**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).

![SysLog History](image)
Display Tunnel Status at IP interface

To view IP interface tunnel status (state directly reflects the physical port state).

**CLI:** Use the `show interface ip` command.

```
PFS5120# show interface ip IP_interface_1112

<table>
<thead>
<tr>
<th>GRE</th>
<th>VXLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>STATE</td>
</tr>
<tr>
<td>------</td>
<td>-------</td>
</tr>
<tr>
<td>IP_interface_1112</td>
<td>up</td>
</tr>
</tbody>
</table>
```

**WebUI:** Access the Configuration>Tunnel Settings>IP Interface GUI.

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.

```
PFS5120# show interface vxlan vxlan_tunnel_1111_gateway

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATE</th>
<th>MAP NAME</th>
<th>MAP NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>vxlan_tunnel_1111_gateway</td>
<td>up</td>
<td>map_tunnels_to_port</td>
<td>map_port_to_tunnel_1111</td>
</tr>
</tbody>
</table>
```
WebUI: Access the Configuration>Tunnel Settings>VXLAN GUI.

VXLAN Tunnel Origination/Termination Limitations

- Up to 1024 different VXLAN interfaces are possible per chassis
- VxLAN VNIDs supported are from 1 to 16777215
  - VXLAN VNIDs must be unique per chassis (the same VNID cannot be used by more than one tunnel).
- Maximum one VxLAN tunnel per remote (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)
- 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:
  - Be used as regular input or output ports in traffic maps/load balance groups
  - Enable monitor port VLAN tagging
  - Have any stripping function enabled
  - Have tunnel termination function enabled
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.

<table>
<thead>
<tr>
<th>Preamble</th>
<th>Destination MAC</th>
<th>Source MAC</th>
<th>Ethertype</th>
<th>Chassis ID TLV</th>
<th>Port ID TLV</th>
<th>Time to live TLV</th>
<th>Optional TLVs</th>
<th>End of LLDPDU TLV</th>
<th>Frame check sequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>01:80:c2:00:00:0e</td>
<td>01:80:c2:00:00:03</td>
<td>Station’s address</td>
<td>0x88CC</td>
<td>Type=1</td>
<td>Type=2</td>
<td>Type=3</td>
<td>Zero or more complete TLVs</td>
<td>Type=0, Length=0</td>
<td></td>
</tr>
<tr>
<td>01:80:c2:00:00:00</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Mandatory TLV</th>
<th>TLV Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis ID</td>
<td>1</td>
<td>Identifies the device</td>
</tr>
<tr>
<td>Port ID</td>
<td>2</td>
<td>Identifies the port</td>
</tr>
<tr>
<td>Time To Live (TTL)</td>
<td>3</td>
<td>Lets the receiving device know how long the received</td>
</tr>
<tr>
<td></td>
<td></td>
<td>information should remain valid.</td>
</tr>
<tr>
<td>End of LLDPDU</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Optional TLVs

Optional TLVs are inserted between the TTL TLV and End of LLDPDU TLV. The basic set of optional TLVs include:

<table>
<thead>
<tr>
<th>Optional TLV</th>
<th>TLV Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Description</td>
<td>4</td>
<td>Displays details about the port</td>
</tr>
<tr>
<td>System Name</td>
<td>5</td>
<td>Displays given name for the device</td>
</tr>
<tr>
<td>System Description</td>
<td>6</td>
<td>Displays version of the software</td>
</tr>
<tr>
<td>System Capabilities</td>
<td>7</td>
<td>Describes the primary function and capabilities of the device.</td>
</tr>
<tr>
<td>Management Address</td>
<td>8</td>
<td>Displays the IP or MAC address of the device</td>
</tr>
</tbody>
</table>

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).
<table>
<thead>
<tr>
<th>TLV</th>
<th>Mandatory/Optional</th>
<th>Value sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis ID</td>
<td>Mandatory</td>
<td>System MAC address</td>
</tr>
<tr>
<td>Port ID</td>
<td>Mandatory</td>
<td>Port sys port ID as an integer</td>
</tr>
<tr>
<td>Time-to-Live</td>
<td>Mandatory</td>
<td>120s</td>
</tr>
<tr>
<td>System Name</td>
<td>Optional</td>
<td>System Name</td>
</tr>
<tr>
<td>Port Description</td>
<td>Optional</td>
<td>Port ID in slot-port format, like 1-1</td>
</tr>
<tr>
<td>System Description</td>
<td>Optional</td>
<td>PFOS Platform</td>
</tr>
</tbody>
</table>
| Management Address    | Optional           | IPv4 Address or IPv6 address if the IPv4 address is set to 0.0.0.0  
|                       |                    | **Note:** 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 enable and Tx disable.
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.

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".

<table>
<thead>
<tr>
<th>Local Port</th>
<th>Chassis ID</th>
<th>Hold Time</th>
<th>System Name</th>
<th>System Desc</th>
<th>Management Address</th>
<th>Remote Port</th>
<th>Port Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>8c:ea:1b:ff:b9:9e</td>
<td>120</td>
<td>PFS-5010-Node119</td>
<td>PFS7010</td>
<td>10.250.177.119</td>
<td>27</td>
<td>1-27</td>
</tr>
<tr>
<td>1-30</td>
<td>8c:ea:1b:ff:b9:9e</td>
<td>120</td>
<td>PFS-5010-Node119</td>
<td>PFS7010</td>
<td>10.250.177.119</td>
<td>49</td>
<td>1-49.1</td>
</tr>
<tr>
<td>1-40</td>
<td>8c:ea:1b:ff:b9:9e</td>
<td>120</td>
<td>PFS-5010-Node119</td>
<td>PFS7010</td>
<td>10.250.177.119</td>
<td>50</td>
<td>1-49.2</td>
</tr>
<tr>
<td>1-7</td>
<td>8c:ea:1b:ff:b9:9e</td>
<td>120</td>
<td>PFS-5010-Node119</td>
<td>PFS7010</td>
<td>10.250.177.119</td>
<td>13</td>
<td>1-13</td>
</tr>
</tbody>
</table>
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 not allowed on Inline Network ports.

- **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 (IPSs) 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.

- **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 within 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. Unless otherwise specified, these tasks are discussed in this chapter.

1. Decide which ports will carry inline traffic or will be used for passive monitoring. Configure the physical settings of the ports. Refer to [Configuring Ports](#), earlier in this document.

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. Refer to [Port Groups](#) earlier in this document.

3. Create a simple tool chain with traffic flow over inline tools in series. Refer to [Simple Tool Chaining](#).

4. Create advanced tool chains for more complicated service chains. Refer to [Advanced Tool Chaining](#)

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. Refer to LinkSafe.

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.

**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.

![Simple Tool Chain Diagram](Image)

*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.

<table>
<thead>
<tr>
<th>Port ID</th>
<th>Name</th>
<th>Class</th>
<th>Link</th>
<th>Speed</th>
<th>XCVR Model</th>
<th>XCVR Type</th>
<th>PWR Rx (dBm)</th>
<th>PWR Tx (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>S1-1_B5</td>
<td>Inline-Network</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FCLF8922P2BTL</td>
<td>1000Base-T</td>
<td>-N/A</td>
<td>-N/A</td>
</tr>
<tr>
<td>1-2</td>
<td>S1-2_TZone</td>
<td>Inline-Network</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FCLF8922P2BTL</td>
<td>1000Base-T</td>
<td>-N/A</td>
<td>-N/A</td>
</tr>
<tr>
<td>1-3</td>
<td>S2-1_B5</td>
<td>Inline-Network</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FCLF8922P2BTL</td>
<td>1000Base-T</td>
<td>-N/A</td>
<td>-N/A</td>
</tr>
<tr>
<td>1-4</td>
<td>S2-2_TZone</td>
<td>Inline-Network</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FCLF8922P2BTL</td>
<td>1000Base-T</td>
<td>-N/A</td>
<td>-N/A</td>
</tr>
<tr>
<td>1-17</td>
<td>AED_A</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>INNOLIGHT TR-PX855-NR3</td>
<td>1G/10GBase-SR</td>
<td>-2.75</td>
<td>-2.98</td>
</tr>
<tr>
<td>1-18</td>
<td>AED_B</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>INNOLIGHT TR-PX855-NR3</td>
<td>1G/10GBase-SR</td>
<td>-2.42</td>
<td>-3.05</td>
</tr>
<tr>
<td>1-21</td>
<td>T1_JPX-1</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>INNOLIGHT TR-PX855-NR3</td>
<td>1G/10GBase-SR</td>
<td>-3.48</td>
<td>-3.02</td>
</tr>
<tr>
<td>1-22</td>
<td>T1_JPX-2</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>INNOLIGHT TR-PX855-NR3</td>
<td>1G/10GBase-SR</td>
<td>-3.78</td>
<td>-2.92</td>
</tr>
<tr>
<td>1-23</td>
<td>T2_JPX-1</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FTLX9571DBCV</td>
<td>1G/10GBase-SR</td>
<td>-2.47</td>
<td>-2.21</td>
</tr>
<tr>
<td>1-24</td>
<td>T2_JPX-2</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FTLX9571DBCV</td>
<td>1G/10GBase-SR</td>
<td>-2.41</td>
<td>-2.37</td>
</tr>
<tr>
<td>1-31</td>
<td>T5_OC8</td>
<td>Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FTLX9571DBCV</td>
<td>1G/10GBase-SR</td>
<td>-2.56</td>
<td>-2.43</td>
</tr>
<tr>
<td>1-32</td>
<td>T6_OC8</td>
<td>Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FTLX9571DBCV</td>
<td>1G/10GBase-SR</td>
<td>-1.19</td>
<td>-1.94</td>
</tr>
<tr>
<td>1-33</td>
<td>T7_OC8</td>
<td>Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FTLX9571DBCV</td>
<td>1G/10GBase-SR</td>
<td>-2.31</td>
<td>-2.17</td>
</tr>
<tr>
<td>1-34</td>
<td>T8_OC8</td>
<td>Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FTLX9571DBCV</td>
<td>1G/10GBase-SR</td>
<td>-2.29</td>
<td>-2.25</td>
</tr>
</tbody>
</table>

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.
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 following graphic shows example inline monitor port configuration for the IPS components in Figure 6.1. See Port Groups for configuration details.

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.
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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Used in Maps</th>
<th>Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>All_Traffic</td>
<td>0</td>
<td>0</td>
<td>( mac offset 0 0 mask 0 )</td>
</tr>
<tr>
<td>WebTraffic</td>
<td>0</td>
<td>0</td>
<td>( Dest Port 443 or Dest Port 80 or Dest Port 81 ) or ( Src Port 443 or Src Port 80 or Src Port 81 )</td>
</tr>
<tr>
<td>nonmatch</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>unfiltered</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

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.

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.

   - 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.

### 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.

![Advanced Tool Chain Use Case Diagram](image_url)

*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.

<table>
<thead>
<tr>
<th>Port ID</th>
<th>Name</th>
<th>Class</th>
<th>Link</th>
<th>Speed</th>
<th>XCVR Model</th>
<th>XCVR Type</th>
<th>PWR Rx (dBm)</th>
<th>PWR Tx (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>S1-1_P1</td>
<td>Inline-Network</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FCLF6521P28TL</td>
<td>1000Base-T</td>
<td>-N/A</td>
<td>-N/A</td>
</tr>
<tr>
<td>1-2</td>
<td>S1-2_P2</td>
<td>Inline-Network</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FCLF6521P28TL</td>
<td>1000Base-T</td>
<td>-N/A</td>
<td>-N/A</td>
</tr>
<tr>
<td>1-3</td>
<td>S2-1_P3</td>
<td>Inline-Network</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FCLF6521P28TL</td>
<td>1000Base-T</td>
<td>-N/A</td>
<td>-N/A</td>
</tr>
<tr>
<td>1-4</td>
<td>S2-2_P4</td>
<td>Inline-Network</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FCLF6521P28TL</td>
<td>1000Base-T</td>
<td>-N/A</td>
<td>-N/A</td>
</tr>
<tr>
<td>1-13</td>
<td>nDA_1A</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>INNOLIGHT TR-PX855-NRS</td>
<td>10/10GBase-SR</td>
<td>2.86</td>
<td>3.27</td>
</tr>
<tr>
<td>1-14</td>
<td>nDA_1B</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>INNOLIGHT TR-PX855-NRS</td>
<td>10/10GBase-SR</td>
<td>2.68</td>
<td>3.25</td>
</tr>
<tr>
<td>1-15</td>
<td>nDA_2A</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>INNOLIGHT TR-PX855-NRS</td>
<td>10/10GBase-SR</td>
<td>2.72</td>
<td>3.04</td>
</tr>
<tr>
<td>1-16</td>
<td>nDA_2B</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>INNOLIGHT TR-PX855-NRS</td>
<td>10/10GBase-SR</td>
<td>2.86</td>
<td>3.86</td>
</tr>
<tr>
<td>1-17</td>
<td>AED_A</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>INNOLIGHT TR-PX855-NRS</td>
<td>10/10GBase-SR</td>
<td>2.91</td>
<td>1.05</td>
</tr>
<tr>
<td>1-18</td>
<td>AED_B</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>INNOLIGHT TR-PX855-NRS</td>
<td>10/10GBase-SR</td>
<td>2.48</td>
<td>3.91</td>
</tr>
<tr>
<td>1-21</td>
<td>T1_IPX-1</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>INNOLIGHT TR-PX855-NRS</td>
<td>10/10GBase-SR</td>
<td>3.54</td>
<td>3.06</td>
</tr>
<tr>
<td>1-22</td>
<td>T1_IPX-2</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>INNOLIGHT TR-PX855-NRS</td>
<td>10/10GBase-SR</td>
<td>3.77</td>
<td>2.92</td>
</tr>
<tr>
<td>1-23</td>
<td>T2_IPX-1</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FXLX575T138CV</td>
<td>10/10GBase-SR</td>
<td>2.45</td>
<td>2.25</td>
</tr>
<tr>
<td>1-24</td>
<td>T2_IPX-2</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FXLX575T138CV</td>
<td>10/10GBase-SR</td>
<td>2.42</td>
<td>2.45</td>
</tr>
<tr>
<td>1-25</td>
<td>T3_IPX-1</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FXLX575T138CV</td>
<td>10/10GBase-SR</td>
<td>3.91</td>
<td>1.97</td>
</tr>
<tr>
<td>1-26</td>
<td>T3_IPX-2</td>
<td>Inline-Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FXLX575T138CV</td>
<td>10/10GBase-SR</td>
<td>1.65</td>
<td>2.55</td>
</tr>
<tr>
<td>1-31</td>
<td>T5_OOB</td>
<td>Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FXLX575T138CV</td>
<td>10/10GBase-SR</td>
<td>2.65</td>
<td>2.51</td>
</tr>
<tr>
<td>1-32</td>
<td>T6_OOB</td>
<td>Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FXLX575T138CV</td>
<td>10/10GBase-SR</td>
<td>1.17</td>
<td>2.02</td>
</tr>
<tr>
<td>1-33</td>
<td>T7_OOB</td>
<td>Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FXLX575T138CV</td>
<td>10/10GBase-SR</td>
<td>2.36</td>
<td>2.19</td>
</tr>
<tr>
<td>1-34</td>
<td>T8_OOB</td>
<td>Monitor</td>
<td>up</td>
<td>1000</td>
<td>FINISAR CORP. FXLX575T138CV</td>
<td>10/10GBase-SR</td>
<td>2.25</td>
<td>2.14</td>
</tr>
</tbody>
</table>
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.

![Inline Network Port Groups](image)

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.

![Inline Monitor Port Groups](image)
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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Lb Criteria</th>
<th>pfMesh Visibility</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>T5_OOB-1</td>
<td>enable</td>
<td>enable</td>
<td>PortGroupNameResolved</td>
</tr>
<tr>
<td>T6_OOB-2</td>
<td>enable</td>
<td>enable</td>
<td>PortGroupNameResolved</td>
</tr>
<tr>
<td>T7_OOB-3</td>
<td>enable</td>
<td>enable</td>
<td>PortGroupNameResolved</td>
</tr>
<tr>
<td>T8_OOB-4</td>
<td>enable</td>
<td>enable</td>
<td>PortGroupNameResolved</td>
</tr>
</tbody>
</table>

Forwarding Filters

The following graphic shows example forwarding filtering configuration for the network traffic in Figure 6.2. See Forwarding Filters for filter configuration details.

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.
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).

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.
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.

![Diagram of A-Side and B-Side Next Tools](image)

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.
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.

7. Add passive monitoring ports group for each tool
8. Click **Apply** in the toolbar to save the settings to the running configuration.

9. 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.
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”.

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.

**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):

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.

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.

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:
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 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/OSPF/RSVP/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 3296 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 supports the following modules:
  - 1G Copper, RJ45 CAT5e, 2 segments
  - 10G/1G Copper, RJ45 CAT6a, 2 segments
  - 1G/10G/40G/100G SM LC, 2 segments
  - 1G/10G 50um MM SX/SR LC, 2 segments
  - 1G/10G 62.5um 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 3296 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 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.

Viewing PowerSafe Hardware Details

You can view the External PowerSafe TAP device details on the Hardware>PowerSafe page.
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.

For all segments on the External PowerSafe device, you can configure Segment Name, Poweroff Mode, and Manual Mode, and Inline Network Ports.

Poweroff Mode

The Poweroff Mode setting defines the connection state that the segment adopts if and when power to the PFS device is lost. The PowerSafe segments will adopt the programmed state automatically when power is lost to the PFS device, and they will not come out of this state until the PFS device is fully up and running again. 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 feature 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.
- **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 3296 must have the Power Safe option enabled. Refer to the Inline Network Port Group settings.
7 Maintenance

These tasks help you maintain and update PFOS:

Uploading Files
Downloading Files
Saving and Loading Configurations
Maintaining Core Files
Maintaining Certificate Files
Maintaining SSH Public Key Files
Maintaining NTP Key Files
Maintaining Log Files
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.
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.

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.
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

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.

Saving 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:

![Core Files Table](core-files-table.png)

**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 File Options](core-file-options.png)

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**

![Log File Options](log-file-options.png)
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**.

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.
Maintaining Certificate Files

PFOS enables you to manage several types of certificate files:

<table>
<thead>
<tr>
<th>Certificate Type</th>
<th>Files</th>
<th>Acquired By</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transport Layer Security (TLS)</strong></td>
<td>server.key - Private key file</td>
<td>PFOS provides default files that are installed at startup and allow any new installation to support HTTPS.</td>
</tr>
<tr>
<td>Provides authentication and data encryption</td>
<td>server.crt - Contains Certificate Authority (CA) certificate and public key</td>
<td>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, as a client certificate for Syslog TLS mutual authentication (see <a href="#">Add a Syslog Server</a> for details). Note: You cannot use PFOS to create a private key or a self-signed certificate; CAs or other trusted authorities generate these files.</td>
</tr>
</tbody>
</table>
| Certificate-Authority                   | xxxxxxxxxx.crt - A certificate file is considered a certificate-authority certificate if the Basic Constraint flag is TRUE. | • PFOS only allows one certificate authority file to be uploaded and installed at a time. You must delete an existing certificate authority file before you can upload a new file.  
• If one or more intermediate certificates and CA certificate are required, you need to concatenate these certificates to a single file with the CA certificate at the bottom.  
• If [Common Criteria mode](#) is enabled, and a CA certificate is not present on the system, a new user certificate upload will be successful, but the install will fail. |
| Certificate Signing Requests (CSRs)     | xxxxxxxxx.key - Private key file (file name is user defined)           | This file can be generated by using the CLI command `generate csr`. PFOS generates a new private key file and the `server.csr`. Both these files are copied to certificate folder. Refer to the [PFOS CLI Reference Guide](#) for details. |
| Contains information a CA needs to create the TLS certificate. | server.csr - Contains CA certificate and public key                   |                                                                                                       |
| Certificate Revoke List (CRL)           | xxxxxxxxx.crl - Private key file (file name is user defined)           | CAs or other trusted authorities generate CRL files; PFOS does not generate .crl files.                |
| Contains a list of revoked digital certificates |                                                                 |                                                                                                       |

Installing Certificate Files

To install a properly signed private key and CA certificate, each file must first be uploaded to PFOS, and then a valid key pair can be installed.

Refer to the following sections for details:
• **Upload a Certificate File**
• **View, Install, or Delete Certificate Files**

**Upload a Certificate 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** or **Certificate-Authority**.

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 and 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. PFOS does not support TLS keys protected by passphrases.

**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 Certificate section of the File Management page. All currently saved certificates and private keys are displayed.
3. To display details about any one item, or to access the certificate editor for any item except the default certificate, 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.

### Maintaining SSH Public Key Files

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.

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

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

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

**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.
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.

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)
```

<table>
<thead>
<tr>
<th>Key Number</th>
<th>An integer from 1-65534 used for identifying each key-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Method</td>
<td>Specify either <strong>MD5</strong> and <strong>SHA1</strong>. For STIG or FIPS compliance, use only <strong>SHA1</strong>.</td>
</tr>
<tr>
<td>Key-value</td>
<td>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.</td>
</tr>
</tbody>
</table>

Upload an NTP Key File

1. Once you have created an NTP key file, go to **File Management > Upload File to Chassis**.
2. In the **Type** drop-down list, select **NTP key**.
3. 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.

![NTP Key](image)

**Note:** To delete a file, click the name of the file and click **Delete** to delete it.

4. Refer to Timing Sources > NTP to configure NTP servers and assign authentication keys.

**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.

![Network tab](image)

2. Click the number of the management interface that you want to configure.
3. Enter the desired IP address(es).

![IP configuration](image)

4. 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.

![Switchover button](image)

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.

For details on uploading specific types of configuration files, refer to the following sections in this chapter:

- 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

On the front panel

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:
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*.

On the rear of the chassis

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.

On the Hardware page, the active and standby management modules are shown on the Management Modules tab:

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.
8 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
Syslog Messages
nGeniusONE PFS Monitoring

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 Page](image)
Statistics

The Statistics page in the Status section shows tabular and graphical views of activity on various system components. Select **Network**, **Deduplication**, **Flow**, or **Control Packets**.

Click a listed slot to display information for all of the configured ports in that slot.

![Statistics Table](image)

**Network statistics**

The following example shows network statistics for a specific slot.

![Network Statistics](image)

The statistics for each port on the line card include:

- **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) Drops**: 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.

To reset network statistics, select the type of statistics (Network or Deduplication), select a slot number, click **Reset Counters**, and then select either **This slot only** or **All network counters**.

To see additional counters, click the wrench icon.

Statistics for Span-Monitor ports are displayed under one physical port.

**Deduplication statistics**

On systems with one or more line cards that support deduplication, the following example shows deduplication statistics for a specific slot.

![Deduplication Statistics](image)

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.

To reset deduplication statistics, click **Reset Counters**, and then select either **This slot only** or **All Deduplication counters**.
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.

Note: 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.

View flow statistics by port or by map

1. Select the desired option, Ports or Maps, at the top of the page:

2. When Ports is selected, to view by port, click a slot number, and then click the desired port. The flow statistics display.
3. When Maps is selected, the flow statistics by map display.

To reset flow statistics, click Reset Counters, and then select either This slot only or All Flow counters.

Control packets statistics

Control packet statistics show information for tunnel termination and pfsMesh on specific ports of a selected line card.
The statistics for each port on the line card include:

- **(Rx/Tx) ARP Packets**: Receive/transmit ARP packet count.
- **(Rx/Tx) ICMP Packets**: Receive/transmit ICMP packet count.
- **(Rx/Tx) pfsMesh Packets**: Number of pfsMesh packets received/transmitted.
- **Drop Packets**: Dropped packets, either excessive or checksum failure packets.

To reset control packet statistics, click **Reset Counters**, and then select either **This slot only** or **All Control Packets counters**.

**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.
Alarms

This page displays the alarm status of each alarm unit on the system. To view additional information about a single alarm unit, click the name in the leftmost column.
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.

  ![Hardware Information](image)

- **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.
- **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.

- **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.
- **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.

  ![](image)

- **Power Supplies**: ID and state.

  ![](image)

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 [Traps/Notifications](#) 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
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 System Settings.

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 “SNMP” in Configuring System Settings.

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:

- 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
- Target MIB (RFC 3413); OID 1.3.6.1.6.3.1.12.1 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.
- 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.

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-category Event</th>
<th>Event</th>
<th>Severity</th>
<th>Enum</th>
<th>Current Syslog String Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication:</td>
<td>access:</td>
<td>LOGIN</td>
<td>NOTICE</td>
<td>0</td>
<td>SysAccCtl. Logged in User:$user,IP:$IP, Context:webui,AccessType:HTTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOGIN_FAILED</td>
<td>WARNING</td>
<td>1</td>
<td>SysAccCtl. Login failed User:$user,IP:$IP, Context:webui,AccessType:HTTP, reason: noauth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOGOUT</td>
<td>NOTICE</td>
<td>2</td>
<td>SysAccCtl. Logged out User:$user,IP:$IP, Context:webui,AccessType:HTTP</td>
</tr>
<tr>
<td></td>
<td>LICENSE_AGREEMENT_</td>
<td>NOTICE</td>
<td>NOTICE</td>
<td>3</td>
<td>SysAccCtl. License agreement accepted User:$user IP:$IP,context:$context</td>
</tr>
<tr>
<td>Category</td>
<td>Sub-category Event</td>
<td>Event</td>
<td>Severity</td>
<td>Enum</td>
<td>Current Syslog String Displayed</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------</td>
<td>---------------------------</td>
<td>----------</td>
<td>------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Port:</td>
<td>basic:</td>
<td>PORT_NAME_CHANGED</td>
<td>NOTICE</td>
<td>4</td>
<td>PortCfgChg. ($slot-$port) Name Chgd from $name to $name by $user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PORT_CLASS_CHANGED</td>
<td>NOTICE</td>
<td>5</td>
<td>PortCfgChg. ($slot-$port) Class Chgd from $class to $class by $user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PORT_LINK_STATE_CHANGED</td>
<td>NOTICE</td>
<td>6</td>
<td>PortCfgChg. ($slot-$port) Link state Chgd from $link to $link by $user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PORT_SPEED_CHANGED</td>
<td>NOTICE</td>
<td>7</td>
<td>PortCfgChg. ($slot-$port) Speed Chgd from $speed to $speed by $user</td>
</tr>
<tr>
<td>advanced:</td>
<td>PORT_STAMPING_CHANGED</td>
<td></td>
<td>NOTICE</td>
<td>8</td>
<td>PortCfgChg. ($slot-$port) Port stamping Chgd from $state to $state by $user</td>
</tr>
<tr>
<td></td>
<td>PORT_TIME_STAMPING_Chg</td>
<td></td>
<td>NOTICE</td>
<td>9</td>
<td>PortCfgChg. ($slot-$port) Time stamping Chgd from $state to $state by user $user</td>
</tr>
<tr>
<td></td>
<td>PORT_GEO_PROBE_TIME_FORMAT_CHANGED</td>
<td></td>
<td>NOTICE</td>
<td>10</td>
<td>PortCfgChg. ($slot-$port) geo probe time format Chgd from $state to $state by user $user</td>
</tr>
<tr>
<td></td>
<td>PORT_VN_TAG_STRIPPING_Chg</td>
<td></td>
<td>NOTICE</td>
<td>11</td>
<td>PortCfgChg. ($slot-$port) Vntag stripping Chgd from $state to $state by $user</td>
</tr>
<tr>
<td></td>
<td>PORT_DEDUP_SETTING_CHANGED</td>
<td></td>
<td>NOTICE</td>
<td>12</td>
<td>PortCfgChg. ($slot-$port) extended load balance Chgd from $state to $state by user $user</td>
</tr>
<tr>
<td></td>
<td>PORT_EXTENDED LB_CHANGED</td>
<td></td>
<td>NOTICE</td>
<td>13</td>
<td>PortCfgChg. ($slot-$port) Dedup setting Chgd from $state to $state by user $user</td>
</tr>
<tr>
<td></td>
<td>PORT_PROTOCOL_STRIPING_CHANGED</td>
<td></td>
<td>NOTICE</td>
<td>14</td>
<td>PortCfgChg. ($slot-$port) protocol stripping setting Chgd from $state to $state by user $user</td>
</tr>
<tr>
<td></td>
<td>PORT_VLAN_TAG_STRIPING_Chg</td>
<td></td>
<td>NOTICE</td>
<td>15</td>
<td>PortCfgChg. ($slot-$port) VLAN tag stripping Chgd from $state to $state by $user</td>
</tr>
<tr>
<td>Category</td>
<td>Sub-category Event</td>
<td>Event</td>
<td>Severity</td>
<td>Enum</td>
<td>Current Syslog String Displayed</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------</td>
<td>-------------</td>
<td>-----------</td>
<td>------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>PORT_SLICING_</td>
<td>NOTICE</td>
<td>PortCfgChg.</td>
<td>16</td>
<td></td>
<td>($slot-$port) slicing Chgd from $state to $state by user $user</td>
</tr>
<tr>
<td>CHANGED</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>APP_MASKDEF_LIB_ADDED</td>
<td>NOTICE</td>
<td>17</td>
<td>AppCfgChg. Maskdef lib $name is added by user $user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PORT_TUNNEL_</td>
<td>WARNING</td>
<td>18</td>
<td>PortCfgChg. Appending Port: $slot-$port in tunnel termination Group: tt1 by $user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CHANGED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System:</td>
<td>access-ctl:</td>
<td>SYS_ACC_CTL_ROLE_CHANGED</td>
<td>NOTICE</td>
<td>19</td>
<td>SysCfgChg. Acc Ctrl role $role is added/deleted/modified: rule $rule added[access: $access, context:$context, feature:$feature] by $user</td>
</tr>
<tr>
<td></td>
<td>SYS_ACC_CTL_USER_CHANGED</td>
<td>NOTICE</td>
<td>20</td>
<td>SysCfgChg. Acc Ctrl user $user is added/deleted/modified: password Set, role:$role by $user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYS_ACC_CTL_AUTH_ORDER_CHANGED</td>
<td>NOTICE</td>
<td>21</td>
<td>SysCfgChg. Acc Ctrl authentication order Chgd to $order_new by $user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYS_ACC_CTL_RADIUS_CHANGED</td>
<td>NOTICE</td>
<td>22</td>
<td>SysCfgChg. Acc Ctrl RADIUS server $host is added/deleted/modified: [port:$port, timeout:$timeout, retransmit:$retransmit key Set] by $user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYS_ACC_CTL_TACACS_CHANGED</td>
<td>NOTICE</td>
<td>23</td>
<td>SysCfgChg. Acc Ctrl TACACS server $host is added/deleted/modified: [port:$port, timeout:$timeout, retransmit:$retransmit key Set] by $user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>info:</td>
<td>SYS_INFO_NAME_CHANGED</td>
<td>NOTICE</td>
<td>24</td>
<td>SysCfgChg. Name Chgd from $value1 to $value2 by $user</td>
</tr>
<tr>
<td>Category</td>
<td>Sub-category Event</td>
<td>Event</td>
<td>Severity</td>
<td>Enum</td>
<td>Current Syslog String Displayed</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------</td>
<td>------------------------------------</td>
<td>----------</td>
<td>------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td></td>
<td>SYS_INFO_CONTACT_CHANGED</td>
<td>NOTICE</td>
<td>NOTICE 25</td>
<td>SysCfgChg. Contact Chgd from $value1 to $value2 by $user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYS_INFO_LOCATION_CHANGED</td>
<td>NOTICE</td>
<td>NOTICE 26</td>
<td>SysCfgChg. Location Chgd from $value1 to $value2 by $user.</td>
<td></td>
</tr>
<tr>
<td>features:</td>
<td>SYS_FIPS_MODE_FEATURE_CHANGED</td>
<td>NOTICE</td>
<td>NOTICE 28</td>
<td>SysCfgChg. FIPS mode setting Chgd from 'state' to 'state' by $user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYS_ACC_MGMT_SSH_CLI_CHANGED</td>
<td>NOTICE</td>
<td>NOTICE 29</td>
<td>SysCfgChg. CLI with SSH access is $enabled/disabled at port $port by $user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYS_ACC_MGMT_HTTP_WEBUI_CHANGED</td>
<td>NOTICE</td>
<td>NOTICE 31</td>
<td>SysCfgChg. web UI with HTTP access is $enabled/disabled at port $port by $user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYS_ACC_MGMT_HTTP_NETCONF_CHANGED</td>
<td>NOTICE</td>
<td>NOTICE 32</td>
<td>SysCfgChg. NETCONF with HTTP access is $enabled/disabled at port $port by $user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYS_ACC_MGMT_HTTPS_WEBUI_CHANGED</td>
<td>NOTICE</td>
<td>NOTICE 33</td>
<td>SysCfgChg. web UI with HTTPS access is $enabled/disabled at port $port by $user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYS_ACC_MGMT_HTTPS_NETCONF_CHANGED</td>
<td>NOTICE</td>
<td>NOTICE 34</td>
<td>SysCfgChg. NETCONF with HTTPS access is $enabled/disabled at port $port by $user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYS_ACC_MGMT_FRONT_PANEL_CHANGED</td>
<td>NOTICE</td>
<td>NOTICE 35</td>
<td>SysCfgChg. Front Panel enabled/disabled by $user.</td>
<td></td>
</tr>
<tr>
<td>network:</td>
<td>SYS_NETWORK_CHANGED</td>
<td>NOTICE</td>
<td>NOTICE 36</td>
<td>SysCfgChg. Network Settings Chgd from '$value1' to '$value2' by $user.</td>
<td></td>
</tr>
<tr>
<td>notifications:</td>
<td>SYS_SYSLOG_CHANGED</td>
<td>NOTICE</td>
<td>NOTICE 37</td>
<td>SysCfgChg. Syslog server settings Chgd from 'state' to 'state' by $user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SYS_TRACE_LOG_CHANGED</td>
<td>NOTICE</td>
<td>NOTICE 38</td>
<td>SysCfgChg. Trace log settings of $facility Chgd from $state to $state by $user.</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Sub-category Event</td>
<td>Event</td>
<td>Severity</td>
<td>Enum</td>
<td>Current Syslog String Displayed</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------</td>
<td>--------------------------------------</td>
<td>----------</td>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SYS_LCD_CHANGED</td>
<td>NOTICE</td>
<td>39</td>
<td>SysCfgChg. LCD setting Chgd from 'state' to 'state' by $user.</td>
</tr>
<tr>
<td>timing-</td>
<td></td>
<td>SYS_TIMING_SOURCE_TIME_CHANGED</td>
<td>NOTICE</td>
<td>40</td>
<td>SysCfgChg. Timing source Chgd from $value to $value by user $user.</td>
</tr>
<tr>
<td></td>
<td>sources:</td>
<td>SYS_TIMING_SOURCE_NTP_CHANGED</td>
<td>NOTICE</td>
<td>41</td>
<td>SysCfgChg. NTP servers Chgd from $value to $value by user $user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SYS_TIMING_SOURCE_GPS_CHANGED</td>
<td>NOTICE</td>
<td>42</td>
<td>SysCfgChg. GPS cable length Chgd from $value to $value by user $user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SYS_TIMING_SOURCE_PTP_CHANGED</td>
<td>NOTICE</td>
<td>43</td>
<td>SysCfgChg. PTP setting Chgd from $value to $value by user $user.</td>
</tr>
<tr>
<td></td>
<td>Source Port VLAN</td>
<td>SYS_MONITOR_PORT_VLAN_TAG_CHANGED</td>
<td>NOTICE</td>
<td>44</td>
<td>SysCfgChg. Monitor port VLAN tagging Chgd from 'type' to 'type' by $user.</td>
</tr>
<tr>
<td></td>
<td>tagging:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic:</td>
<td>map:</td>
<td>FLOWMAP_ADDED</td>
<td>NOTICE</td>
<td>45</td>
<td>TrfCfgChg. Map $map filter: $filter input ports: $slot-$port output ports: $slot-$port is added by user $user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FLOWMAP_DELETED</td>
<td>NOTICE</td>
<td>46</td>
<td>TrfCfgChg. Map $map is deleted by user $user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FLOWMAP_MODIFIED</td>
<td>NOTICE</td>
<td>47</td>
<td>TrfCfgChg. Map $map is modified by user $user</td>
</tr>
<tr>
<td></td>
<td>lbg:</td>
<td>LBG_ADDED</td>
<td>NOTICE</td>
<td>48</td>
<td>TrfCfgChg. LBG $lbg ports: $slot-$port failover action: $failover_action type: $type is added by user $user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LBG_DELETED</td>
<td>NOTICE</td>
<td>49</td>
<td>TrfCfgChg. LBG $lbg is deleted by user $user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LBG_MODIFIED</td>
<td>NOTICE</td>
<td>50</td>
<td>TrfCfgChg. LBG $lbg $item from [original_setting] to [new_setting] is modified by user $user</td>
</tr>
<tr>
<td></td>
<td>filter:</td>
<td>FILTER_ADDED</td>
<td>NOTICE</td>
<td>51</td>
<td>TrfCfgChg. Filter $filter expression: $expression is added by user $user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FILTER_DELETED</td>
<td>NOTICE</td>
<td>52</td>
<td>TrfCfgChg. Filter $filter is deleted by user $user</td>
</tr>
<tr>
<td>Category</td>
<td>Sub-category Event</td>
<td>Event</td>
<td>Severity</td>
<td>Enum</td>
<td>Current Syslog String Displayed</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------</td>
<td>-------</td>
<td>----------</td>
<td>------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td></td>
<td>FILTER_MODIFIED</td>
<td>NOTICE</td>
<td>53</td>
<td>TrfCfgChg. Filter $filter expression from $original_expression to $new_expression is modified by user $user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>lb-criteria:</td>
<td>LB_CRITERIA_ADDED</td>
<td>NOTICE</td>
<td>54</td>
<td>TrfCfgChg. LB criteria $criteria is added by user $user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LB_CRITERIA_DELETED</td>
<td>NOTICE</td>
<td>55</td>
<td>TrfCfgChg. LB criteria $criteria is deleted by user $user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LB_CRITERIA_MODIFIED</td>
<td>NOTICE</td>
<td>56</td>
<td>TrfCfgChg. LB criteria $criteria is modified by user $user.</td>
</tr>
<tr>
<td></td>
<td>applications:</td>
<td>dedup: APP_DEDUP_LIB_ADDED</td>
<td>NOTICE</td>
<td>57</td>
<td>AppCfgChg. Deduplication lib $lib is added by user $user.</td>
</tr>
<tr>
<td></td>
<td>protocol:</td>
<td>protocol APP_PROTOCOL_ADDED</td>
<td>NOTICE</td>
<td>59</td>
<td>AppCfgChg. Application protocol $protocol is added by user $user.</td>
</tr>
<tr>
<td></td>
<td>protocol:</td>
<td>protocol APP_PROTOCOL_DELETED</td>
<td>NOTICE</td>
<td>60</td>
<td>AppCfgChg. Application protocol $protocol is deleted by user $user.</td>
</tr>
<tr>
<td></td>
<td>protocol:</td>
<td>protocol APP_PROTOCOL_MODIFIED</td>
<td>NOTICE</td>
<td>61</td>
<td>AppCfgChg. Application protocol $protocol is modified by user $user.</td>
</tr>
<tr>
<td></td>
<td>mpls-l3:</td>
<td>mpls-l3 APP_MPLS-L3_ADDED</td>
<td>NOTICE</td>
<td>62</td>
<td>AppCfgChg. Application mpls-l3 $mpls-l3 is added by user $user.</td>
</tr>
<tr>
<td>Category</td>
<td>Sub-category Event</td>
<td>Event</td>
<td>Severity</td>
<td>Enum</td>
<td>Current Syslog String Displayed</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------</td>
<td>-------</td>
<td>----------</td>
<td>------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td></td>
<td>APP_MPLS-L3_DELETED</td>
<td>NOTICE</td>
<td>67</td>
<td>AppCfgChg. Application mpls-l3 $mpls-l3 is deleted by user $user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>APP_MPLS-L3_MODIFIED</td>
<td>NOTICE</td>
<td>68</td>
<td>AppCfgChg. Application mpls-l3 $mpls-l3 modified by user $user.</td>
<td></td>
</tr>
<tr>
<td>extended lb:</td>
<td>APP_EXTENDED_LB_ADDED</td>
<td>NOTICE</td>
<td>69</td>
<td>AppCfgChg. Application extended lb $lib is added by user $user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>APP_EXTENDED_LB_DELETED</td>
<td>NOTICE</td>
<td>70</td>
<td>AppCfgChg. Application extended lb $lib is deleted by user $user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>APP_EXTENDED_LB_MODIFIED</td>
<td>NOTICE</td>
<td>71</td>
<td>AppCfgChg. Application extended lb $lib is modified by user $user.</td>
<td></td>
</tr>
<tr>
<td>ELB protocol:</td>
<td>APP_ELB_PROTOCOL_ADDED</td>
<td>NOTICE</td>
<td>72</td>
<td>AppCfgChg. Application elb protocol $protocol is added by user $user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>APP_ELB_PROTOCOL_DELETED</td>
<td>NOTICE</td>
<td>73</td>
<td>AppCfgChg. Application elb protocol $protocol is deleted by user $user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>APP_ELB_PROTOCOL_MODIFIED</td>
<td>NOTICE</td>
<td>74</td>
<td>AppCfgChg. Application elb protocol $protocol modified by user $user.</td>
<td></td>
</tr>
<tr>
<td>VLAN-tag:</td>
<td>APP_VLAN_TAG_STRIP_LIB_ADDED</td>
<td>NOTICE</td>
<td>75</td>
<td>AppCfgChg. Application vlan tag strip lib $lib is added by user $user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>APP_VLAN_TAG_STRIP_LIB_DELETED</td>
<td>NOTICE</td>
<td>76</td>
<td>AppCfgChg. Application vlan tag strip lib $lib is deleted by user $user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>APP_VLAN_TAG_STRIP_LIB_MODIFIED</td>
<td>NOTICE</td>
<td>77</td>
<td>AppCfgChg. Application vlan tag strip lib $lib modified by user $user.</td>
<td></td>
</tr>
<tr>
<td>port-filter:</td>
<td>APP_PORT_FILTER_ADDED</td>
<td>NOTICE</td>
<td>78</td>
<td>AppCfgChg. Advanced-filter $filter is added by user $user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>APP_PORT_FILTER_DELETED</td>
<td>NOTICE</td>
<td>79</td>
<td>AppCfgChg. Advanced-filter $filter is deleted by user $user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>APP_PORT_FILTER_MODIFIED</td>
<td>NOTICE</td>
<td>80</td>
<td>AppCfgChg. Advanced-filter $filter modified by user $user.</td>
<td></td>
</tr>
<tr>
<td>offset:</td>
<td>APP_OFFSET_LIB_ADDED</td>
<td>NOTICE</td>
<td>81</td>
<td>AppCfgChg. Offset lib $lib is added by user $user.</td>
<td></td>
</tr>
</tbody>
</table>
### Chassis

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-category Event</th>
<th>Event</th>
<th>Severity</th>
<th>Enum</th>
<th>Current Syslog String Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fru: Line Card:</td>
<td></td>
<td>CARD_LC_INSERT</td>
<td>NOTICE</td>
<td>89</td>
<td>SysHS. Line card inserted in slot $slot.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_LC_REMOVE</td>
<td>NOTICE</td>
<td>90</td>
<td>SysHS. Line card removed from slot $slot.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_LC_RESET</td>
<td>INFORMATION</td>
<td>91</td>
<td>SysHS. Linecard $slot has been reset. (not work when resetting from shutdown state)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_LC_SHUTDOWN</td>
<td>NOTICE</td>
<td>92</td>
<td>SysHS. Line card shutdown for slot $slot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_LC_UPGRADE</td>
<td>NOTICE</td>
<td>93</td>
<td>SysHS, Line card firmware $upgrade_action for slot $slot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_LC_FAILURE</td>
<td>CRITICAL</td>
<td>94</td>
<td>SysHS. Line card $slot went to a failed state</td>
</tr>
<tr>
<td>Fabric Card:</td>
<td></td>
<td>CARD_FC_INSERT</td>
<td>NOTICE</td>
<td>95</td>
<td>SysHS. fabric card inserted in slot $slot.</td>
</tr>
<tr>
<td>Category</td>
<td>Sub-Category Event</td>
<td>Event</td>
<td>Severity</td>
<td>Enum</td>
<td>Current Syslog String Displayed</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------</td>
<td>---------------------</td>
<td>----------</td>
<td>------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Fabric</td>
<td></td>
<td>CARD_FC_REMOVE</td>
<td>NOTICE</td>
<td>96</td>
<td>SysHS. Fabric card removed from slot $slot.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_FC_SHUTDOWN</td>
<td>NOTICE</td>
<td>97</td>
<td>SysHS. Fabric card shutdown for slot $slot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_FC_FAILURE</td>
<td>ERROR</td>
<td>98</td>
<td>SysHS. Fabric card failure for slot $slot</td>
</tr>
<tr>
<td>CPU Card</td>
<td></td>
<td>CARD_CPU_INSERT</td>
<td>NOTICE</td>
<td>99</td>
<td>SysHS. CPU card A inserted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_CPU_REMOVE</td>
<td>NOTICE</td>
<td>100</td>
<td>SysHS. CPU card A removed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_CPU_UPGRADE</td>
<td>NOTICE</td>
<td>101</td>
<td>SysHS. CPU card firmware is upgrading</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_CPU_FAILURE</td>
<td>ERROR</td>
<td>102</td>
<td>SysHS. CPU card A failed</td>
</tr>
<tr>
<td>Fan tray</td>
<td></td>
<td>CARD_FAN_INSERT</td>
<td>NOTICE</td>
<td>103</td>
<td>SysHS. Fan Tray inserted in slot $slot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_FAN_Remove</td>
<td>NOTICE</td>
<td>104</td>
<td>SysHS. Fan Tray removed from slot $slot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_FAN_SPEED_READ_ERROR</td>
<td>ERROR</td>
<td>105</td>
<td>SysHS. Fan speed read error in tray $tray fan:$fan_idx_list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_FAN_ABSENT</td>
<td>ERROR</td>
<td>106</td>
<td>SysHS. $device $slot - fans are missing</td>
</tr>
<tr>
<td>Power supply</td>
<td></td>
<td>CARD_PWR_SUPPLY_INSERT</td>
<td>NOTICE</td>
<td>107</td>
<td>SysHS. Power Supply Unit inserted in slot $slot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_PWR_SUPPLY_REMOVE</td>
<td>NOTICE</td>
<td>108</td>
<td>SysHS. Power Supply Unit removed from slot $slot</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CARD_PWR_SUPPLY_ERROR</td>
<td>ERROR</td>
<td>109</td>
<td>SysHS. Power supply $slot is $status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WARMSTART</td>
<td>NOTICE</td>
<td>130</td>
<td>Sys. Warmstart.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>REBOOT</td>
<td>NOTICE</td>
<td>111</td>
<td>Sys. Reboot with option:reboot is issued by $user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FACTORY_RESET</td>
<td>NOTICE</td>
<td>112</td>
<td>Sys. Reboot with option:factory reset is issued by $user</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CLEAR_CONFIG</td>
<td>NOTICE</td>
<td>113</td>
<td>Sys. Reboot with option:clear configuration is issued by $user</td>
</tr>
<tr>
<td>core-</td>
<td>dump:</td>
<td>CORE_FILES_PRESENT</td>
<td>NOTICE</td>
<td>114</td>
<td>Sys. Core files present</td>
</tr>
<tr>
<td>Category</td>
<td>Sub-category Event</td>
<td>Event</td>
<td>Severity</td>
<td>Enum</td>
<td>Current Syslog String Displayed</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------</td>
<td>-------------------------</td>
<td>----------</td>
<td>------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td></td>
<td>CORE_FILE_DELETED</td>
<td>NOTICE</td>
<td>116</td>
<td></td>
<td>Sys. Core dump file $file deleted by user $user</td>
</tr>
<tr>
<td></td>
<td>disk-space:</td>
<td>DISK_USAGE_WARNING</td>
<td>WARNING</td>
<td>117</td>
<td>Sys. Disk usage is above the warning level. Current usage: $sda_type $percentage%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DISK_USAGE_ALERT</td>
<td>ALERT</td>
<td>118</td>
<td>Sys. Disk usage is at a critical level. Current usage: $sda_type $percentage%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DISK_USAGE_NORMAL</td>
<td>NOTICE</td>
<td>240</td>
<td>Sys. Disk usage is normal. Current usage: '%s&quot;, diskUsage</td>
</tr>
<tr>
<td>file-mgmt:</td>
<td>SOFTWARE_UPLOADED</td>
<td>NOTICE</td>
<td>119</td>
<td></td>
<td>Sys. VXOS software pkg $pkg Uploaded by user $user</td>
</tr>
<tr>
<td></td>
<td>SOFTWARE_INSTALLED</td>
<td>NOTICE</td>
<td>120</td>
<td></td>
<td>Sys. VXOS software pkg $pkg installed by user $user</td>
</tr>
<tr>
<td></td>
<td>SOFTWARE_DELETED</td>
<td>NOTICE</td>
<td>121</td>
<td></td>
<td>Sys. VXOS software pkg $pkg deleted by user $user</td>
</tr>
<tr>
<td></td>
<td>FIRMWARE_UPLOADED</td>
<td>NOTICE</td>
<td>122</td>
<td></td>
<td>Sys. VXOS firmware pkg $pkg Uploaded by user $user</td>
</tr>
<tr>
<td></td>
<td>FIRMWARE_INSTALLED</td>
<td>NOTICE</td>
<td>123</td>
<td></td>
<td>Sys. VXOS firmware pkg $pkg installed by user $user</td>
</tr>
<tr>
<td></td>
<td>FIRMWARE_DELETED</td>
<td>NOTICE</td>
<td>124</td>
<td></td>
<td>Sys. VXOS firmware pkg $pkg deleted by user $user</td>
</tr>
<tr>
<td></td>
<td>CONFIGURATION_FILE_UPLOADED</td>
<td>NOTICE</td>
<td>125</td>
<td></td>
<td>Sys. VXOS Configuration file $file Uploaded by user $user</td>
</tr>
<tr>
<td></td>
<td>CONFIGURATION_FILE_DELETED</td>
<td>NOTICE</td>
<td>127</td>
<td></td>
<td>Sys. VXOS Configuration file $file deleted by user $user</td>
</tr>
<tr>
<td></td>
<td>STARTUP_CONFIG_DELETED</td>
<td>NOTICE</td>
<td>128</td>
<td></td>
<td>Sys. Startup-config is deleted by user $user</td>
</tr>
<tr>
<td>coldstart:</td>
<td>COLDSTART</td>
<td>NOTICE</td>
<td>129</td>
<td></td>
<td>Cold Start (power-up)</td>
</tr>
<tr>
<td></td>
<td>CHASSIS_DEFAULT_MAC_ALERT</td>
<td>NOTICE</td>
<td>132</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port:</td>
<td>in-out:</td>
<td>XCVR_INSERT</td>
<td>INFORMATION</td>
<td>135</td>
<td>SysPort. XCVR inserted into ($slot-$port)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>XCVR_REMOVE</td>
<td>INFORMATION</td>
<td>136</td>
<td>SysPort. XCVR removed from ($slot-$port)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>XCVR_MISMATCH</td>
<td>WARNING</td>
<td>137</td>
<td>SysPort. XCVR mismatched in ports $slot-$port</td>
</tr>
<tr>
<td>link-state:</td>
<td>LINK_UP</td>
<td>WARNING</td>
<td>138</td>
<td></td>
<td>SysPort. Port $slot-$port is now online (link up)</td>
</tr>
<tr>
<td>Category</td>
<td>Sub-category Event</td>
<td>Event</td>
<td>Severity</td>
<td>Enum</td>
<td>Current Syslog String Displayed</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------</td>
<td>------------</td>
<td>----------</td>
<td>------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>LINK_DOWN</td>
<td>ALERT</td>
<td>139</td>
<td></td>
<td>SysPort. Port $slot-$port is offline (link down)</td>
</tr>
<tr>
<td></td>
<td>TEMPERATURE_HIGH</td>
<td>NOTICE</td>
<td>147</td>
<td></td>
<td>SysEnv. Temperature ALERT: High temperature threshold reached</td>
</tr>
<tr>
<td></td>
<td>CARD_TEMPERATURE_HIGH</td>
<td>ERROR</td>
<td>157</td>
<td></td>
<td>SysEnv. Temperature out-of-range ALARM: Absolute High temperature threshold 80 degrees reached. Slot $slot</td>
</tr>
</tbody>
</table>
Frequently Asked Questions

Will the system work when power fails?

If all LEDs are off, then the system is not receiving power. When power is off, or when power failure occurs, the system maintains the uninterrupted throughput of network traffic with 100% integrity. However, this traffic is not regenerated to the monitoring ports. The user can at all times be certain of a 100% network uplink when power is lost.

Can I feed my system with data from an existing optical tap?

Yes; all that is required is connecting the external tap output port into the desired network Rx port on your system. Some of the optical signal appears on the matching network port Tx output due to the internal loop-through on inline devices.

Can I mix 50μm and 62.5μm fiber devices?

Multi-mode fiber of different sizes can be mixed, but the link might show significantly higher losses. Typically, light exiting 50μm fiber into 62.5μm fiber has about the same loss as a normal connection. However, going from 62.5μm fiber to 50μm fiber incurs a 1-6dB higher loss due to light escaping out the side of the larger diameter fiber. Any such arrangements should be verified with an optical power meter.

Can I mix single-mode and multi-mode fiber?

Usually not. Most single-mode and multi-mode device operate on different wavelengths. If both devices operate on the same wavelength, a special cable can be used to allow such connections. However, there are optical power losses and other problems associated with such devices.

My copper 10/100/1000 SFP transceiver will not link at 10Mbps and 100Mbps.

The PFS 5000/7000 and 6000 Series do not support 10Mbps and 100Mbps speeds.

A standard SFP transceiver will operate only at 1G, not 10M or 100M. Therefore, any SFP that is 1G-only (copper or fiber) will work. These SFPs have a serializer/deserializer (SERDES) interface on the back side, which the SFP standard requires.

There are also non-standard SFPs that support 10/100/1000 copper. These devices use Serial Gigabit Media Independent Interface (SGMII) as the interface, which is similar but not interchangeable. Some SFPs support both SERDES and SGMII, but require special programming to work right.

Most gigabit devices support SERDES or SGMII SFPs, unless they require special programming. The safest bet is to use 1G-only modules, which will always be SERDES and SFP standard compliant.
Some SFPs do not default to auto-negotiation enabled. NETSCOUT does not pre-configure SFPs and assumes that, when SFPs are inserted, they are ready to link up automatically with the correct default settings listed on the datasheet of the SFP. NETSCOUT recommends that you use SFPs on which auto-negotiation is enabled by default.

**Whom do I contact if I cannot find the solution in this guide?**

For further assistance, contact NETSCOUT customer support.
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.
- **Type 3**: Used in forwarding filters.

The syntax for Type 2 and Type 3 filter expressions is the same, except that Type 2 filter expressions have these differences:

- In the following table, items with range can be specified with a range of values, such as value1-value2, except for IP address ranges, which must use a base address and a mask. For Type 2 filter expressions, an IP address range is specified using – instead of mask, and is only for IPv4.
- No support for type in Type 2 filter expressions.
- No support for offset in Type 2 filter expressions.
- No support for inner_vlan in Type 2 filter expressions.

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 in this document for the maximum possible filter resources available for use.

<table>
<thead>
<tr>
<th>Packet field</th>
<th>Alternate forms</th>
<th>Comparison value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac source</td>
<td>mac source address&lt;br&gt;ethernet source address&lt;br&gt;source (mac</td>
<td>ethernet) address&lt;br&gt;[bidi</td>
</tr>
</tbody>
</table>
### Table A.1 - Packet fields in filter expressions (continued)

<table>
<thead>
<tr>
<th>Packet field</th>
<th>Alternate forms</th>
<th>Comparison value</th>
</tr>
</thead>
<tbody>
<tr>
<td>etype</td>
<td>[mac</td>
<td>ethernet] etype value</td>
</tr>
</tbody>
</table>
| 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.  
  **Note:** 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. |
| vlan         | [mac|ethernet] {outer|inner} vlanid value | Decimal value in the range 0-4095. 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. |
| priority     | [mac|ethernet] {outer|inner} pri 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. |
### Table A.1 - Packet fields in filter expressions (continued)

<table>
<thead>
<tr>
<th>Packet field</th>
<th>Alternate forms</th>
<th>Comparison value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip source</td>
<td>ip {source</td>
<td>src} {address</td>
</tr>
<tr>
<td>ip destination</td>
<td>ip dest[ination] {address</td>
<td>range} dest[ination] ip {address</td>
</tr>
<tr>
<td>ip tos</td>
<td>ip tos value</td>
<td>8-bit value specified as two hexadecimal digits.</td>
</tr>
<tr>
<td>ip protocol</td>
<td>ip prot value</td>
<td>Decimal value 0-255.</td>
</tr>
<tr>
<td>ip flow</td>
<td>ip flow value</td>
<td>20-bit value specified as five hexadecimal digits, as per RFC3232.</td>
</tr>
<tr>
<td>14 source port</td>
<td>{14</td>
<td>tcp</td>
</tr>
</tbody>
</table>
### Table A.1 - Packet fields in filter expressions (continued)

<table>
<thead>
<tr>
<th>Packet field</th>
<th>Alternate forms</th>
<th>Comparison value</th>
</tr>
</thead>
<tbody>
<tr>
<td>l4 destination port</td>
<td>{l4</td>
<td>tcp</td>
</tr>
<tr>
<td>type</td>
<td>type tcpflag</td>
<td>Filter packets based on various combinations of TCP flags. Valid values for tcpflag are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPSyn SYN bit is set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPNotSyn SYN bit is not set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPFIN FIN bit is set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPNotFin FIN bit is not set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPRST RST bit is set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPNotRst RST bit is not set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPPSH PSH bit is set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPNotPSH PSH bit is not set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPACK ACK bit is set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPNotACK ACK bit is not set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPURG URG bit is set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPNotURG URG bit is not set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPCwr CWR bit is set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPNotCwr CWR bit is not set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPECN ECN bit is set</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCPNotECN ECN bit is not set</td>
</tr>
</tbody>
</table>

TCP flag filter fields are not supported in Type 2 (advanced) filters. The TCPCwr, TCPNotCwr, TCPECN, and TCPNotECN TCP flags are not supported on the PFS 5010/7010.
### Packet fields in filter expressions (continued)

<table>
<thead>
<tr>
<th>Packet field</th>
<th>Alternate forms</th>
<th>Comparison value</th>
</tr>
</thead>
<tbody>
<tr>
<td>offset</td>
<td>{mac</td>
<td>ip</td>
</tr>
</tbody>
</table>
Configuring SNMP

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 5.5 CLI Reference Guide for CLI command details.

<table>
<thead>
<tr>
<th>Steps</th>
<th>Web UI</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Enable SNMP and Configure SNMP Versions</td>
<td>Notifications&gt;SNMP&gt;Agent</td>
<td>snmp agent agent-options</td>
</tr>
<tr>
<td>2 Create a New SNMP Community (Optional)</td>
<td>Notifications&gt;SNMP&gt;Community</td>
<td>snmp community community-options</td>
</tr>
<tr>
<td>3 Add Security Name to View-Based Access Control Model (Optional)</td>
<td>Notifications&gt;SNMP&gt;VACM</td>
<td>snmp vacm vacm-options</td>
</tr>
<tr>
<td>4 Grant Access Rights to the VACM Group</td>
<td>Notifications&gt;SNMP&gt;VACM</td>
<td>snmp vacm vacm-options</td>
</tr>
<tr>
<td>5 Limit SNMP Access Rights</td>
<td>Notifications&gt;SNMP&gt;VACM</td>
<td>snmp vacm vacm-options</td>
</tr>
</tbody>
</table>
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).

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.

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.

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 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.

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.
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.

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Applicable Security Models</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-no-priv</td>
<td>Any, v3</td>
<td>A connection that is secured with a passphrase and authentication but no encryption.</td>
</tr>
<tr>
<td>auth-priv</td>
<td>Any, v3</td>
<td>A connection that is secured with both authentication and encryption.</td>
</tr>
<tr>
<td>no-auth-no-priv</td>
<td>Any, v1, v2c, v3</td>
<td>A connection that uses a simple passphrase (known as a shared secret) to secure the communication.</td>
</tr>
</tbody>
</table>

4. Select Read, Write, and Notify MIB Views.
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
```

The second example uses `snmpget` and `snmpset` commands for the specified OID for the default public community.

```
``
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”.

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.

4. Then use SystemParams as the Write View for Security Model “any”.

B Configuring SNMP
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).

**Note:** You may also leave “Write View” as empty, then it'll give no permission to set any OID.

### 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 5.5 CLI Reference Guide** for CLI command details.

<table>
<thead>
<tr>
<th>Steps</th>
<th>Web UI</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong> Enable SNMP and Configure SNMP Versions</td>
<td>Notifications&gt;SNMP&gt;Agent</td>
<td>snmp agent agent-options</td>
</tr>
<tr>
<td><strong>2</strong> Create a User-Based Security Model (USM) with Authentication and Privacy</td>
<td>Notifications&gt;SNMP&gt;USM</td>
<td>snmp community community-options</td>
</tr>
<tr>
<td><strong>3</strong> Add the USM User to VACM Group</td>
<td>Notifications&gt;SNMP&gt;VACM</td>
<td>snmp vasm vasm-options</td>
</tr>
<tr>
<td><strong>4</strong> Request Authentication and Privacy Password for USM</td>
<td>Notifications&gt;SNMP&gt;VACM</td>
<td>snmp usm usm-options</td>
</tr>
<tr>
<td><strong>5</strong> Limit Access Rights for SNMPSet</td>
<td>Notifications&gt;SNMP&gt;VACM</td>
<td>snmp vasm vasm-options</td>
</tr>
</tbody>
</table>
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.

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.
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 "" -1 noAuthNoPriv 10.250.176.149
```

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.
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 "" -1 noAuthNoPriv
10.250.176.149 iso
```

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 "" -1 AuthPriv
10.250.176.149 iso
```
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.

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.
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).

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 5.5 CLI Reference Guide for CLI command details.

<table>
<thead>
<tr>
<th>Steps</th>
<th>Web UI</th>
<th>CLI</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 SNMP Notify Tags</td>
<td>Notifications&gt;SNMP&gt;Notify</td>
<td>snmp notify notify-options</td>
</tr>
<tr>
<td>2 Add Trap Receiver IP Address to Target Table</td>
<td>Notifications&gt;SNMP&gt;Target</td>
<td>snmp target target-options</td>
</tr>
</tbody>
</table>
### 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.

---

#### Add Trap Receiver IP Address to Target Table

You can create a Trap Receiver at Notifications>SNMP>Target.
SNMP v2c Receiver Example
The following page shows an SNMP v2c Receiver example.

- 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.

- 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.
Notifications>Events

Select different categories of event notifications by enabling Syslog, SNMP, or NETCONF for each function.
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.

![Example Third-Party SNMP Trap Receiver](image)

**Variable Bindings:**

- **Name:** iso.org.dod.internet.mgmt.mib-2.system.sysUpTime
  - **Value:** [TimeTicks] 8 minutes 15 seconds (37758)
- **Name:** snmpTrapOID
  - **Value:** [OID] linkUp
- **Name:** iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifIndex
  - **Value:** [Integer] 47
- **Name:** iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifAdminStatus
  - **Value:** [Integer] up (1)
- **Name:** iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus
  - **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.
SNMP MIB and Trap Definitions

This appendix 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.

Traps/Notifications

Interfaces MIB Traps

The following traps from the Interfaces MIB (RFC 2863) are supported.

<table>
<thead>
<tr>
<th>Object</th>
<th>linkDown</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>1.3.6.1.6.3.1.1.5.3</td>
</tr>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>IF-MIB (RFC 2863)</td>
</tr>
<tr>
<td>Trap Components</td>
<td>ifIndex</td>
</tr>
<tr>
<td>ifAdminStatus</td>
<td>ifOperStatus</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

ClearTrap | linkUp

<table>
<thead>
<tr>
<th>Object</th>
<th>linkUp</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>1.3.6.1.6.3.1.1.5.4</td>
</tr>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>IF-MIB (RFC 2863)</td>
</tr>
<tr>
<td>Trap Components</td>
<td>ifIndex</td>
</tr>
<tr>
<td>ifAdminStatus</td>
<td>ifOperStatus</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
</tbody>
</table>

ClearTrap | linkDown
VSS Enterprise MIB Traps

The following traps from VSS-SYSTEM-MIB are supported.

<table>
<thead>
<tr>
<th>Object</th>
<th>vsTempHighNotif</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.21671.3.1.0.2</td>
</tr>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>VSS-SYSTEM-MIB</td>
</tr>
<tr>
<td>Trap Components</td>
<td>vsTemperatureStatusDescr</td>
</tr>
<tr>
<td></td>
<td>vsTemperatureStatusValue</td>
</tr>
<tr>
<td>Description</td>
<td>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.</td>
</tr>
<tr>
<td>Description String</td>
<td>&quot;Temperature of Line Card# %d has reached a high state&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Temperature of Fabric Module# %d has reached a high state&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Temperature of Management Module# %d has reached a high state&quot;</td>
</tr>
<tr>
<td>ClearTrap</td>
<td>vsTempNormalNotif</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Object</th>
<th>vsCfgChangeNotif</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.21671.3.1.0.3</td>
</tr>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>VSS-SYSTEM-MIB</td>
</tr>
<tr>
<td>Trap Components</td>
<td>vsCfgChangeTime</td>
</tr>
<tr>
<td></td>
<td>vsCfgChangeCommandSrc</td>
</tr>
<tr>
<td></td>
<td>vsCfgChangeCommandUser</td>
</tr>
<tr>
<td></td>
<td>vsCfgChangeCommandSrcAddrType</td>
</tr>
<tr>
<td></td>
<td>vsCfgChangeCommandSrcAddr</td>
</tr>
<tr>
<td></td>
<td>vsCfgChangeNode</td>
</tr>
<tr>
<td></td>
<td>vsCfgChangeDescr</td>
</tr>
<tr>
<td>Description</td>
<td>A vsCfgChangeNotif is generated by the managed system when any configuration on the system has changed.</td>
</tr>
<tr>
<td>ClearTrap</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Object</th>
<th>vsAuthenticationNotif</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.21671.3.1.0.4</td>
</tr>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>VSS-SYSTEM-MIB</td>
</tr>
<tr>
<td>Trap Components</td>
<td>vsAuthenticationChangeTime</td>
</tr>
<tr>
<td></td>
<td>vsAuthenticationCommandSrc</td>
</tr>
<tr>
<td></td>
<td>vsAuthenticationType</td>
</tr>
<tr>
<td></td>
<td>vsAuthenticationDescr</td>
</tr>
<tr>
<td>Description</td>
<td>A vsAuthenticationNotif is generated by the managed system when a user attempts to access the system.</td>
</tr>
<tr>
<td>Description String</td>
<td>vsAuthenticationChangeTime=07:E3:0A:1B:12:17:38:00:2B:00:00</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>vsAuthenticationCommandSrc=2(cli)</td>
</tr>
<tr>
<td></td>
<td>vsAuthenticationType=LOGIN_SUCCESS/LOGOUT/LOGIN_FAILED/LOGIN_BLOCKED/LICENSE_AGREEMENT_ACCEPTED/EVENT_TYPELICENSE_AGREEMENT_DECLINED.</td>
</tr>
<tr>
<td></td>
<td>vsAuthenticationDescr=User:admin,IP:10.200.130.51,AccessType:SSH/HTTPS/UDP</td>
</tr>
<tr>
<td>ClearTrap</td>
<td>Self</td>
</tr>
<tr>
<td>Object</td>
<td>vsRestartNotif</td>
</tr>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.21671.3.1.0.5</td>
</tr>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>VSS-SYSTEM-MIB</td>
</tr>
<tr>
<td>Trap Components</td>
<td>vsRestartDescr</td>
</tr>
<tr>
<td>Description</td>
<td>A vsRestartNotif is generated by the managed system when the system or any process is going to restart.</td>
</tr>
<tr>
<td>Description String</td>
<td>&quot;Reboot with option:factory reset is issued by $user for $cmd_mgmt&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Reboot with option:clear configuration is issued by $user&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Reboot is issued by $user for $cmd_mgmt&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Reboot is issued by $user. It will clear configuration due to software downgrade&quot;</td>
</tr>
<tr>
<td>ClearTrap</td>
<td>N/A</td>
</tr>
<tr>
<td>Object</td>
<td>vsFRUInsertedNotif</td>
</tr>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.21671.3.1.0.6</td>
</tr>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>VSS-SYSTEM-MIB</td>
</tr>
<tr>
<td>Trap Components</td>
<td>vsFRUInsertedDescr</td>
</tr>
<tr>
<td>Description</td>
<td>A vsFRUInsertedNotif is generated by the managed system whenever any FRU (Field Replaceable Unit) is inserted in the system.</td>
</tr>
<tr>
<td>Description String</td>
<td>&quot;Line card inserted for slot %d&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Fabric card inserted in slot %d&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Mgmt card %d inserted&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Fan Tray inserted in slot %d&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Power Supply Unit inserted in slot %d&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Powersafe Device found vendor id %X product id %X Modules:&quot;</td>
</tr>
<tr>
<td>ClearTrap</td>
<td>vsFRURemovedNotif</td>
</tr>
<tr>
<td>Object</td>
<td>vsFRURemovedNotif</td>
</tr>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.21671.3.1.0.7</td>
</tr>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>VSS-SYSTEM-MIB</td>
</tr>
<tr>
<td>Trap Components</td>
<td>vsFRURemovedDescr</td>
</tr>
<tr>
<td>Description</td>
<td>A vsFRURemovedNotif is generated by the managed system whenever any FRU (Field Replaceable Unit) is removed from the system.</td>
</tr>
</tbody>
</table>
### 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"

### Clear Trap
- vsFRUInsertedNotif

### 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 in slots $cards in positions $positions by user $user"
- "VXOS firmware pkg $simpleName uploaded by user $user on $dest_mgmt"
- "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"
### 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

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.21671.3.1.0.11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>VSS-SYSTEM-MIB</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.21671.3.1.0.12</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>VSS-SYSTEM-MIB</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.21671.3.1.0.13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>VSS-SYSTEM-MIB</td>
</tr>
</tbody>
</table>

**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
<table>
<thead>
<tr>
<th>Object</th>
<th>vsTriggerPolicyNotif</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.21671.3.1.0.14</td>
</tr>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>VSS-SYSTEM-MIB</td>
</tr>
<tr>
<td>Trap Components</td>
<td>vsTriggerPolicyDescr</td>
</tr>
<tr>
<td>Description</td>
<td>A vsTriggerPolicyNotif is generated by the managed system, when a trigger policy state has changed either from active to inactive or inactive to active.</td>
</tr>
<tr>
<td>Description String</td>
<td>&quot;Trigger profile %s is now true/active&quot; &quot;Trigger profile %s is now false/inactive&quot;</td>
</tr>
<tr>
<td>ClearTrap</td>
<td>Self</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Object</th>
<th>vsFRUErrorNotif</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.21671.3.1.0.15</td>
</tr>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>VSS-SYSTEM-MIB</td>
</tr>
<tr>
<td>Trap Components</td>
<td>vsTriggerPolicyDescr</td>
</tr>
<tr>
<td>Description</td>
<td>A vsFRUErrorNotif is generated by the managed system, whenever any FRU error is detected in the system.</td>
</tr>
<tr>
<td>Description String</td>
<td>&quot;ALARM: Power Supply %d failed&quot; &quot;Powersafe Unable to enable PFS6002 USB power&quot; &quot;Powersafe USB devices not found&quot;</td>
</tr>
<tr>
<td>ClearTrap</td>
<td>vsFRUNormalNotif</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Object</th>
<th>vsFRUNormalNotif</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.21671.3.1.0.16</td>
</tr>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>VSS-SYSTEM-MIB</td>
</tr>
<tr>
<td>Trap Components</td>
<td>vsFRUNormalDescr</td>
</tr>
<tr>
<td>Description</td>
<td>A vsFRUErrorNotif is generated by the managed system, whenever any FRU error is detected in the system.</td>
</tr>
<tr>
<td>Description String</td>
<td>&quot;Power Supply %d is normal&quot;</td>
</tr>
<tr>
<td>ClearTrap</td>
<td>vsFRUErrorNotif</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Object</th>
<th>vsTempNormalNotif</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID</td>
<td>.1.3.6.1.4.1.21671.3.1.0.17</td>
</tr>
<tr>
<td>Status</td>
<td>Current</td>
</tr>
<tr>
<td>MIB</td>
<td>VSS-SYSTEM-MIB</td>
</tr>
<tr>
<td>Trap Components</td>
<td>vsFRUNormalDescr</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>ClearTrap</td>
<td></td>
</tr>
</tbody>
</table>
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

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

<table>
<thead>
<tr>
<th>Object (if)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number</td>
<td>Integer32</td>
<td>1.3.6.1.2.1.2.1.1</td>
<td>The number of network interfaces (regardless of their current state) present on this system</td>
</tr>
</tbody>
</table>

### ifTable

<table>
<thead>
<tr>
<th>Object (if)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Index</td>
<td>1.3.6.1.2.1.2.1.2.1.1</td>
<td>A unique value, greater than zero, for each interface</td>
</tr>
<tr>
<td>Descr</td>
<td>String</td>
<td>1.3.6.1.2.1.2.1.2.1.2</td>
<td>A textual string containing information about the interface</td>
</tr>
<tr>
<td>Type</td>
<td>Type</td>
<td>1.3.6.1.2.1.2.1.2.1.3</td>
<td>The type of interface</td>
</tr>
<tr>
<td>Mtu</td>
<td>Integer32</td>
<td>1.3.6.1.2.1.2.1.2.1.4</td>
<td>The size of the largest packet which can be sent/received on the interface, specified in octets</td>
</tr>
<tr>
<td>Speed</td>
<td>Gauge32</td>
<td>1.3.6.1.2.1.2.1.2.1.5</td>
<td>An estimate of the interface's current bandwidth in bits per second</td>
</tr>
<tr>
<td>PhysAddress</td>
<td>Address</td>
<td>1.3.6.1.2.1.2.1.2.1.6</td>
<td>The interface's address at its protocol sub-layer</td>
</tr>
<tr>
<td>AdminStatus</td>
<td>Integer</td>
<td>1.3.6.1.2.1.2.1.2.1.7</td>
<td>The desired state of the interface</td>
</tr>
<tr>
<td>OperStatus</td>
<td>Integer</td>
<td>1.3.6.1.2.1.2.1.2.1.8</td>
<td>The current operational state of the interface</td>
</tr>
<tr>
<td>LastChange</td>
<td>TimeTicks</td>
<td>1.3.6.1.2.1.2.1.2.1.9</td>
<td>The value of sysUpTime at the time the interface entered its current operational state</td>
</tr>
<tr>
<td>InOctets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.2.1.2.1.10</td>
<td>The total number of octets received on the interface, including framing characters</td>
</tr>
<tr>
<td>InUcastPkts</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.2.1.2.1.11</td>
<td>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</td>
</tr>
<tr>
<td>InDiscards</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.2.1.2.1.13</td>
<td>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</td>
</tr>
<tr>
<td>InErrors</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.2.1.2.1.14</td>
<td>For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol</td>
</tr>
<tr>
<td>InUnknownProtos</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.2.1.2.1.15</td>
<td>For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol</td>
</tr>
<tr>
<td>OutOctets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.2.1.2.1.16</td>
<td>The total number of octets transmitted out of the interface, including framing characters</td>
</tr>
</tbody>
</table>
### OutUcastPkts
- **Type**: Counter32
- **OID**: 1.3.6.1.2.1.2.2.1.17
- **Comment**: 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
- **Type**: Counter32
- **OID**: 1.3.6.1.2.1.2.2.1.19
- **Comment**: The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted.

### OutErrors
- **Type**: Counter32
- **OID**: 1.3.6.1.2.1.2.2.1.20
- **Comment**: For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors.

### ifXTable
<table>
<thead>
<tr>
<th>Object (if)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>1.3.6.1.2.1.31.1.1.1.1</td>
<td>The textual name of the interface</td>
</tr>
<tr>
<td>InMulticastPkts</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.31.1.1.1.2</td>
<td>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</td>
</tr>
<tr>
<td>InBroadcastPkts</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.31.1.1.1.3</td>
<td>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</td>
</tr>
<tr>
<td>OutMulticastPkts</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.31.1.1.1.4</td>
<td>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</td>
</tr>
<tr>
<td>OutBroadcastPkts</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.31.1.1.1.5</td>
<td>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</td>
</tr>
<tr>
<td>HCInOctets</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.31.1.1.1.6</td>
<td>The total number of octets received on the interface, including framing characters</td>
</tr>
<tr>
<td>HCInUcastPkts</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.31.1.1.1.7</td>
<td>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</td>
</tr>
<tr>
<td>Object (if)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
<td>----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>HCInMulticastPkts</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.31.1.1.1.8</td>
<td>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</td>
</tr>
<tr>
<td>HCInBroadcastPkts</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.31.1.1.1.9</td>
<td>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</td>
</tr>
<tr>
<td>HCOOutOctets</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.31.1.1.1.10</td>
<td>The total number of octets transmitted out of the interface, including framing characters</td>
</tr>
<tr>
<td>HCOOutUcastPkts</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.31.1.1.1.11</td>
<td>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</td>
</tr>
<tr>
<td>HCOOutMulticastPkts</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.31.1.1.1.12</td>
<td>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</td>
</tr>
<tr>
<td>HCOOutBroadcastPkts</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.31.1.1.1.13</td>
<td>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</td>
</tr>
<tr>
<td>LinkUpDownTrapEnable</td>
<td>Integer</td>
<td>1.3.6.1.2.1.31.1.1.1.14</td>
<td>Indicates whether linkUp/linkDown traps should be generated for this interface</td>
</tr>
<tr>
<td>HighSpeed</td>
<td>Gauge32</td>
<td>1.3.6.1.2.1.31.1.1.1.15</td>
<td>An estimate of the interface’s current bandwidth in units of 1,000,000 bits per second</td>
</tr>
<tr>
<td>PromiscuousMode</td>
<td>TruthValue</td>
<td>1.3.6.1.2.1.31.1.1.1.16</td>
<td>This object has a value of false(2) if this interface only accepts packets/frames that are addressed to this station</td>
</tr>
<tr>
<td>ConnectorPresent</td>
<td>TruthValue</td>
<td>1.3.6.1.2.1.31.1.1.1.17</td>
<td>This object has the value true(1) if the interface sublayer has a physical connector and the value ‘false(2)’ otherwise</td>
</tr>
<tr>
<td>Alias</td>
<td>String</td>
<td>1.3.6.1.2.1.31.1.1.1.18</td>
<td>This object is an alias name for the interface as specified by a network manager, and provides a non-volatile handle for the interface</td>
</tr>
<tr>
<td>CounterDiscontinuityTime</td>
<td>TimeStamp</td>
<td>1.3.6.1.2.1.31.1.1.1.19</td>
<td>The value of sysUpTime on the most recent occasion at which any one or more of this interface’s counters suffered a discontinuity</td>
</tr>
</tbody>
</table>
RMON-MIB (RFC 2819)

The following statistics from the RMON-MIB (RFC 2819) are supported.

<table>
<thead>
<tr>
<th>Object(etherStats)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Integer32</td>
<td>1.3.6.1.2.1.16.1.1.1.1</td>
<td>A unique value that identifies an etherStats entry.</td>
</tr>
<tr>
<td>DataSource</td>
<td>OBJECT IDENTIFIER</td>
<td>1.3.6.1.2.1.16.1.1.1.2</td>
<td>The source of the data that this etherStats entry is configured to analyze.</td>
</tr>
<tr>
<td>DropEvents</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.3</td>
<td>The total number of events in which packets were dropped by the probe due to lack of resources.</td>
</tr>
<tr>
<td>Octets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.4</td>
<td>The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Pkts</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.5</td>
<td>The total number of packets (including bad packets, broadcast packets, and multicast packets) received.</td>
</tr>
<tr>
<td>BroadcastPkts</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.6</td>
<td>The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.</td>
</tr>
<tr>
<td>MulticastPkts</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.7</td>
<td>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.</td>
</tr>
<tr>
<td>CRCAlignErrors</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.8</td>
<td>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).</td>
</tr>
<tr>
<td>UndersizePkts</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.9</td>
<td>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.</td>
</tr>
<tr>
<td>OversizePkts</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.10</td>
<td>The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td>Object(etherStats)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------</td>
<td>----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Fragments</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.11</td>
<td>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).</td>
</tr>
<tr>
<td>Jabbers</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.12</td>
<td>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).</td>
</tr>
<tr>
<td>Collisions</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.13</td>
<td>The best estimate of the total number of collisions on this Ethernet segment.</td>
</tr>
<tr>
<td>Pkts64Octets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.14</td>
<td>The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>Pkts65to127Octets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.15</td>
<td>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).</td>
</tr>
<tr>
<td>Pkts128to255Octets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.16</td>
<td>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).</td>
</tr>
<tr>
<td>Pkts256to511Octets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.17</td>
<td>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).</td>
</tr>
<tr>
<td>Pkts512to1023Octets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.18</td>
<td>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).</td>
</tr>
<tr>
<td>Pkts1024to1518Octets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.1.1.19</td>
<td>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).</td>
</tr>
<tr>
<td>Object(etherStats)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Owner</td>
<td>OwnerString</td>
<td>1.3.6.1.2.1.16.1.1.1.20</td>
<td>The entity that configured this entry and is therefore using the resources assigned to it.</td>
</tr>
<tr>
<td>Status</td>
<td>EntryStatus</td>
<td>1.3.6.1.2.1.16.1.1.1.21</td>
<td>The status of this etherStats entry.</td>
</tr>
</tbody>
</table>

**HC-RMON-MIB (RFC 3273)**

The following statistics from the HC-RMON-MIB (RFC 3273) are supported.

**etherStatsHighCapacityTable**

<table>
<thead>
<tr>
<th>Object (etherStatsHighCapacity)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>OverflowPkts</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.7.1.1</td>
<td>The number of times the associated etherStatsPkts counter has overflowed.</td>
</tr>
<tr>
<td>Pkts</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.16.1.7.1.2</td>
<td>The total number of packets (including bad packets, broadcast packets, and multicast packets) received.</td>
</tr>
<tr>
<td>OverflowOctets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.7.1.3</td>
<td>The number of times the associated etherStatsOctets counter has overflowed.</td>
</tr>
<tr>
<td>Octets</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.16.1.7.1.4</td>
<td>The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>OverflowPkts64Octets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.7.1.5</td>
<td>The number of times the associated etherStatsPkts-64Octets counter has overflowed.</td>
</tr>
<tr>
<td>Pkts64Octets</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.16.1.7.1.6</td>
<td>The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).</td>
</tr>
<tr>
<td>OverflowPkts65to127Octets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.7.1.7</td>
<td>The number of times the associated etherStats-Pkts65to127Octets counter has overflowed.</td>
</tr>
<tr>
<td>Pkts65to127Octets</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.16.1.7.1.8</td>
<td>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).</td>
</tr>
<tr>
<td>Object (etherStatsHighCapacity)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------</td>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Pkts65to127Octets</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.16.1.7.1.8</td>
<td>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).</td>
</tr>
<tr>
<td>OverflowPkts128to255Octets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.7.1.9</td>
<td>The number of times the associated etherStats-Pkts128to255Octets counter has overflowed.</td>
</tr>
<tr>
<td>Pkts128to255Octets</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.16.1.7.1.10</td>
<td>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).</td>
</tr>
<tr>
<td>OverflowPkts256to511Octets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.7.1.11</td>
<td>The number of times the associated etherStatsPkts256to511Octets counter has overflowed.</td>
</tr>
<tr>
<td>Pkts256to511Octets</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.16.1.7.1.12</td>
<td>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).</td>
</tr>
<tr>
<td>OverflowPkts512to1023Octets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.7.1.13</td>
<td>The number of times the associated etherStats-Pkts512to1023Octets counter has overflowed.</td>
</tr>
<tr>
<td>Pkts512to1023Octets</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.16.1.7.1.14</td>
<td>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).</td>
</tr>
<tr>
<td>OverflowPkts1024to1518Octets</td>
<td>Counter32</td>
<td>1.3.6.1.2.1.16.1.7.1.15</td>
<td>The number of times the associated etherStats-Pkts1024to1518Octets counter has overflowed.</td>
</tr>
<tr>
<td>Pkts1024to1518Octets</td>
<td>Counter64</td>
<td>1.3.6.1.2.1.16.1.7.1.16</td>
<td>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).</td>
</tr>
</tbody>
</table>
## System Information

### Community MIB

RFC 3584

### snmpCommunityTable

<table>
<thead>
<tr>
<th>Object (snmpCommunity)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>String</td>
<td>1.3.6.1.6.3.18.1.1.1.1</td>
<td>The unique index value of a row in this table</td>
</tr>
<tr>
<td>Name</td>
<td>Octet String</td>
<td>1.3.6.1.6.3.18.1.1.1.2</td>
<td>The community string for which a row in this table represents a configuration</td>
</tr>
<tr>
<td>SecurityName</td>
<td>String</td>
<td>1.3.6.1.6.3.18.1.1.1.3</td>
<td>A human readable string representing the corresponding value of snmpCommunityName in a Security Model independent format</td>
</tr>
<tr>
<td>ContextEngineID</td>
<td>ID</td>
<td>1.3.6.1.6.3.18.1.1.1.4</td>
<td>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</td>
</tr>
<tr>
<td>ContextName</td>
<td>String</td>
<td>1.3.6.1.6.3.18.1.1.1.5</td>
<td>The context in which management information is accessed when using the community string specified by the corresponding instance of snmpCommunityName</td>
</tr>
<tr>
<td>TransportTag</td>
<td>Integer</td>
<td>1.3.6.1.6.3.18.1.1.1.6</td>
<td>This object specifies a set of transport endpoints from which a command responder application will accept management requests</td>
</tr>
<tr>
<td>StorageType</td>
<td>Integer</td>
<td>1.3.6.1.6.3.18.1.1.1.7</td>
<td>The storage type for this conceptual row in the snmpCommunityTable</td>
</tr>
<tr>
<td>Status</td>
<td>Status</td>
<td>1.3.6.1.6.3.18.1.1.1.8</td>
<td>The status of this conceptual row in the snmpCommunityTable</td>
</tr>
</tbody>
</table>

### snmpTargetAddrExtTable

<table>
<thead>
<tr>
<th>Object (snmpTarget)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddrTMask</td>
<td>String</td>
<td>1.3.6.1.6.3.18.1.2.1.1</td>
<td>The mask value associated with an entry in the snmpTargetAddrTable</td>
</tr>
<tr>
<td>AddrMMS</td>
<td>Integer32</td>
<td>1.3.6.1.6.3.18.1.2.1.2</td>
<td>The maximum message size value associated with an entry in the snmpTargetAddrTable</td>
</tr>
</tbody>
</table>
## View-based Access Control Model (VACM) MIB

RFC 3415

**vacmSecurityToGroup**

<table>
<thead>
<tr>
<th>Object (vacm)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurityModel</td>
<td>Integer</td>
<td>1.3.6.1.6.3.16.1.2.1.1</td>
<td>The Security Model, by which the vacmSecurityName referenced by this entry is provided</td>
</tr>
<tr>
<td>SecurityName</td>
<td>String</td>
<td>1.3.6.1.6.3.16.1.2.1.2</td>
<td>The securityName for the principal, represented in a Security Model independent format, which is mapped by this entry to a groupName</td>
</tr>
<tr>
<td>GroupName</td>
<td>String</td>
<td>1.3.6.1.6.3.16.1.2.1.3</td>
<td>The name of the group to which this entry (such as the combination of securityModel and securityName) belongs</td>
</tr>
<tr>
<td>SecurityToGroupStorageType</td>
<td>Integer</td>
<td>1.3.6.1.6.3.16.1.2.1.4</td>
<td>The storage type for this conceptual row</td>
</tr>
<tr>
<td>SecurityToGroupStatus</td>
<td>Integer</td>
<td>1.3.6.1.6.3.16.1.2.1.5</td>
<td>The status of this conceptual row</td>
</tr>
</tbody>
</table>

**vacmAccessTable**

<table>
<thead>
<tr>
<th>Object (vacmAccess)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ContextPrefix</td>
<td>String</td>
<td>1.3.6.1.6.3.16.1.4.1.1</td>
<td>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</td>
</tr>
<tr>
<td>SecurityModel</td>
<td>String</td>
<td>1.3.6.1.6.3.16.1.4.1.2</td>
<td>In order to gain the access rights allowed by this conceptual row, this securityModel must be in use</td>
</tr>
<tr>
<td>SecurityLevel</td>
<td>Integer</td>
<td>1.3.6.1.6.3.16.1.4.1.3</td>
<td>The minimum level of security required in order to gain the access rights allowed by this conceptual row</td>
</tr>
<tr>
<td>ContextMatch</td>
<td>Integer</td>
<td>1.3.6.1.6.3.16.1.4.1.4</td>
<td>If the value of this object is exact(1), then all rows where the contextName exactly matches vacmAccessContextPrefix are selected</td>
</tr>
<tr>
<td>ReadViewName</td>
<td>String</td>
<td>1.3.6.1.6.3.16.1.4.1.5</td>
<td>The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes read access</td>
</tr>
<tr>
<td>WriteViewName</td>
<td>String</td>
<td>1.3.6.1.6.3.16.1.4.1.6</td>
<td>The value of an instance of this object identifies the MIB view of the SNMP context to which this conceptual row authorizes write access</td>
</tr>
<tr>
<td>NotifyViewName</td>
<td>String</td>
<td>1.3.6.1.6.3.16.1.4.1.7</td>
<td>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</td>
</tr>
<tr>
<td>Object (vacmAccess)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------</td>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Storage Type</td>
<td>Integer</td>
<td>1.3.6.1.6.3.16.1.4.1.8</td>
<td>The storage type for this conceptual row</td>
</tr>
<tr>
<td>Status</td>
<td>Integer</td>
<td>1.3.6.1.6.3.16.1.4.1.9</td>
<td>The status of this conceptual row</td>
</tr>
</tbody>
</table>

**vacmMIBViews**

<table>
<thead>
<tr>
<th>Object (vacmViewTreeFamily)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ViewName</td>
<td>String</td>
<td>1.3.6.1.6.3.16.1.5.2.1.1</td>
<td>The human readable name for a family of view subtrees</td>
</tr>
<tr>
<td>Subtree</td>
<td>ID</td>
<td>1.3.6.1.6.3.16.1.5.2.1.2</td>
<td>The MIB subtree which when combined with the corresponding instance of vacmViewTreeFamilyMask defines a family of view subtrees</td>
</tr>
<tr>
<td>Mask</td>
<td>Octet String</td>
<td>1.3.6.1.6.3.16.1.5.2.1.3</td>
<td>The bit mask which, in combination with the corresponding instance of vacmViewTreeFamilySubtree, defines a family of view subtrees</td>
</tr>
<tr>
<td>Type</td>
<td>Integer</td>
<td>1.3.6.1.6.3.16.1.5.2.1.4</td>
<td>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</td>
</tr>
<tr>
<td>StorageType</td>
<td>Type</td>
<td>1.3.6.1.6.3.16.1.5.2.1.5</td>
<td>The storage type for this conceptual row</td>
</tr>
<tr>
<td>Status</td>
<td>Status</td>
<td>1.3.6.1.6.3.16.1.5.2.1.6</td>
<td>The status of this conceptual row</td>
</tr>
</tbody>
</table>

**User-based Security Model (USM) MIB**

**RFC 3414**

**usmStats**

<table>
<thead>
<tr>
<th>Object (usmStats)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>UnsupportedSecLevels</td>
<td>Counter32</td>
<td>1.3.6.1.6.3.15.1.1.1.1</td>
<td>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</td>
</tr>
<tr>
<td>NotInTimeWindows</td>
<td>Counter32</td>
<td>1.3.6.1.6.3.15.1.1.2</td>
<td>The total number of packets received by the SNMP engine which were dropped because they appeared outside of the authoritative SNMP engine's window</td>
</tr>
<tr>
<td>UnknownUserNames</td>
<td>Counter32</td>
<td>1.3.6.1.6.3.15.1.1.3</td>
<td>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</td>
</tr>
</tbody>
</table>
### usmStats

<table>
<thead>
<tr>
<th>Object (usmStats)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>UnknownEngineIDs</td>
<td>Counter32</td>
<td>1.3.6.1.6.3.15.1.1.4</td>
<td>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</td>
</tr>
<tr>
<td>WrongDigests</td>
<td>Counter32</td>
<td>1.3.6.1.6.3.15.1.1.5</td>
<td>The total number of packets received by the SNMP engine which were dropped because they did not contain the expected digest value</td>
</tr>
<tr>
<td>DecryptionErrors</td>
<td>Counter32</td>
<td>1.3.6.1.6.3.15.1.1.6</td>
<td>The total number of packets received by the SNMP engine which were dropped because they could not be decrypted</td>
</tr>
</tbody>
</table>

### usmUser

<table>
<thead>
<tr>
<th>Object (usmUser)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>EngineID</td>
<td>ID</td>
<td>1.3.6.1.6.3.15.1.2.2.1.1</td>
<td>An SNMP engine's administratively-unique identifier</td>
</tr>
<tr>
<td>Name</td>
<td>String</td>
<td>1.3.6.1.6.3.15.1.2.2.1.2</td>
<td>A human readable string representing the name of the user</td>
</tr>
<tr>
<td>SecurityName</td>
<td>String</td>
<td>1.3.6.1.6.3.15.1.2.2.1.3</td>
<td>A human readable string representing the user in Security Model independent format</td>
</tr>
<tr>
<td>CloneFrom</td>
<td>Pointer</td>
<td>1.3.6.1.6.3.15.1.2.2.1.4</td>
<td>A pointer to another conceptual row in this usmUserTable</td>
</tr>
<tr>
<td>AuthProtocol</td>
<td>Type</td>
<td>1.3.6.1.6.3.15.1.2.2.1.5</td>
<td>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</td>
</tr>
<tr>
<td>AuthKeyChange</td>
<td>Change</td>
<td>1.3.6.1.6.3.15.1.2.2.1.6</td>
<td>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</td>
</tr>
<tr>
<td>OwnAuthKeyChange</td>
<td>Change</td>
<td>1.3.6.1.6.3.15.1.2.2.1.7</td>
<td>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</td>
</tr>
<tr>
<td>PrivProtocol</td>
<td>Type</td>
<td>1.3.6.1.6.3.15.1.2.2.1.8</td>
<td>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</td>
</tr>
<tr>
<td>PrivKeyChange</td>
<td>Change</td>
<td>1.3.6.1.6.3.15.1.2.2.1.9</td>
<td>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</td>
</tr>
</tbody>
</table>
### Target MIB

**RFC 3413**

**snmpTargetObjects**

<table>
<thead>
<tr>
<th>Object (snmpTargetAddr)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>1.3.6.1.6.3.12.1.2.1.1.1</td>
<td>The locally arbitrary, but unique identifier associated with this snmpTargetAddrEntry</td>
</tr>
<tr>
<td>TDomain</td>
<td>Domain</td>
<td>1.3.6.1.6.3.12.1.2.1.2</td>
<td>This object indicates the transport type of the address contained in the snmpTargetAddrTAddress object</td>
</tr>
<tr>
<td>TAddress</td>
<td>Address</td>
<td>1.3.6.1.6.3.12.1.2.1.3</td>
<td>This object contains a transport address</td>
</tr>
<tr>
<td>Timeout</td>
<td>Time Interval</td>
<td>1.3.6.1.6.3.12.1.2.1.4</td>
<td>This object should reflect the expected maximum round trip time for communicating with the transport address defined by this row</td>
</tr>
<tr>
<td>RetryCount</td>
<td>Integer32</td>
<td>1.3.6.1.6.3.12.1.2.1.5</td>
<td>This object specifies a default number of retries to be attempted when a response is not received for a generated message</td>
</tr>
<tr>
<td>TagList</td>
<td>List</td>
<td>1.3.6.1.6.3.12.1.2.1.6</td>
<td>This object contains a list of tag values which are used to select target addresses for a particular operation</td>
</tr>
<tr>
<td>Params</td>
<td>String</td>
<td>1.3.6.1.6.3.12.1.2.1.7</td>
<td>The value of this object identifies an entry in the snmpTargetParamsTable</td>
</tr>
<tr>
<td>StorageType</td>
<td>Type</td>
<td>1.3.6.1.6.3.12.1.2.1.8</td>
<td>The storage type for this conceptual row</td>
</tr>
<tr>
<td>RowStatus</td>
<td>Status</td>
<td>1.3.6.1.6.3.12.1.2.1.9</td>
<td>The status of this conceptual row</td>
</tr>
</tbody>
</table>
### snmpTargetParams

<table>
<thead>
<tr>
<th>Object (snmpTargetParams)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>1.3.6.1.6.3.12.1.3.1.1.1</td>
<td>The locally arbitrary, but unique identifier associated with this snmpTargetParamsEntry</td>
</tr>
<tr>
<td>MPModel</td>
<td>Model</td>
<td>1.3.6.1.6.3.12.1.3.1.2</td>
<td>The Message Processing Model to be used when generating SNMP messages using this entry</td>
</tr>
<tr>
<td>SecurityModel</td>
<td>Model</td>
<td>1.3.6.1.6.3.12.1.3.1.3</td>
<td>The Security Model to be used when generating SNMP messages using this entry</td>
</tr>
<tr>
<td>SecurityName</td>
<td>String</td>
<td>1.3.6.1.6.3.12.1.3.1.4</td>
<td>The securityName which identifies the Principal on whose behalf SNMP messages will be generated using this entry</td>
</tr>
<tr>
<td>SecurityLevel</td>
<td>Level</td>
<td>1.3.6.1.6.3.12.1.3.1.5</td>
<td>The Level of Security to be used when generating SNMP messages using this entry</td>
</tr>
<tr>
<td>StorageType</td>
<td>Type</td>
<td>1.3.6.1.6.3.12.1.3.1.6</td>
<td>The storage type for this conceptual row</td>
</tr>
<tr>
<td>RowStatus</td>
<td>Status</td>
<td>1.3.6.1.6.3.12.1.3.1.7</td>
<td>The status of this conceptual row</td>
</tr>
</tbody>
</table>

### Notification MIB

**RFC 3413**

snmpNotifyObjects

<table>
<thead>
<tr>
<th>Object (snmpNotify)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String</td>
<td>1.3.6.1.6.3.13.1.1.1.1</td>
<td>The locally arbitrary, but unique identifier associated with this snmpNotifyEntry</td>
</tr>
<tr>
<td>Tag</td>
<td>Value</td>
<td>1.3.6.1.6.3.13.1.1.1.2</td>
<td>This object contains a single tag value which is used to select entries in the snmpTargetAddrTable</td>
</tr>
<tr>
<td>Type</td>
<td>Integer</td>
<td>1.3.6.1.6.3.13.1.1.1.3</td>
<td>This object determines the type of notification to be generated for entries in the snmpTargetAddrTable selected by the corresponding instance of snmpNotifyTag</td>
</tr>
<tr>
<td>StorageType</td>
<td>Type</td>
<td>1.3.6.1.6.3.13.1.1.1.4</td>
<td>The storage type for this conceptual row</td>
</tr>
<tr>
<td>RowStatus</td>
<td>Status</td>
<td>1.3.6.1.6.3.13.1.1.1.5</td>
<td>The status of this conceptual row</td>
</tr>
</tbody>
</table>

### NTCT-PFS-HEALTH-MIB

nphPfsHlthStatus

<table>
<thead>
<tr>
<th>Object</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>nphDeviceId</td>
<td>String</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.1</td>
<td>Indicates vendor-specific product ID string for the given packet flow switch (PFS)</td>
</tr>
</tbody>
</table>
### nphInterfaceTable

<table>
<thead>
<tr>
<th>Object (nphInterface)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifIndex</td>
<td>InterfaceIndex</td>
<td>1.3.6.1.2.1.2.2.1.1</td>
<td>A unique value, greater than zero, for each interface</td>
</tr>
<tr>
<td>Type</td>
<td>Integer</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.2.1.1</td>
<td>Indicates that the interface is operating in one of the NphIfType modes</td>
</tr>
<tr>
<td>Class</td>
<td>Integer</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.2.1.2</td>
<td>Indicates the class of the interface</td>
</tr>
</tbody>
</table>

### nphFlowMapTable

<table>
<thead>
<tr>
<th>Object (nphFlow)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Unsigned32</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.3.1</td>
<td>Indicates an arbitrary integer value which uniquely identifies a traffic flow in nphFlowMapTable</td>
</tr>
<tr>
<td>Name</td>
<td>String</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.3.1.1.2</td>
<td>Indicates the name of the map for a given packet flow</td>
</tr>
<tr>
<td>Filter</td>
<td>String</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.3.1.1.3</td>
<td>Indicates name of the filter for a given packet flow</td>
</tr>
</tbody>
</table>

### nphFlowInterfaceTable

<table>
<thead>
<tr>
<th>Object (nphFlowInterface)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>nphFlowMapIndex</td>
<td>Unsigned32</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.3.1</td>
<td>Indicates an arbitrary integer value which uniquely identifies a traffic flow in nphFlowMapTable</td>
</tr>
<tr>
<td>InIf</td>
<td>InterfaceIndex</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.3.2.1.1</td>
<td>Indicates the ifindex of the input interface for a given packet flow</td>
</tr>
<tr>
<td>Index</td>
<td>Unsigned32</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.3.2.1.2</td>
<td>Indicates an arbitrary integer value which uniquely identifies a traffic flow entry in nphFlowInterfaceTable</td>
</tr>
<tr>
<td>OutIf</td>
<td>InterfaceIndex</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.3.2.1.3</td>
<td>Indicates the ifindex of the output interface for a given packet flow</td>
</tr>
</tbody>
</table>
### nphFlowLbgTable

<table>
<thead>
<tr>
<th>Object (nphFlowLbg)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>nphFlowMapIndex</td>
<td>Unsigned32</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.3.1.1.1</td>
<td>Indicates an arbitrary integer value which uniquely identifies a traffic flow in nphFlowMapTable</td>
</tr>
<tr>
<td>nphFlowInterfaceInf</td>
<td>InterfaceIndex</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.3.2.1.1</td>
<td>Indicates the ifindex of the input interface for a given packet flow</td>
</tr>
<tr>
<td>Index</td>
<td>Unsigned32</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.3.3.1.1</td>
<td>Indicates an arbitrary integer value which uniquely identifies a traffic flow entry in nphFlowLbgTable</td>
</tr>
<tr>
<td>Name</td>
<td>String</td>
<td>1.3.6.1.4.1.21671.3.2.1.1.3.3.1.2</td>
<td>Indicates the name of the LBG (load balance group) for a given packet flow</td>
</tr>
</tbody>
</table>

### nphFilterStatsTable

<table>
<thead>
<tr>
<th>Object (nphFilterStats)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifIndex</td>
<td>InterfaceIndex</td>
<td>1.3.6.1.2.1.2.2.1.1</td>
<td>A unique value, greater than zero, for each interface</td>
</tr>
<tr>
<td>Filter</td>
<td>String</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.1.1.1</td>
<td>indicates the filter name on which traffic is monitored</td>
</tr>
<tr>
<td>Pkts</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.1.1.2</td>
<td>indicates the total number of packets received on the corresponding ifIndex and nphFilterStatsFilter</td>
</tr>
</tbody>
</table>

### nphIfExtTable

<table>
<thead>
<tr>
<th>Object (nphIfExt)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifIndex</td>
<td>InterfaceIndex</td>
<td>1.3.6.1.2.1.2.2.1.1</td>
<td>A unique value, greater than zero, for each interface</td>
</tr>
<tr>
<td>CRCOctets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.1.1.1</td>
<td>Total number of CRC error octets received on this interface. Shows ‘0’ always</td>
</tr>
<tr>
<td>Object (nphIfExt)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------</td>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InMulticastOctets</td>
<td>Counter4</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.2</td>
<td>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</td>
</tr>
<tr>
<td>InUndersizeOctets</td>
<td>Counter4</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.3</td>
<td>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</td>
</tr>
<tr>
<td>InOversizeCOctets</td>
<td>Counter4</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.4</td>
<td>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</td>
</tr>
<tr>
<td>InUcastOctets</td>
<td>Counter4</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.5</td>
<td>Number of octets received which were not addressed to a multicast or broadcast address at this sub-layer. Shows '0' always</td>
</tr>
<tr>
<td>InBroadcastOctets</td>
<td>Counter4</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.6</td>
<td>Total number of good octets received which were addressed to a broadcast address at this sub-layer. Shows '0' always</td>
</tr>
<tr>
<td>InDropPks</td>
<td>Counter4</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.7</td>
<td>Total number of packets received that were dropped due to buffer overflow</td>
</tr>
<tr>
<td>InDropOctets</td>
<td>Counter4</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.8</td>
<td>Total number of octets received that were dropped due to buffer overflow. Shows '0' always</td>
</tr>
<tr>
<td>Object (nphIfExt)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------</td>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InPkts1519to2047Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.9</td>
<td>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)</td>
</tr>
<tr>
<td>InPkts2048to4095Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.10</td>
<td>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)</td>
</tr>
<tr>
<td>InPkts4096to9216Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.11</td>
<td>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)</td>
</tr>
<tr>
<td>InOverPkts9216Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.12</td>
<td>Total number of packets received that were longer than 9216 packets (excluding framing bits, but including FCS octets) and were otherwise well formed</td>
</tr>
<tr>
<td>InIPv4Pkts</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.13</td>
<td>Total number of packets received that were directed to a IPv4 address. Shows '0' always</td>
</tr>
<tr>
<td>InIPv4Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.14</td>
<td>Total number of octets received that were directed to a IPv4 address. Shows '0' always</td>
</tr>
<tr>
<td>InIPv4FragmentsPkts</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.15</td>
<td>Total number of fragmented packets received that were directed to a IPv4 address. Shows '0' always</td>
</tr>
<tr>
<td>Object (nphIfExt)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------</td>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>InIPv4FragmentsOctets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.16</td>
<td>Total number of fragmented octets received that were directed to a IPv4 address. Shows '0' always</td>
</tr>
<tr>
<td>InIPv6Pktst</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.17</td>
<td>Total number of packets (including bad packets) received that were directed to a IPv6 address. Shows '0' always</td>
</tr>
<tr>
<td>InIPv6Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.18</td>
<td>Total number of octets received that were directed to a IPv6 address. Shows '0' always</td>
</tr>
<tr>
<td>InIPv6FragmentsPktst</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.19</td>
<td>Total number of fragmented packets received that were directed to a IPv6 address. Shows '0' always</td>
</tr>
<tr>
<td>InIPv6FragmentsOctets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.20</td>
<td>Total number of fragmented octets received that were directed to a IPv6 address. Shows '0' always</td>
</tr>
<tr>
<td>OutMulticastOctets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.21</td>
<td>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</td>
</tr>
<tr>
<td>OutUndersizeOctets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.22</td>
<td>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</td>
</tr>
<tr>
<td>Object (nphIfExt)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------</td>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OutOversizeOctets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.23</td>
<td>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</td>
</tr>
<tr>
<td>OutUcastOctets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.24</td>
<td>Number of octets transmitted which were not addressed to a multicast or broadcast address at this sub-layer. Shows '0' always</td>
</tr>
<tr>
<td>OutBroadcastOctets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.25</td>
<td>Total number of good octets transmitted which were addressed to a broadcast address at this sub-layer. Shows '0' always</td>
</tr>
<tr>
<td>OutDropPkts</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.26</td>
<td>Total number of packets transmitted that were dropped due to buffer overflow.</td>
</tr>
<tr>
<td>OutDropOctets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.27</td>
<td>Total number of octets transmitted that were dropped due to buffer overflow. Shows '0' always</td>
</tr>
<tr>
<td>OutPkts1519to2047Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.28</td>
<td>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).</td>
</tr>
<tr>
<td>OutPkts2048to4095Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.29</td>
<td>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).</td>
</tr>
<tr>
<td>Object (nphIfExt)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------</td>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OutPkts4096to9216Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.30</td>
<td>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).</td>
</tr>
<tr>
<td>OutOverPkts9216Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.31</td>
<td>Total number of packets transmitted that were longer than 9216 packets (excluding framing bits, but including FCS octets) and were otherwise well formed.</td>
</tr>
<tr>
<td>OutIPv4Pkts</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.32</td>
<td>Total number of packets transmitted that were directed to a IPv4 address. Shows '0' always.</td>
</tr>
<tr>
<td>Counter64</td>
<td>OutIPv4Octets</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.33</td>
<td>The total number of octets transmitted that were directed to a IPv4 address. Shows '0' always.</td>
</tr>
<tr>
<td>OutIPv4FragmentsPkts</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.34</td>
<td>Total number of fragmented packets transmitted that were directed to a IPv4 address. Shows '0' always.</td>
</tr>
<tr>
<td>OutIPv4FragmentsOctets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.35</td>
<td>Total number of fragmented octets transmitted that were directed to a IPv4 address. Shows '0' always.</td>
</tr>
<tr>
<td>OutIPv6Pkts</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.36</td>
<td>Total number of packets (including bad packets) transmitted that were directed to a IPv6 address. Shows '0' always.</td>
</tr>
<tr>
<td>Object (nphIfExt)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------</td>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OutIPv6Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.37</td>
<td>Total number of octets transmitted that were directed to a IPv6 address. Shows '0' always</td>
</tr>
<tr>
<td>OutIPv6FragmentsPkts</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.38</td>
<td>Total number of fragmented packets transmitted that were directed to a IPv6 address. Shows '0' always</td>
</tr>
<tr>
<td>OutIPv6FragmentsOctets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.39</td>
<td>Total number of fragmented octets transmitted that were directed to a IPv6 address. Shows '0' always</td>
</tr>
<tr>
<td>OutUndersizePkts</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.40</td>
<td>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</td>
</tr>
<tr>
<td>OutOversizePkts</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.41</td>
<td>Total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed</td>
</tr>
<tr>
<td>OutPkts64Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.42</td>
<td>Total number of packets (including bad packets) transmitted that were 64 octets in length (excluding framing bits but including FCS octets)</td>
</tr>
<tr>
<td>OutPkts65to127Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.43</td>
<td>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)</td>
</tr>
<tr>
<td>Object (nphIfExt)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OutPkts128to255Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.44</td>
<td>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)</td>
</tr>
<tr>
<td>OutPkts256to511Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.45</td>
<td>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)</td>
</tr>
<tr>
<td>OutPkts512to1023Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.46</td>
<td>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)</td>
</tr>
<tr>
<td>OutPkts1024to1518Octets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.47</td>
<td>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)</td>
</tr>
<tr>
<td>PeakPkts</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.48</td>
<td>Indicates the peak packets count on the given interface. Shows '0' always</td>
</tr>
<tr>
<td>PeakTimePkts</td>
<td>DateAndTime</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.49</td>
<td>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</td>
</tr>
<tr>
<td>Object (nphfExt)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------</td>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PeakOctets</td>
<td>Counter64</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.50</td>
<td>Indicates the peak octets count on the given interface. Shows '0' always.</td>
</tr>
<tr>
<td>PeakTimeOctets</td>
<td>DateAndTime</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.51</td>
<td>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</td>
</tr>
<tr>
<td>InThroughput</td>
<td>DisplayString</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.52</td>
<td>Indicates the throughput in Mbps received on the given interface.</td>
</tr>
<tr>
<td>InMaxThroughput</td>
<td>DisplayString</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.53</td>
<td>Indicates the maximum throughput in Mbps received on the given interface.</td>
</tr>
<tr>
<td>OutThroughput</td>
<td>DisplayString</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.54</td>
<td>Indicates the throughput in Mbps transmitted from the given interface.</td>
</tr>
<tr>
<td>OutMaxThroughput</td>
<td>DisplayString</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.55</td>
<td>Indicates the maximum throughput in Mbps transmitted from the given interface.</td>
</tr>
<tr>
<td>InUtilization</td>
<td>DisplayString</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.56</td>
<td>Indicates the utilization in percentage on the given input interface.</td>
</tr>
<tr>
<td>InMaxUtilization</td>
<td>DisplayString</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.57</td>
<td>Indicates the maximum utilization in percentage on the given input interface.</td>
</tr>
<tr>
<td>OutUtilization</td>
<td>DisplayString</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.58</td>
<td>Indicates the utilization in percentage on the given output interface.</td>
</tr>
<tr>
<td>OutMaxUtilization</td>
<td>DisplayString</td>
<td>1.3.6.1.4.1.21671.3.2.1.2.2.1.59</td>
<td>Indicates the maximum utilization in percentage on the given output interface.</td>
</tr>
</tbody>
</table>
### VSS-SYSTEM-MIB

#### vsTemperatureStatusTable

<table>
<thead>
<tr>
<th>Object (vsTemperature Status)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Unsigned32</td>
<td>1.3.6.1.4.1.21671.3.1.1.1.1.1.1</td>
<td>Indicates an arbitrary integer value which uniquely identifies an entry in vsTemperatureStatusTable</td>
</tr>
<tr>
<td>Descr</td>
<td>String</td>
<td>1.3.6.1.4.1.21671.3.1.1.1.1.1.2</td>
<td>Indicates the human-readable description of the entity with the temperature being monitored</td>
</tr>
<tr>
<td>Value</td>
<td>Gauge32</td>
<td>1.3.6.1.4.1.21671.3.1.1.1.1.1.3</td>
<td>Indicates the temperature value of the entity being monitored</td>
</tr>
</tbody>
</table>

#### vsNotifsControl

<table>
<thead>
<tr>
<th>Object (vsNotifsControl)</th>
<th>Type</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsTempHighNotifEnable</td>
<td>TruthValue</td>
<td>1.3.6.1.4.1.21671.3.1.1.2.2</td>
<td>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.</td>
</tr>
<tr>
<td>vsCfgChangeNotifEnable</td>
<td>TruthValue</td>
<td>1.3.6.1.4.1.21671.3.1.1.2.3</td>
<td>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.</td>
</tr>
<tr>
<td>vsAuthenticationNotifEnable</td>
<td>TruthValue</td>
<td>1.3.6.1.4.1.21671.3.1.1.2.4</td>
<td>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.</td>
</tr>
<tr>
<td>Object (vsNotifsControl)</td>
<td>Type</td>
<td>OID</td>
<td>Comment</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------</td>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>vsFRUNotifEnable</td>
<td>TruthValue</td>
<td>1.3.6.1.4.1.21671.3.1.1.2.5</td>
<td>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.</td>
</tr>
<tr>
<td>vsSystemNotifEnable</td>
<td>BITS</td>
<td>1.3.6.1.4.1.21671.3.1.1.2.6</td>
<td>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.</td>
</tr>
<tr>
<td>vsPfsMeshNotifEnable</td>
<td>TruthValue</td>
<td>1.3.6.1.4.1.21671.3.1.1.2.7</td>
<td>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.</td>
</tr>
<tr>
<td>vsHlthChckStateNotifEnable</td>
<td>TruthValue</td>
<td>1.3.6.1.4.1.21671.3.1.1.2.8</td>
<td>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.</td>
</tr>
<tr>
<td>vsTriggerPolicyNotifEnable</td>
<td>TruthValue</td>
<td>1.3.6.1.4.1.21671.3.1.1.2.9</td>
<td>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.</td>
</tr>
<tr>
<td>vsTunnelStateNotifEnable</td>
<td>TruthValue</td>
<td>1.3.6.1.4.1.21671.3.1.1.2.10</td>
<td>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.</td>
</tr>
</tbody>
</table>