

SteelCentral™ NetShark User's Guide

Including the virtual edition

Version 10.9

April 2016



Contacts

Riverbed Technology
680 Folsom St.
San Francisco CA, 94107 USA

General

Telephone: 415.247.8800
E-mail: info@riverbed.com
Web: <http://www.riverbed.com>

Technical Support

Telephone: 415.247.7381
E-mail: support@riverbed.com

This Documentation and Riverbed

This document and the accompanying product documentation describes the functions of the Riverbed software product(s) ("SOFTWARE") identified above (this document and the product documentation are collectively referred to as "DOCUMENTATION"). Riverbed Technology, 680 Folsom St., San Francisco, California 94107 is the sole owner of all rights, title, and interest to the DOCUMENTATION and SOFTWARE.

Nothing herein shall grant or imply a license to the DOCUMENTATION or SOFTWARE. The right to use the DOCUMENTATION and SOFTWARE shall result only from entering into a Master Software License Agreement and a Software Usage Agreement, and paying the applicable license fees.

Terms and Conditions of Use

Eligible Users

This document is subject to restrictions on use and distribution is intended solely for persons who are subject to the terms and conditions of Riverbed's Software Master License Agreement or persons authorized by Riverbed ("Eligible Users"). As a condition of being granted access to and use of this document, each User represents that: i) the User is an Eligible User of a Licensee under a valid Riverbed Software Master License Agreement or the User is authorized by Riverbed and ii) the User accepts the terms and conditions of Riverbed's Software Master License Agreement and the terms and conditions governing the use of this document.

Confidential Information

The User agrees that the DOCUMENTATION, including this document, are the proprietary property of Riverbed and constitutes a trade secret of Riverbed. The User agrees that access to and use of this document does not grant any title or rights of ownership. The User shall not copy or reproduce, in whole or in part, disclose or permit third parties access to this document without the prior written consent of Riverbed. This document may not be stored, in whole or in part, in any media without the prior written consent of Riverbed. Any unauthorized use of this document will be subject to legal action that may result in criminal and/or civil penalties against the User.

Intellectual Property and Proprietary Notices

© 2016 Riverbed Technology, Inc. All rights reserved.

Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed Technology. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein may not be used without the prior written consent of Riverbed Technology or their respective owners.

The absence of a patent or mark from the above notices does not constitute a waiver of intellectual property rights that Riverbed Technology, Inc. has established in any of its products, service names or marks in use. Alteration, removal, obscuring, or destruction of any proprietary legend, copyright, trademark, patent, or intellectual property notice contained in this document is prohibited.

Portions of SteelCentral™ products contain copyrighted information of third parties. Title thereto is retained, and all rights therein are reserved, by the respective copyright owner. PostgreSQL is (1) Copyright © 1996-2009 The PostgreSQL Development Group, and (2) Copyright © 1994-1996 the Regents of the University of California; PHP is Copyright © 1999-2009 The PHP Group; gnuplot is Copyright © 1986-1993, 1998, 2004 Thomas Williams, Colin Kelley; ChartDirector is Copyright © 2007 Advanced Software Engineering; Net-SNMP is (1) Copyright © 1989, 1991, 1992 Carnegie Mellon University, Derivative Work 1996, 1998-2000 Copyright © 1996, 1998-2000 The Regents of The University of California, (2) Copyright © 2001-2003 Network Associates Technology, Inc., (3) Copyright © 2001-2003 Cambridge Broadband Ltd., (4) Copyright © 2003 Sun Microsystems, Inc., (5) Copyright © 2003-2008 Sparta, Inc. and (6) Copyright © 2004 Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications, (7) Copyright © Fabasoft R&D Software; Apache is Copyright © 1999-2005 by The Apache Software Foundation; Tom Sawyer Layout is Copyright © 1992 - 2007 Tom Sawyer Software; Click is (1) Copyright © 1999-2007 Massachusetts Institute of Technology, (2) Copyright © 2000-2007 Riverbed Technology, Inc., (3) Copyright © 2001-2007 International Computer Science Institute, and (4) Copyright © 2004-2007 Regents of the University of California; OpenSSL is (1) Copyright © 1998-2005 The OpenSSL Project and (2) Copyright © 1995-1998 Eric Young (ey@cryptsoft.com); Netdisco is (1) Copyright © 2003, 2004 Max Baker and (2) Copyright © 2002, 2003 The Regents of The University of California; SNMP::Info is (1) Copyright © 2003-2008 Max Baker and (2) Copyright © 2002, 2003 The Regents of The University of California; mm is (1) Copyright © 1999-2006 Ralf S. Engelschall and (2) Copyright © 1999-2006 The OSSP Project; ares is Copyright © 1998 Massachusetts Institute of Technology; libpq++ is (1) Copyright © 1996-2004 The PostgreSQL Global Development Group, and (2) Copyright © 1994 the Regents of the University of California; Yahoo is Copyright © 2006 Yahoo! Inc.; pd4ml is Copyright © 2004-2008 zefer.org; Rapid7 is Copyright © 2001-2008 Rapid7 LLC; CmdTool2 is Copyright © 2008 Intel Corporation; QLogic is Copyright © 2003-2006 QLogic Corporation; Tarari is Copyright © 2008 LSI Corporation; Crypt_CHAP is Copyright © 2002-2003, Michael Bretterklieber; Auth_SASL is Copyright © 2002-2003 Richard Heyes; Net_SMTP is Copyright © 1997-2003 The PHP Group; XML_RPC is (1) Copyright © 1999-2001 Edd Dumbill, (2) Copyright © 2001-2006 The PHP Group; Crypt_HMAC is Copyright © 1997-2005 The PHP Group; Net_Socket is Copyright © 1997-2003 The PHP Group; PEAR::Mail is Copyright © 1997-2003 The PHP Group; libradius is Copyright © 1998 Juniper Networks. This software is based in part on the work of the Independent JPEG Group the work of the FreeType team.

Restricted Rights Legend

The DOCUMENTATION and SOFTWARE are subject to the restrictions on use and distribution in the Riverbed Software Master License Agreement (for Agencies of the U.S. Government). Any use of the DOCUMENTATION or any SOFTWARE by an agency of the U.S. Government or a direct contractor of an agency of the U.S. Government requires a valid Riverbed Software Master License Agreement and Riverbed Software Usage Agreement.

For all users, this Software and Documentation are subject to the restrictions (including those on use and distribution) in Riverbed's Master License Agreement. Use of this Software or Documentation requires a current Riverbed license and shall be governed solely by the terms of that license. All other use is prohibited. For the U.S. Government and its contractors, the Software is restricted computer software in accordance with Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. The Software and Documentation qualify as "commercial items," "commercial computer software," and "commercial computer software documentation."

No Warranty and Limitation of Liability

ALL INFORMATION PROVIDED IN THIS USER MANUAL IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND EITHER EXPRESS OR IMPLIED INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. No representations by Riverbed, such as statements of capability, suitability for use, accuracy or performance, shall be a warranty by Riverbed, or bind Riverbed or vary any term or condition of any Software Master License Agreement, unless contained in written agreement and signed by Riverbed and any other party or parties to such Software Master License Agreement.

In no event shall Riverbed be liable for any incidental, indirect, special, or consequential damages whatsoever (including but not limited to lost profits arising out of or relating to this document or the information contained herein) even if Riverbed has been advised, knew, or should have known of the possibility of such damages.

THE USER UNDERSTANDS AND ACCEPTS THAT RIVERBED SHALL NOT BE LIABLE FOR DAMAGES WHICH ARE: (i) INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR CONSEQUENTIAL, OR (ii) THE RESULT FROM LOSS OF USE, DATA, OR PROFITS, OR (iii) FROM THE USE OF THE SOFTWARE AND DOCUMENTATION, WHETHER BROUGHT IN AN ACTION OF CONTRACT, TORT, OR OTHERWISE, EVEN IF RIVERBED WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Export Controls

Any User of the DOCUMENTATION including this document shall comply with the laws of the United States, including the provisions of the U.S. Department of Commerce, Bureau of Industry Security ("BIS"), *Export Administration Regulations (EAR)*, the U.S. Department of State, *International Traffic in Arms Regulations*, and the U.S. Department of Treasury, Office of Foreign Assets Control, regarding the export, re-export and disclosure of the DOCUMENTATION or the SOFTWARE. Any export, re-export or disclosure of the DOCUMENTATION or the SOFTWARE shall be subject to the prior written consent of Riverbed. Users shall not remove any Destination Control Notices provided by Riverbed from the DOCUMENTATION or the SOFTWARE.

Destination Control Statement

The DOCUMENTATION and the SOFTWARE were manufactured in the United States by Riverbed. The initial export of the DOCUMENTATION and the SOFTWARE from the United States, and any subsequent relocation or re-export to another country shall comply with the laws of the United States relating to the export of technical data, equipment, software, and know-how. Any diversion contrary to the laws of the United States is prohibited.



Riverbed Technology
680 Folsom Street
San Francisco, CA 94107

Phone: 415.247.8800
Fax: 415.247.8801
Web: <http://www.riverbed.com>

712-00091-15

Contents

- Chapter 1 - Overview..... 1**
 - SteelCentral NetShark family of products 1
 - User interfaces..... 1
 - Storage..... 1
 - Capture jobs..... 2
 - Traffic classification 2
 - Synchronizing Traffic Definitions..... 3
 - Microflow Indexing 3
 - Advanced traffic metrics calculation and export 4
 - SSL Traffic Decryption 4
 - SteelCentral Packet Analyzer 5

- Chapter 2 - Tasks..... 7**
 - Connecting to a NetShark..... 7
 - Logging in using a browser..... 7
 - Logging in using Packet Analyzer 8
 - Logging out 9
 - Checking appliance status..... 9
 - Time Synchronization 9
 - Setting basic appliance parameters..... 10
 - Configuring data export to NetProfiler 11
 - Configuring NetFlow v9 export 12
 - Configuring data collection ports..... 12
 - NetShark appliances 13
 - NetShark virtual edition..... 16
 - Capturing network data 17
 - Adding /editing capture jobs 17
 - Viewing capture job status 20
 - Controlling capture jobs 22
 - Using Packet Analyzer to create capture jobs 22
 - Exporting packets to a file 23

| | |
|---|----|
| Using SSL Decryption | 24 |
| Specifications | 24 |
| Defining Decryption Keys | 24 |
| Entering Decryption Keys | 26 |
| Assigning User Groups to Decryption Keys | 26 |
| Decrypting HTTP traffic using SSL | 27 |
| Managing users and groups | 28 |
| Credential Manager | 28 |
| Capabilities | 28 |
| Adding users and groups | 30 |
| Changing user passwords | 31 |
| Unlocking a locked-out user | 31 |
| Setting up the login screen | 32 |
| Authenticating users | 33 |
| Managing security functions | 40 |
| Setting up logging | 40 |
| Local logging | 41 |
| Remote Syslog logging | 41 |
| RADIUS/TACACS+ logging | 42 |
| Setting up a firewall | 43 |
| Managing certificates | 45 |
| Managing the appliance: SNMP and Notifications | 49 |
| Enabling SNMP management | 49 |
| Setting up notifications | 51 |
| Using the Packet Analyzer Concurrent License server | 55 |
| Updating system software | 56 |
| Performing maintenance functions | 57 |
| Gathering system information | 58 |
| Downloading logs | 58 |
| Viewing storage status | 58 |
| Reinitializing and reformatting packet storage | 60 |
| Halting and rebooting the system | 60 |
| Configuring and managing 6170 storage units | 61 |
| NetShark CLI Packet Storage and Service commands | 61 |
| NetShark Web interface storage information and management | 61 |
| Enrolling storage units | 62 |
| Adding storage units to packet storage | 62 |
| Changing the packet storage RAID level | 63 |
| Maintaining a Storage Unit | 64 |
| Replacing a base unit or a storage unit | 66 |
| Restoring a storage unit to its base unit | 66 |
| Advanced Configuration Settings | 67 |
| Updating Predefined Port and Port Group Definitions | 67 |
| Port definitions | 69 |
| Port group definitions | 72 |
| Application definitions | 73 |

| | |
|--|------------|
| Advanced settings | 78 |
| Troubleshooting an initial installation | 79 |
| Securing your appliance configuration | 80 |
| Common Criteria initial setup | 80 |
| Common Criteria operation | 84 |
| JITC-hardened initial setup | 86 |
| Chapter 3 - Reference | 89 |
| CLI commands | 89 |
| Certificate commands | 91 |
| Interface commands | 92 |
| License commands | 92 |
| Packet Storage commands | 93 |
| Service commands | 93 |
| System commands | 95 |
| Uptime-report commands | 97 |
| Clock command | 97 |
| Wizard command | 98 |
| Help command | 98 |
| Exit command | 98 |
| Appendix A - Changing System Settings | 99 |
| Changing BIOS settings for NetShark Model xx00 appliances | 99 |
| How to change the BIOS password | 99 |
| How to disable booting from removable media | 103 |
| Appendix B - Installing NetShark Software | 105 |
| Installing NetShark from a USB memory stick | 105 |
| Step 1 - Download the software | 105 |
| Step 2 - Create bootable USB memory sticks | 105 |
| Step 3 - Insert the bootable USB memory stick into the system | 105 |
| Step 4 - Connect to the console port | 106 |
| Step 5 - Configure the BIOS | 106 |
| Step 6 - Install the software | 106 |
| Step 7 - Remove the USB memory stick and power-cycle the appliance | 106 |
| Step 8 - Run the configuration wizard | 107 |

CHAPTER 1 Overview

SteelCentral NetShark family of products

The NetShark products capture and analyze network traffic. They come in two general forms:

- NetShark-rack-mounted standalone hardware devices for capturing and analyzing network packet data
- NetShark virtual edition -packet capture and analysis software running as virtual machines in virtual environments

These products capture packets at network speeds up to 10 Gbps. They can also generate Microflow Indexing, described below. Microflow Indexing provides summary data, allowing for very rapid analysis of some types of network traffic information. In addition, the NetShark products can capture network flow information and forward it to Riverbed® SteelCentral™ NetProfiler for analysis.

User interfaces

Initial configuration of NetShark products is performed through a console interface. This configuration is described in the *Quick Start Guides* for NetShark and NetShark virtual editions.

Normal operation of the appliances is performed through a Web user interface (Web interface) that is accessible from a standard Web browser or through the Riverbed® SteelCentral™ Packet Analyzer.

Storage

The NetShark products include two separate storage subsystems:

- The System Storage subsystem contains the NetShark appliance operating system, software, pcap trace files, View metrics, and Microflow Indexing data for Job Traces and pcap files. Within System Storage, User Data Storage contains files under user control, such as Microflow Indexing data and pcap files. The status and amount of User Data Storage used is shown under System Information on the Status page of the NetShark Web interface.
- The Packet Storage subsystem is used by the NetShark Packet Recorder to store job traces. This storage system is optimized to provide high-speed writing to disk and fast read access for arbitrary time intervals within a job trace.

Related Topics

- [“Checking appliance status” on page 9](#)

- [“Viewing storage status” on page 58](#)

Capture jobs

Network traffic data capture is organized into capture jobs. Capture job parameters specify start times for capture jobs, capture job duration, data filtering, and so on. You will encounter these terms in your work with NetShark products:

- **Capture job:** A *capture job* refers to the specific parameters associated with a packet recording session. These parameters include the job name, the network interface, a BPF filter, start and stop criteria, and an upper bound on the amount of storage to be used by the capture job.
- **Job trace:** The *job trace* represents the network traffic saved in the packet storage. Each capture job is associated with exactly one job trace, which has the same name as the capture job.
- **Trace clips:** *Trace clips* represent user-defined time intervals within a job trace.
- **Jobs repository:** In Packet Analyzer, the Files panel for a NetShark appliance contains a folder called the *Jobs Repository* that has an icon and the name for each job trace in the appliance.
- **Virtual job device:** In Packet Analyzer, the Devices panel for a NetShark appliance contains an icon and the name for each *Virtual Job Device* representing the network interface associated with a capture job on the appliance. Views can be applied to these capture job interfaces creating a visual analysis and representation of what was captured by the corresponding capture job.

Each NetShark appliance network interface can support 15 running, non-indexing capture jobs. If any of these jobs include indexing, the number of running capture jobs supported on the interface is 14. An unlimited number of stopped capture jobs can be created.

Traffic classification

In software version 10.5 (and later), traffic classification in NetShark and NetShark virtual edition can provide application-level intelligence in packet capture and analysis, as well as in flow exports. Using the same deep packet inspection (DPI) engine as Riverbed® SteelHead™ appliances, traffic classification uses the following definitions:

- Port Definitions
- Port Group Definitions
- Application Definitions

Application definitions include:

- Layer 4 Mappings
- Layer 7 Fingerprints
- System Applications mappings.

Layer 7 Fingerprints have the highest priority in identifying an application, followed by Application Definitions, and Layer 4 Mappings. An “Override” can be set for one or more Layer 4 Mappings, giving these mappings the highest priority in identifying an application.

Configure and manage traffic classification from the Settings tab in the NetShark Web user interface. Click the tab and select Port Definitions, Port Group Definitions, or Application Definitions from the menu.

Packet Analyzer does not do DPI classification on local interfaces. Also, DPI views are not allowed on local sources.

Note: Views applied to offline files captured before 10.5 use the Port Names, Port Groups, and Layer 4 Mapping definitions. Layer 7 Signatures and Application Definitions are not retroactive.

Related Topics

- [“Updating Predefined Port and Port Group Definitions” on page 67](#)
- [“Port definitions” on page 69](#)
- [“Port group definitions” on page 72](#)
- [“Application definitions” on page 73](#)

Synchronizing Traffic Definitions

Synchronization is disabled by default. Enable synchronization on the NetProfiler Export tab of the NetShark Web interface.

Synchronization ensures consistent identification of your network traffic for viewing and analysis. When a NetShark exports network flow statistics to a NetProfiler, the NetProfiler Port Definitions, Port Group Definitions, Layer 4 Mappings, and Layer 7 Signatures can be synchronized with the NetShark. When synchronization is done:

- The NetShark Port Names, Port Groups, Layer 4 Mappings, and L7 Fingerprints are overwritten and replaced with those of the NetProfiler.
- Only Service Response Time on the Port Definitions page can be modified. Modifications on the Port Definitions, Port Group Definitions, or Application Definitions pages are disabled.

Also, a NetShark can manually synchronize these same definitions with Packet Analyzer for use in viewing and analyzing local traffic.

Note: Starting with release 10.6, NetProfiler and NetShark are shipped with the same Port Names, Port Groups, and Layer 4 Mappings configured. New installations of NetProfiler and NetShark also have the new shared Port Names, Port Groups, and Layer 4 Mappings. Note: Updating a NetProfiler or NetShark to version 10.6 does not update the existing port and application definitions.

In version 10.6 (and later), when Packet Analyzer connects to a NetShark, a message is displayed if the port names, port groups, L4 mappings, and L7 fingerprints are not the same. The message explains how to correct this if necessary.

Microflow Indexing

Microflow Indexing (indexing) captures summary information about conversations between devices on the network. This information is all that is needed by Packet Analyzer to calculate many of the View metrics that describe the traffic stream. Because it is already in summary form, processing of Microflow Indexing data for View metrics is very fast.

In simplified terms, the Microflow Indexing process is this: For each packet, there is a conversation identifier consisting of the 5-tuple:

- source IP address
- destination IP address
- IP protocol
- source port
- destination port

When the Microflow Indexing feature is enabled for a capture job, the NetShark appliance computes the total bytes and number of packets for each unique conversation identifier in the traffic stream for each second. This information is stored in a file in System Storage and is referred to as Microflow Indexing data.

Related Topics

- [“Microflow Indexing” on page 19](#)

Advanced traffic metrics calculation and export

A NetShark must see both directions of traffic flow on the same physical interface (or vNIC on NetShark virtual edition) to calculate and export the following to a NetProfiler appliance:

- DPI metrics for applications
- VoIP metrics for IP telephony
- Service Response Time metrics for TCP connections

Otherwise, only basic flow metrics are calculated and exported.

The use of a NetShark appliance aggregating interface (TurboCap Board Aggregating Port or TurboCap Aggregating Port) does enable these advanced traffic metrics to be calculated in views and capture jobs, but aggregating ports cannot be configured for export to a NetProfiler.

SSL Traffic Decryption

In software version 10.7 (and later), HTTP traffic encrypted using the SSL protocol can be decrypted when the key exchange algorithm uses RSA keys. Decrypted data is used to calculate traffic metrics for use in Packet Analyzer views. For example, using SSL decryption, the view “Bandwidth Usage > Web > Web Bandwidth - Top Status Codes” can include metrics for previously unavailable SSL-encrypted traffic.

An administrator enters a decryption key by assigning a unique server IP address and TCP port to a PEM-formatted RSA private key.

- Private keys are stored in a secure vault, a separate, encrypted store, on a NetShark appliance, NetShark virtual edition, or Riverbed[®] SteelCentral[™] NetExpress.
- If a private key includes a certificate, an SHA1 fingerprint is calculated and displayed with the decryption key on the Settings > SSL Decryption page of the NetShark Web interface.
- Private keys can only be added or removed from the secure vault.
- The creation and use of SSL decryption keys can be audited using NetShark logs and notifications.

Access control to a decryption key is set by assigning groups to the key when it is entered.

- Group members can decrypt traffic when they apply a view to an interface or a trace file or a trace clip.
- A group's eligibility for decryption key use is determined by the capabilities assigned to the group.
- Group assignments to a decryption key can be edited by an administrator after a key is entered.

Decrypted SSL packets are not stored and cannot be exported or sent outside an appliance. When a request is made to send packets to Wireshark, Riverbed® SteelCentral™ Transaction Analyzer, a file, or NetProfiler, copies of the packets captured on the network are sent - the packets are not decrypted.

SSL decryption is not supported on traffic or traces on the local system of a Packet Analyzer. For more information, see [“Using SSL Decryption”](#) in Chapter 2.

SteelCentral Packet Analyzer

Packet Analyzer integrates closely with NetShark to analyze and display captured network data. Packet Analyzer is a distributed analysis tool, using NetShark to perform computations and integrating the results for display. This distributed processing saves network bandwidth-only the results, not the underlying packet data, are transferred across the network-and allows Packet Analyzer to manipulate very large packet trace files.

Packet Analyzer contains an extensive collection of network traffic analysis metrics (Views), and can analyze live or offline traffic sources. It allows drag-and-drop drill down (successive application of Views), visualization and analysis of long-duration and multi-source packet captures, trigger-alert mechanisms, and report generation.

CHAPTER 2 Tasks

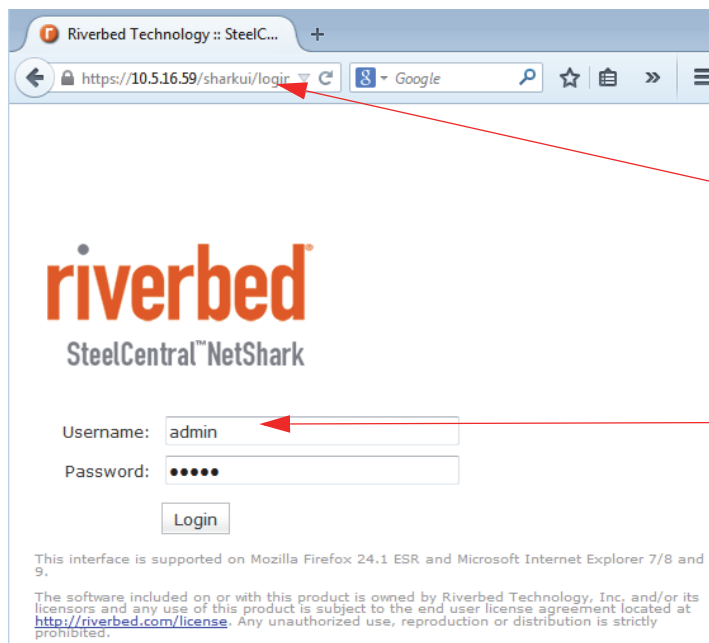
Tasks for NetShark and NetShark virtual edition are very similar, often identical. Differences are noted in the text. Screen shots shown in the following pages may be from either product. In cases where there is a significant difference, screen shots from both products are shown.

Connecting to a NetShark

Connect to a NetShark through its Web user interface (Web interface). You can do this using your Web browser or using Packet Analyzer.

Logging in using a browser

The NetShark Web interface is supported on Mozilla Firefox 24.1 ESR and Microsoft Internet Explorer 7/8 and 9. Check that SSL, cookies, and JavaScript are enabled in your browser.



1) Point your browser at `https://<NetShark>` where `<NetShark>` is the IP address or DNS name of the appliance.

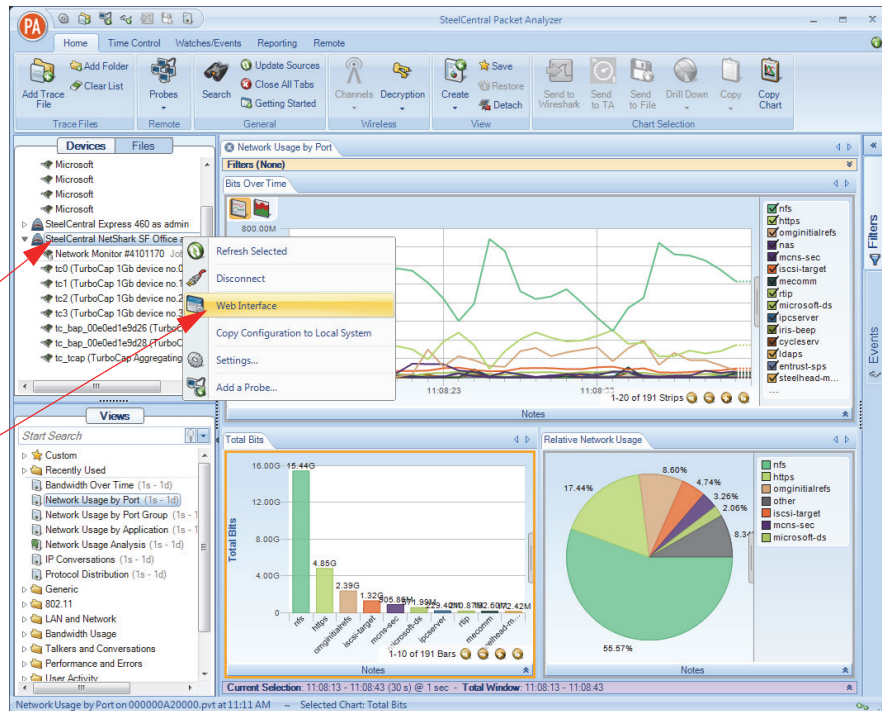
2) Enter username and password, then click **Login**. (Default value is "admin" for both username and password.)

Logging in using Packet Analyzer

When Packet Analyzer is connected to a NetShark probe, you can right-click on the probe in the Devices pane or the Files pane and select Web Interface from the context menu.

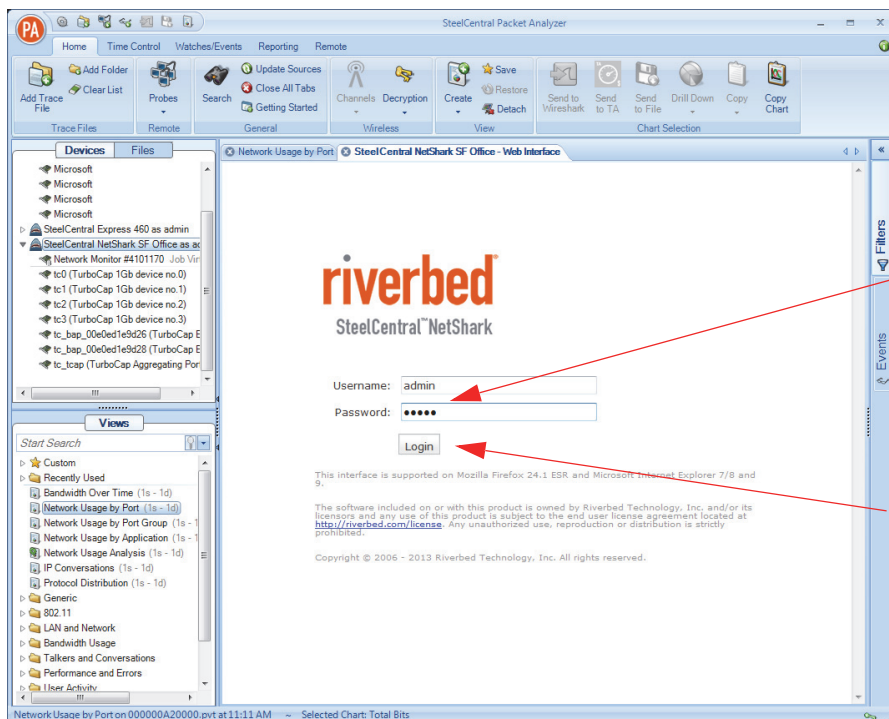
1) Right-click on the probe.

2) Select Web Interface.



3) Enter the Username and Password. (Default value is "admin" for both username and password.)

4) Click the Login button.



Logging out

Checking appliance status

Click the Status tab in the NetShark Web interface to bring up the Status screen.

Status

Capture Jobs Status of capture jobs

| Job | Status | Packet Capture Size |
|--------------------------|----------------|---------------------|
| Network Monitor #4101170 | RUNNING | 511.91 GB |

System Information Storage and memory usage

| OS File System | | Packet Storage | | Memory | |
|--------------------|-------------------------|-------------------|------------------------|------------|----------------|
| Status: | OK | Status: | OK | Status: | OK |
| Total: | 425.95 GB | Total: | 3.63 TB | Total: | 5.83 GB |
| Used: | 8.70 GB (2.04%) | Used: | 512 GB (13.74%) | Available: | 3.33 GB |
| Allocated (Index): | 11.16 GB (2.79%) | Allocated (Jobs): | 512 GB (13.74%) | | |

NetProfilers Configured For Export NetProfiler statistics

| NetProfilers | Status | Info |
|--------------|-----------|------|
| 10.5.14.109 | OK | -- |

| NetProfiler Export Statistics | | |
|-------------------------------|----------------|----------------|
| | Exported Flows | Rejected Flows |
| Total (last minute): | 33.18 K | 0 |
| Total (last week): | 39.97 M | 0 |
| Avg per minute (last week): | 3.96 K | 0 |
| Peak (last week): | 52.20 K | 0 |

Interfaces Status of interfaces

| Interface | Link Status | Received Packets |
|-----------|-------------|------------------|
| tc0 | UP | 8.55 G |
| tc1 | UP | 0 |
| tc2 | UP | 0 |
| tc3 | DOWN | 0 |

Time Synchronization

The time synchronization protocol and configuration is initially specified in the NetShark CLI wizard that is run when NetShark is installed. Changes can be made on the Settings > Basic Settings tab of the NetShark Web interface.

A Remote Peer is the host name or IP address of a time server, which may be different from a master time server often configured in the CLI wizard or Basic Settings Web page. There can be only one active time source under Synchronization. Configuration indicates whether a time source is configured or learned. Authenticated indicates whether the server/peer connection is authenticated (optional).

Setting basic appliance parameters

The Settings -> Basic Settings screen allows you to change the configuration parameters that you set during initial configuration.

Basic Settings

Host Information

Host Name: Enter a name for the appliance.

Note: Domain name and host name together must not exceed 63 characters. Host and domain names must comply with [RFC 1123](#).

Timezone: Select a city in the appliance's time zone.

Time synchronization: PTP Select working Management Port with LAN access to master PTP clock.

Interface:

NTP Enter addresses for NTP time servers.

Note: Enter server addresses, one per line. Optionally, a server may be specified as [server]:[index]:[algorithm]:[key], where [server] is a server address, [index] is a positive 32-bit integer, [algorithm] is "SHA1" or "MD5", and [key] is an authentication key. Server addresses must comply with [RFC 1123](#). Authentication keys may **not** contain spaces, double quotes, or the special characters "#", ";", or ":",.

SteelCentral NetShark is currently using the NetProfiler(s) listed above as NTP Server(s)

Management Ports

Primary Management Port (primary)

Enable DHCP on primary

IP Address:

Netmask:

Default IP Gateway:

Secondary Management Port (aux)

Enable DHCP on aux

IP Address:

Netmask:

Default IP Gateway:

Click to use DHCP addressing, or enter IP address, mask, and gateway.¹

Domain Information

Primary DNS: Enter DNS information.

Secondary DNS: Click to enable FIPS mode.

Domain Name: Click to enable SSH access.

Security Configuration

Enable FIPS 140-2 Compatible Cryptography

Remote Shell Access

Enable Secure Shell (SSH) Access

Apply Click to apply settings.

¹ Important: primary and aux should not be enabled on the same network.

Precision Time Protocol (PTP), IEEE 1588 (version 2) is a software-based implementation. The NetShark is a slave and requires a PTP master on its local area network. You can select which active management interface to use for the PTP communication (default is primary). Communication is done using UDP ports 319 and 320 over IPv4. When using PTP and NetProfiler export is enabled, the NetShark time does not synch with the NetProfiler.

The “Enable FIPS 140-2 Compatible Cryptography” check box enables the use of a cryptographic module that has been certified to be FIPS 140-2 compliant (certificate #1747). This mode of operation is referred to as “FIPS mode” for brevity.

Changes to the Host Name, IP Address, or Timezone parameters require a reboot.

Configuring data export to NetProfiler

Use the NetProfiler Export tab in the NetShark Web interface to configure flow export. You can configure a NetShark to export network flow statistics to one or two NetProfiler appliances. When exporting flows to a NetProfiler running a pre-10.5 software version, VoIP metrics are ignored, whether or not DPI is enabled. Only basic flow information is recognized in this case.

Important: If a NetShark uses the maximum flow export rate of 12.M fpm, the NetProfiler appliance must be able to process that flow export rate.

NetProfiler Export

1) Click to enable export. → Enable Flow Export

2) Enter IP address or DNS name for up to two NetProfiler appliances. →

NetProfiler Information

NetProfiler For Export:

Enable Synchronization of Ports, Port Groups and Application Definitions:

3) Enter IP address/DNS name and UDP port for up to two Flow collectors. →

Flow collectors (NetFlow v9)

Flow Collector address:

UDP Port:

4) Enable all ports or individual ports to export data. →

5) Enter a BPF filter, if desired. →

6) Enable output of VoIP metrics, if desired. →

7) Enable output of DPI metrics, if desired. →

8) Click to apply configuration. →

Exported Interfaces

Enable/Disable All Interfaces

| Enabled | Interface | BPF Filter | VoIP Enabled | DPI Enabled |
|-------------------------------------|-----------|----------------------|--------------------------|--------------------------|
| <input checked="" type="checkbox"/> | tc0 | <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | tc1 | <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | tc2 | <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | tc3 | <input type="text"/> | <input type="checkbox"/> | <input type="checkbox"/> |

You can specify one BPF filter per interface.

When NetProfiler Export is configured, NetShark uses the configured NetProfiler appliances as NTP servers for time synchronization. When PTP is selected as the time source, it does not synchronize with a NetProfiler.

You can view the configured NetProfiler Export and Flow Collector settings and their export statistics on the NetShark Web interface Status page.

Configuring NetFlow v9 export

NetFlow v9 export is configured on the NetProfiler Export tab of the NetShark Web interface. You can configure NetFlow v9 flow export to one or two NetFlow v9 collectors. Version 10.8 (and later) supports the export of standard NetFlow v9 records in standard UDP packets.

- Enable Flow Export must be checked.
- Export runs in parallel with NetProfiler export.

Check the configuration and status of the flow collectors on the NetShark Web interface Status page under the Flow collectors (NetFlow v9) For Export heading.

Configuring data collection ports

Because of product differences between a NetShark and a NetShark virtual edition — one has physical ports, the other does not — separate descriptions of the interface configuration are given below.

NetShark appliances

Interfaces are contained on one or more network interface cards located at the back of the NetShark appliance chassis. Physical ports are grouped into logical boards composed of two ports each. In the example screen below, a card with four ports is represented as two boards with two ports each. Click the Interfaces tab in the NetShark Web interface to configure the installed interfaces.

The screenshot displays the 'Interfaces' configuration page for 'Board 0'. It shows two interface configurations side-by-side:

- Interface Data Center:**
 - Id:** mon1_0
 - Name:** Office Data Center
 - Description:** 10.10.5.11-24
 - MAC Address:** 00:e0:ed:2a:37:bf
 - Timestamping:** NetShark Internal
 - Blink Status:** OFF (Start Blink button)
 - Enable Deduplication:**
 - Link Information:** Link Status: UP, Link Speed: 10 Gbps Full Duplex, Bytes RX: 0 B, Packets RX: 0
 - Speed Options:**
 - 10 Mbps Half Duplex
 - 10 Mbps Full Duplex
 - 100 Mbps Half Duplex
 - 100 Mbps Full Duplex
 - 1 Gbps Full Duplex
 - 10 Gbps Full Duplex
- Interface Denver Office LAN:**
 - Id:** mon1_1
 - Name:** Denver Office LAN
 - Description:** 192.168.44.3-26
 - MAC Address:** 00:e0:ed:2a:37:be
 - Timestamping:** NetShark Internal
 - Blink Status:** OFF (Start Blink button)
 - Enable Deduplication:**
 - Link Information:** Link Status: UP, Link Speed: 10 Gbps Full Duplex, Bytes RX: 0 B, Packets RX: 0
 - Speed Options:**
 - 10 Mbps Half Duplex
 - 10 Mbps Full Duplex
 - 100 Mbps Half Duplex
 - 100 Mbps Full Duplex
 - 1 Gbps Full Duplex
 - 10 Gbps Full Duplex

At the bottom left, there is an 'Apply' button with a red arrow pointing to it and the text 'Click to save changes.'

You can configure several parameters for each interface, described below.

Identifying the physical interface (setting Blink)

The Start Blink button causes the LED next to the network interface (located on the back panel of the NetShark appliance) to blink. This can help you positively identify the interface you are configuring.

The image shows a close-up of the 'Blink Status' control. It displays 'Blink Status: OFF' and a 'Start Blink' button. A red arrow points to the button with the text 'Click to start blink. Click again to stop.'

When you no longer need the LED to blink, turn it off by clicking the Stop Blink button (in the same location).

Name

The default interface ID for a NetShark model xx70 is monS_N, where “S” is the slot where the NIC is installed and “N” is the port index within the NIC card (0-3), the same convention used in NetExpress products. If you move the NIC into another slot, the interface names change. Note: If an interface name is mon0_N the NIC is installed in an incorrect slot.

A NetShark model xx00 uses the same convention for interface names as was used in earlier versions, tcN.

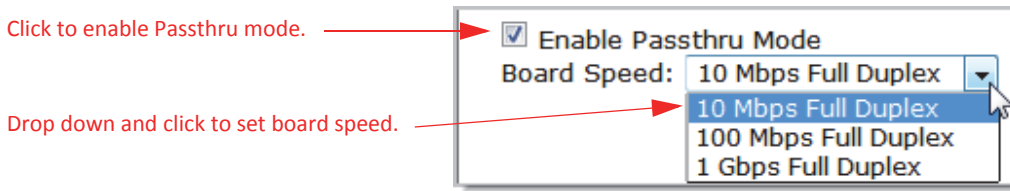
You can assign a name to a NetShark interface. A 24-character name is displayed as entered. Names longer than 24 characters are compressed when displayed. This name is propagated to all connected Packet Analyzer clients and NetProfilers. It appears everywhere the interface is referred to in the NetShark Web interface. It also appears in references to the interface in Packet Analyzer and NetProfiler.

Description

You can assign a description to an interface, containing helpful information, for example, its location, use, or owner. A 24-character description is displayed as entered. Descriptions longer than 24 characters are compressed when displayed. This description is propagated to all connected Packet Analyzer clients and NetProfilers. It appears in the NetShark Web interface and also in Packet Analyzer or NetProfiler interfaces. Where a description is used, if no description is assigned, the supplied default interface description appears, for example, TurboCap 1 GB device n.

Setting Passthru mode

Passthru mode is supported only for 1G copper NICs in NetShark model xx00 appliances. When Passthru mode is enabled the two interfaces of a logical board act as a network tap: packets received on one interface are sent out through the other interface, and vice versa. The board can negotiate only one fixed, full-duplex rate on the two ports.



When Passthru mode is disabled the board operates as two independent ports.

Setting Timestamping

The Timestamping parameter lets you select the timing source for data captures made by the interface. Timestamping settings can be modified only on an interface where no capture job has been defined.

Use *NetShark Internal* for connection to _____ **Timestamping:**

Use tap selection for connection to _____

mirror (SPAN) port.

network tap.

| NetShark Internal |
|----------------------------------|
| cPacket (timestamp only) |
| cPacket (timestamping + slicing) |
| Gigamon (Header) |
| Gigamon (Trailer) |
| Gigamon (Trailer X12-TS) |
| VSS (Timestamp only) |
| VSS (Port ID & Timestamp) |
| Anue |
| Arista |

When timestamping is set to NetShark Internal, capture packets are timestamped using the NetShark appliance's internal clock reference. The other options use the internal clocks of the selected network tap, eliminating any latency and improving timestamp precision. Make sure to select the timestamping mode corresponding to the tap the interface is physically connected to; otherwise you may get unpredictable results (false packets, false timestamps, dropped packets, and so on).

Setting the Timestamping parameter gives you the highest level of timing accuracy at a capture interface. Timestamping can help maintain accuracy when analyzing packet flows using Multi-Segment Analysis with Packet Analyzer.

Eliminating packet redundancy (setting Deduplication)

If the NetShark appliance is receiving packets from more than one source in the same network (by using a SPAN port or an aggregating tap, for example), it may receive some of the packets more than once. Enabling Deduplication causes the appliance to discard the duplicate packets, allowing for more accurate traffic analysis.

Click to discard redundant packets. → Enable Deduplication

Note that Deduplication consumes additional resources, and may affect performance in a busy network. Deduplication applies only to one single physical interface. It does not deduplicate packets from multiple turbocap ports.

NetShark virtual edition

One interface, `mon0`, is preconfigured and is installed as part of the deployment process. You can add up to three additional interfaces after deployment. Interfaces are assigned to logical boards, one interface per board. The example screen below shows a typical configuration with a single interface.

There are no parameters to set for the interfaces on a NetShark virtual edition.

The screenshot shows the NetShark virtual edition web interface. At the top, the logo for riverbed SteelCentral NetShark Virtual Edition is visible. The hostname is `shark`, the version is `10.7`, and the uptime is `0 d 00:41:38`. The navigation menu includes Status, Capture Jobs, NetProfiler Export, Interfaces, Settings, and System. The main content area is titled "Interfaces" and shows the configuration for Board 0. The Board Settings section displays the Description as `mon0` and the Type as `libpcap`. The Interface `mon0` section shows the Id as `mon0`, Name as an empty field, Description as `mon0`, and MAC Address as `00:0c:29:19:ba:0e`. The Link Information section shows the Link Status as `UP`, Link Speed as `10 Gbps Full Duplex`, Bytes RX as `120 B`, and Packets RX as `2`. Red lines with labels point to the Board Settings, Interface mon0, and Link Information sections. An "Apply" button is located at the bottom of the configuration area.

Board information

Interface information

Link information

Board 0

Board Settings

Description: **mon0**

Type: **libpcap**

Interface mon0

Id: **mon0**

Name:

Description:

MAC Address: **00:0c:29:19:ba:0e**

Link Information

Link Status: **UP**

Link Speed: **10 Gbps Full Duplex**

Bytes RX: **120 B**

Packets RX: **2**

Apply

Capturing network data

Adding /editing capture jobs

The parameters of an existing job can be edited only if the job is stopped.

1) Click the Capture Jobs tab.

2) Click **Add a New Job** to add a job or click **Edit** to edit an existing stopped job.

3) Enter/adjust capture job parameters (details below).

4) Click to save capture job configuration.

Capture Jobs

Capture Job Summary

| Job Name | Interface | Status | Size | Actions |
|--|---------------|---------|------|---|
| Traffic Monitor 411221 | Data Center | RUNNING | 0 B | View Stop |
| SF Office Traffic | SF Office LAN | STOPPED | 0 B | Edit Start Clear Remove |

[Add A New Job](#)

Add New Job

Capture Settings

Name:

Status: **Stopped**

Interface:
(NetProfiler Export Enabled)

BPF Filter:

Maximum packet size for capture: Bytes

Enable Indexing

Enable DPI

Start new job immediately

Retention Settings

Data Retention | **Start / Stop Settings**

Packet Data (Packet Storage Total Space: 65.48 TB, Unallocated Space: 44.84 TB)

Packet Retention Size: TB % Of Disk

Additional Retention Criteria: Packets
 Seconds

Microflow Index (User Data Storage Total Space: 2.96 TB, Unallocated Space: 2.57 TB)

Retain Index On Disk Up To: GB % Of Disk

Additional Retention Criteria: Days
 Synchronize With Packet Recording

Note: Packets are stored in specially formatted packet storage. Indexes are stored in the conventional User Data Storage.

Capture settings

- Enter a job name. _____
- Select an interface. _____
- Enter a BPF filter, if desired. _____
- Set the maximum number of bytes saved for each packet —the *snaplen*. Specifying 65535 captures the entire packet. _____
- Click to enable Microflow Indexing. _____
- Click to enable DPI metrics. _____
- Click to start the job as soon as you save the job parameters. _____

Capture Settings

Name:

Status: **Stopped**

Interface: (NetProfiler Export Enabled)

BPF Filter:

Maximum packet size for capture: Bytes

Enable Indexing

Enable DPI

Start new job immediately

A BPF filter can select a subset of network traffic for capturing. For example, the filter `src host 192.168.43.17` captures only packets with a source address of 192.168.43.17. You can find more information on BPF filters at <http://wiki.wireshark.org/CaptureFilters>.

Data Retention settings

Note: Retention criteria are evaluated after each 128 MB capture block, then enforced.

- Specify the amount of packet data to save. _____
- Specify the maximum amount of indexing data to save. _____
- Click to synchronize indexing with packet recording. _____

Retention Settings

Data Retention | Start / Stop Settings

Packet Data (Packet Storage Total Space: 65.48 TB, Unallocated Space: 44.84 TB)

Packet Retention Size: TB % Of Disk

Additional Retention Criteria: Packets

Seconds

Microflow Index (User Data Storage Total Space: 2.96 TB, Unallocated Space: 2.57 TB)

Retain Index On Disk Up To: GB % Of Disk

Additional Retention Criteria: Days

Synchronize With Packet Recording

Note: Packets are stored in specially formatted packet storage. Indexes are stored in the conventional User Data Storage.

Specify the amount of storage to reserve for packet data, either in bytes or as a percentage of the packet storage size. Additionally, you can specify a maximum amount of packets to store or a maximum time interval to record. After a limit is reached, the oldest packets are discarded as new packets arrive.

Note that a NetShark appliance stores packet data on its Packet Storage RAID array and stores Microflow Indexing data in the User Data Storage subsystem of System Storage.

Microflow Indexing

Microflow Indexing computes summary data for conversations between devices on the network. (See Microflow Indexing on page 3 for more information.) Its behavior depends on the states of two check boxes, both on the Add New Job page.

Table 1

| | |
|---|---|
| <input type="checkbox"/> Enable Indexing <input type="checkbox"/> Synchronize With Packet Recording | No Microflow Indexing data will be collected. This is generally reserved for cases where the indexing computation affects the performance of packet capture. |
| <input checked="" type="checkbox"/> Enable Indexing <input type="checkbox"/> Synchronize With Packet Recording | If indexing is enabled but not synchronized with packet recording, the amount of indexing data stored on the disk is determined by the amount of storage allocated (bytes or percentage of disk space) or the time interval (days). When the space or time limit is reached, the oldest index summaries are discarded as new ones arrive. Indexing time is typically set to be significantly longer than packet recording time since it consumes much less storage. |
| <input checked="" type="checkbox"/> Enable Indexing <input checked="" type="checkbox"/> Synchronize With Packet Recording | The duration of Microflow Indexing is kept synchronized with that of packet capture. This ensures that all Packet Analyze Views of the network traffic-both those that use only the indexing data and those that require only packet data-are available for the entire time period. It likely limits the amount of indexing data that can be retained, however. |

Start / Stop settings

Two types of settings are available: start and/or stop times and job size limits. One or both types of settings can be applied. Capture stops after the first limit of any type is reached.

Retention Settings

Data Retention

Start / Stop Settings

Requested Start/Stop Time:

Capture Start Time

Capture Stop Time

Note: Time format is 'MM/DD/YYYY HH:MM:SS' browser local time. The local time zone offset (from UTC) is -0800.

Stop Rule:

MB % Of Disk

Packets

Seconds

Note: These options are only available if indexing is not enabled for this job.

Note: The 'Stop Rule' values apply each time the job is started, not to the job as a whole. For example, if a job already contains 2GB of traffic and a 1GB 'Stop Rule' is applied, the job will be stop when its size reaches 3GB.

Specify specific start and/or stop times.

Specify job size limit in terms of storage space, and/or packets, and/or length of time.

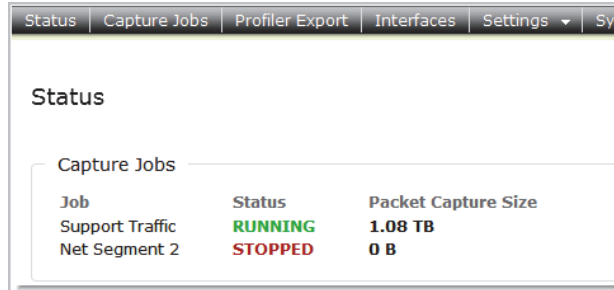
The Start / Stop settings are not available if Microflow Indexing has been enabled for the capture job.

Viewing capture job status

For quick capture job status, look on the Status page.

Click the **Status** tab to see quick job status.

Status of capture jobs



The screenshot shows a web interface with a navigation bar at the top containing tabs: Status, Capture Jobs, Profiler Export, Interfaces, Settings, and Sys. The main content area is titled "Status" and contains a section for "Capture Jobs". Below this section is a table with three columns: Job, Status, and Packet Capture Size. The table lists two jobs: "Support Traffic" with a status of "RUNNING" and a size of "1.08 TB", and "Net Segment 2" with a status of "STOPPED" and a size of "0 B".

| Job | Status | Packet Capture Size |
|-----------------|----------------|---------------------|
| Support Traffic | RUNNING | 1.08 TB |
| Net Segment 2 | STOPPED | 0 B |

The Status page updates the capture statistics periodically. Click the Status tab to update the page manually.

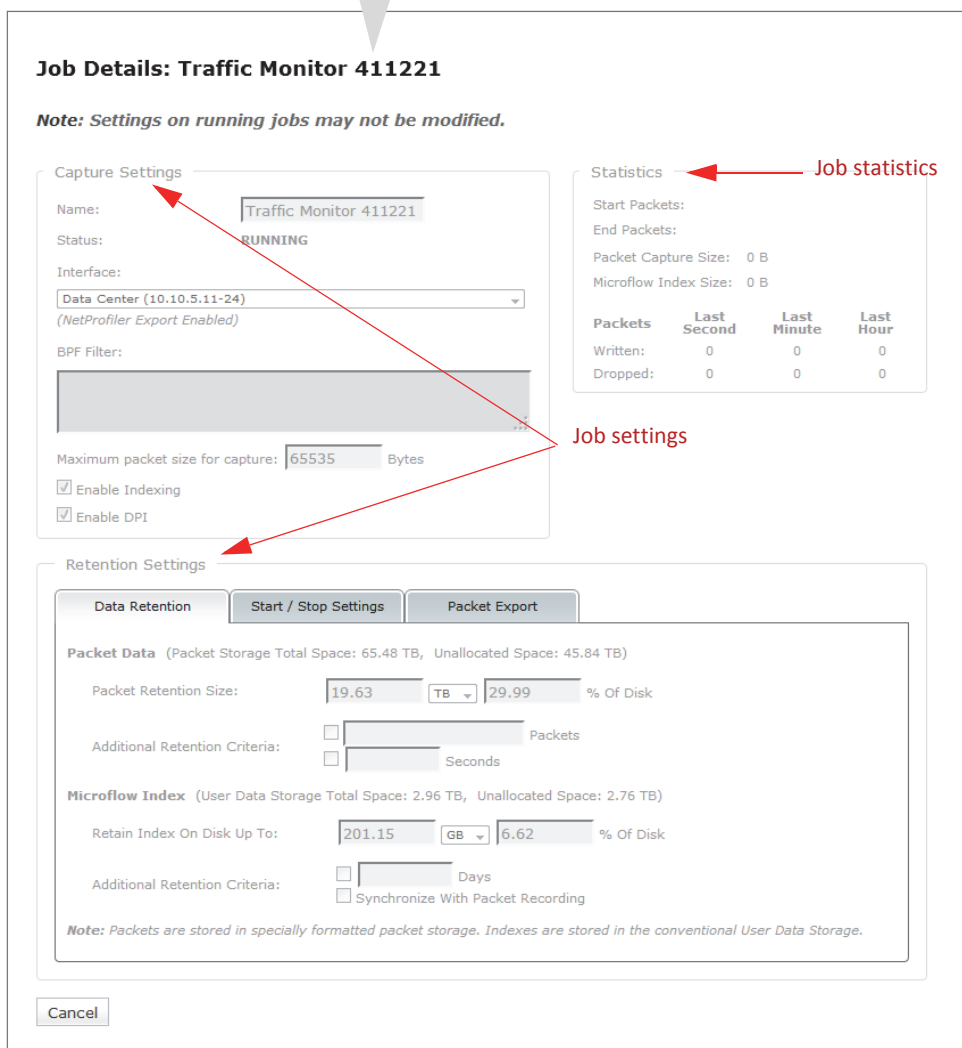
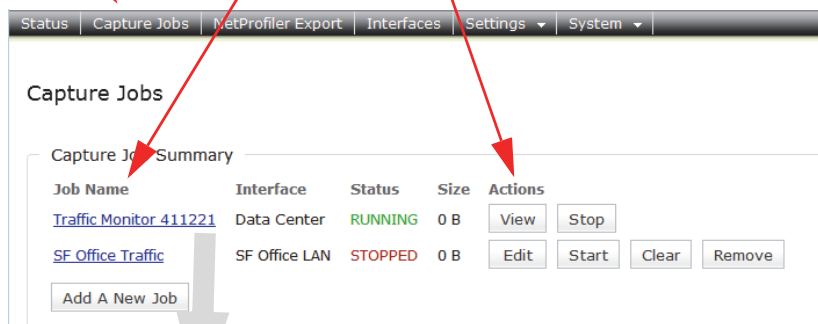
For more information, go to the Job Details page for a particular job, as described below.

Job Details page

Details about any capture job's status are available by following the steps below.

1) Click the Capture Jobs tab.

2) Click the Job Name or the View or Edit buttons to see the Job Details.



Controlling capture jobs

Capture jobs start or stop automatically under certain circumstances:

- You checked the Start New Job Immediately check box when setting up the job, and then clicked the Save button.
- A preset Absolute Start/Stop Time is reached.
- The job matches a Stop capturing after rule (storage space, number of packets, or elapsed time).

You can control jobs manually using the buttons on the Capture Jobs page. Note that the buttons change according to the status of the job.

The screenshot shows the 'Capture Jobs' page in the NetShark web interface. The page has a navigation bar with tabs for 'Status', 'Capture Jobs', 'Profiler Export', 'Interfaces', 'Settings', and 'System'. Below the navigation bar is the 'Capture Jobs' section, which includes a 'Capture Job Summary' table and an 'Add A New Job' button. The table lists two jobs: 'Support Traffic' (RUNNING) and 'Net Segment 2' (STOPPED). The 'Support Traffic' job has 'View' and 'Stop' buttons. The 'Net Segment 2' job has 'Edit', 'Start', 'Clear', and 'Remove' buttons. Red arrows point from text annotations to these buttons: 'Click to stop a running job.' points to the 'Stop' button; 'Click to start a stopped job.' points to the 'Start' button; 'Click to clear packet and indexing data from storage.' points to the 'Clear' button; and 'Click to clear packet and indexing data and to delete the job configuration.' points to the 'Remove' button.

| Job Name | Interface | Status | Size | Actions |
|---------------------------------|---------------|---------|----------|-------------------------|
| Support Traffic | Net Segment 1 | RUNNING | 51.20 GB | View Stop |
| Net Segment 2 | Net Segment 2 | STOPPED | 0 B | Edit Start Clear Remove |

Annotations:

- Click to stop a running job. (points to Stop button)
- Click to start a stopped job. (points to Start button)
- Click to clear packet and indexing data from storage. (points to Clear button)
- Click to clear packet and indexing data and to delete the job configuration. (points to Remove button)

Using Packet Analyzer to create capture jobs

Packet Analyzer is well integrated with NetShark and provides access to the NetShark Web interface to create and manage capture jobs on a NetShark. Accessing the NetShark Web interface using Packet Analyzer is explained in "[Logging in using Packet Analyzer.](#)"

For full information on using this hardware/software combination to set up capture jobs, please see the "NetShark Packet Recorder" section of the *SteelCentral Packet Analyzer Reference Manual*.

Exporting packets to a file

You can export packets from a capture job to a file on your local system.

- 1) Click the Capture Jobs tab.
- 2) Click a job name or a **View** or **Edit** button to bring up the Job Details page.

Capture Jobs

Capture Job Summary

| Job Name | Interface | Status | Size | Actions |
|---------------------------------|--------------------------|---------|----------|---|
| Support Traffic | Data Center | RUNNING | 36.65 GB | <input type="button" value="View"/> <input type="button" value="Stop"/> |
| Net Segment 2 | San Francisco Office LAN | STOPPED | 0 B | <input type="button" value="Edit"/> <input type="button" value="Start"/> <input type="button" value="Clear"/> <input type="button" value="Remove"/> |

Job Details: Support Traffic

Note: Settings on running jobs may not be modified.

Capture Settings

Name:

Status: **RUNNING**

Interface: (NetProfiler Export Enabled)

BPF Filter:

Maximum packet size for capture: Bytes

Enable Indexing

Enable DPI

Statistics

Start Packets: 7/12/2014 14:54:44 (-0700)
 End Packets: 7/12/2014 15:10:21 (-0700)

Packet Capture Size: 93.72 GB
 Microflow Index Size: 96.98 MB

| Packets | Last Second | Last Minute | Last Hour |
|----------|-------------|-------------|-----------|
| Written: | 124.85 K | 7.42 M | 114.44 M |
| Dropped: | 0 | 0 | 0 |

Retention Settings

Data Retention | **Start / Stop Settings** | **Packet Export**

Start Export: From Beginning Of Job
 From Start Time:
Note: Time format is 'MM/DD/YYYY HH:MM:SS' browser local time. The local time zone offset (from UTC) is -0700.

End Export: At End Of Job
 At End Time:
Note: Time format is 'MM/DD/YYYY HH:MM:SS' browser local time. The local time zone offset (from UTC) is -0700.

After Bytes Have Been Recorded
 After Packets Have Been Recorded

Export File Format & Timestamp Resolution:
 pcap (microsecond)
 pcap (nanosecond)
 pcap-ng (microsecond)
 pcap-ng (nanosecond)

Limit Each Packet To:
 No Limit
 Bytes

- 3) Set the packet export Start/End parameters (time and/or size).

- 4) Set export file format and time resolution.

- 5) Click to prepare export.

- 6) Click to download.

Using SSL Decryption

In software version 10.7 (and later) HTTP traffic encrypted using the SSL protocol can be decrypted when the key exchange algorithm uses RSA keys, as specified below.

Specifications

SSL/TLS versions

- SSL v2
- SSL v3
- TLS 1.0
- TLS 1.1
- TLS 1.2 (limited to AES CBC)

Private Keys

- Type: RSA
- Format: PEM
 - PKCS#1
 - PKCS#8
 - plain text or password encrypted
- Supported key lengths (bits): 128, 256, 512, 1k, 2k, 4k, 8k
- Maximum length: 8192 bits
- Maximum number of keys: 512

Certificate Fingerprint Display

- SHA1 digest (if a certificate is included with an RSA private key)

Supported Layer 7 Protocol

- HTTPS

Supported Session Resumption

- Session ID

Defining Decryption Keys

A decryption key contains a server's RSA private key and optional password; the server's IP address and a TCP port (IP/port pair); a description; and at least one assigned user group. A maximum of 512 decryption keys can be entered. If a private key includes a certificate an SHA1 fingerprint is calculated and listed with the decryption key information.

- Each IP/port pair can be assigned to only one private key.
- A private key can be assigned to one or more unique IP/port pairs.
- If the private key or IP/port pair changes a decryption key must be removed and replaced with a new key.

- Decryption key descriptions and the groups assigned to a decryption key can be edited by an administrator (a user belonging to a group with the “is Administrator” capability).

Important: Before updating or installing NetShark software, be sure you understand the impact on SSL decryption keys:

- A software update preserves SSL decryption keys.
- A software install (fresh install) deletes SSL decryption keys.

Note: Adding, editing, removing, and using SSL decryption keys can be audited. See Settings > Logging Settings in the NetShark Web interface and “Setting up logging” for more information. You also can be notified about decryption key activity - see Settings > Notification Settings in the NetShark Web interface and “Setting up notifications” for more information.

Entering Decryption Keys

An administrator must log in to the NetShark and go to the Settings > SSL Decryption page in the NetShark Web interface.

SSL Decryption

Sharing Views Containing Decrypted Information
 Allow users to share views that include decrypted data

Enabled Protocol HTTP

Apply

Decryption Keys

| <input type="checkbox"/> | Server IP | Server Port | Description | Groups | Fingerprint |
|--------------------------|----------------|-------------|------------------------------------|-------------------------------|--|
| <input type="checkbox"/> | 216.246.0.13 | 443 | PEM Key Server B3-12 | Administrators | - |
| <input type="checkbox"/> | 131.83.131.211 | 7 | PEM Key w-certificate Server M24-3 | Administrators | SHA1:1D:BF:2D:C6:02:1E:4E:31:D8:14:DA:BF:07:0B:76:11:2D:6D:2D:1B |
| <input type="checkbox"/> | 10.5.14.95 | 443 | Internal Web Server J1-412 | Administrators NormalUsers | - |

Add New Edit Selected Remove Selected

Enable/disable sharing views containing decrypted SSL traffic data.

If a private key includes a certificate, the calculated fingerprint is listed here.

Add New SSL Decryption Key

Server IP:

Server Port:

Description:

PEM:

Password:

Groups:

Add Cancel

Server IP address (xxx.xxx.xxx.xxx)

RSA private key or private key plus certificate

Enter if private key is protected with a password.

Select groups to use decryption key when applying a view.

Assigning User Groups to Decryption Keys

Access control to decryption keys is set by a user's group memberships, as follows:

- Only users belonging to a group with the "is Administrator" capability (administrators) can enter and edit a key. Group members can use any decryption key to decrypt traffic for views. The SSL Decryption page in the NetShark Web interface lists all decryption keys and includes buttons to add, edit or remove selected keys. Note: Private keys can only be added or removed - they cannot be edited.

- Users belonging to a group with “Can Apply Views On Files” and/or “Can Apply Views On Interfaces” capabilities can use decryption keys. Group members can use decryption keys assigned to any groups they belong to for decrypting traffic for views. The SSL Decryption page in the NetShark Web interface shows all keys for the groups a user belongs to.
- Users belonging to groups without “is Administrator,” or “Can Apply Views On Files” and/or “Can Apply Views On Interfaces” capabilities cannot use decryption keys and cannot decrypt traffic for views. The SSL Decryption page in the NetShark Web interface shows “No Keys Defined.”

Users and groups are configured on the Settings > Users and Groups page of the NetShark Web interface. For more information, see “Managing users and groups” in this document.

Decrypting HTTP traffic using SSL

For decryption, traffic using SSL encryption must meet the following requirements:

- The key exchange algorithm uses RSA keys.
- The captured traffic includes both the client side and the server side of a conversation.
- The capture traffic includes the full initial SSL session establishment sequence.

CAUTION: Views using HTTP metrics can include traffic information and data from SSL-encrypted traffic. Such views may contain decrypted data you do not want disclosed, for example, cookies or Web objects. By default, these views can be shared with other groups who would otherwise not be able to see the decrypted data. Administrators can turn off the sharing of views containing decrypted traffic data under “Sharing Views Containing Decrypted Information” on the SSL Decryption page. To disable, uncheck the “Enabled” box under “Sharing Views Containing Decrypted Information” on the SSL Decryption page.

Note: All shared views containing decrypted data must be unshared or closed before sharing can be disabled.

Check the following before decrypting SSL-encrypted HTTP traffic for views:

- The decryption key is entered on the appliance capturing the traffic or storing the trace file of interest.
- The sharing of views containing decrypted traffic data with other groups who cannot decrypt the traffic in the view has been enabled (the default setting) or disabled as needed.

When a user applies a view:

- If the traffic uses an IP/port pair that matches a decryption key assigned to a group the user belongs to, the packets are decrypted to provide traffic information and data to calculate metrics for the view. NetShark notifications can be sent or log messages triggered when a decryption key is used.
- If a user is not a member of a group assigned to the decryption key, no error is issued and the traffic is not decrypted.

Note: Decrypted packets are not stored and cannot be exported or sent outside the appliance. Copies of the packets captured on the network are sent to Wireshark, SteelCentral Transaction Analyzer, a file, or NetProfiler - the packets are not decrypted.

Managing users and groups

All communication between the SteelCentral NetShark and the SteelCentral Packet Analyzer uses SSL-encrypted Web communications and requires HTTP basic access authentication credentials (HTTP Authentication). The NetShark passes the authentication credentials to the Credential Manager, which determines whether the user has the permission to execute the requested operation. If not, the NetShark returns a not enough privileges error to the Packet Analyzer making the request.

Credential Manager

The Credential Manager running in the SteelCentral NetShark supports two types of authentication:

- **Local authentication.** The management of credentials is governed by the user configuration file co-located with the NetShark.
- **Remote authentication.** The management of credentials uses an external authentication/auditing server using either the RADIUS or TACACS+ protocols.

Each user has ownership of the resources that the user created, including files, folders, and views that are applied to a traffic source. With the exception of administrators, users cannot see a file or a view created by another user, and a user cannot close a view or delete a file that was created by another user.

Resources, however, can be shared among one or more groups. For local authentication, a user can be a member of one or more groups, whereas for remote authentication, a user can be a member of only one group.

Members of a group share a common folder identified with the group name. This folder can be used for trace file sharing, and all the users in the group have read and write access to the folder. When a resource is dragged into this folder, all the other members of the group immediately have access to it.

Views can be shared with other groups by right-clicking on them and selecting share with. As soon as a view is shared, the selected group immediately sees it in their sources panel. Note: sharing views is supported only with local authentication.

Users and groups are configured using the NetShark Web interface (Settings > Users And Groups).

Capabilities

The Web interface is used to configure the capabilities for users and groups. A capability is a privilege that can be granted or revoked, and is specified as an attribute of a group. The SteelCentral NetShark currently implements the following capabilities:

- **Is Administrator.** Gives members full access to the NetShark. Administrators see all the resources in the system, including views, files and folders that have been created by other users. Administrators have full control of all these resources.
- **Can Apply Views On Files.** Members can apply views to traces files residing on the NetShark, capture jobs and trace clips. In order to apply a view to a capture job or trace clip, the capability **Can Access Probe Files** is also required.
- **Can Apply Views On Interfaces.** Members can apply views to the interfaces and job interfaces on the NetShark.
- **Can Share Views.** Members can share the views created on the NetShark with any group on the same appliance. If this capability is not granted, a user can share a view with only the groups to which he belongs.

- **Can Create Files.** Enables members of the group to create files on the NetShark, by selecting Send to File in Packet Analyzer.
- **Can Import Files.** Members can import files into the NetShark through drag and drop or by clicking Import Files Into Probes in the Remote Ribbon of Packet Analyzer.
- **Can Export Files.** Members can export files from the NetShark, and move them to Packet Analyzer or to another NetShark (assuming the user has sufficient capability on the target NetShark to create a trace file). When this capability is not granted, the user is not able to export a trace file to Wireshark, because that involves exporting packets out of the NetShark to Packet Analyzer.
- **Can Create Jobs.** Members can create and manage capture jobs from the NetShark Web interface.
- **Can Schedule Watches.** Members can add a watch on a view or apply a view that has a predefined watch associated with it.
- **Can Access Probe Files.** Members can access capture jobs and trace clips located on the NetShark.

Capability policy

Since for local authentication a user can be part of one or more groups, conflicts can arise among the capabilities of the multiple groups to which a user belongs. To solve these conflicts, the NetShark grants a capability if it is enabled for any group of which the user is a member.

Adding users and groups

You must have a username and password to log in to a NetShark. Each username is associated with a user group, and each group has a set of capabilities (privileges). Add new users and groups as follows:

1) Click Settings, then Users and Groups.

2) Click to add new User or Group.

Enter user name and password.

Enter group name and description.

Select group.

Check box to enable user lockout.

Select capabilities.

Add New User

New User Name:

New User Password:

Repeat New User Password:

Group Membership:

- Administrators
- NormalUsers
- Viewers

User Can Be Locked Out:

Add New Group

Group Name:

Group Description:

Group Capabilities:

- Is Administrator
- Can Apply Views On Files
- Can Apply Views On Interfaces
- Can Share Views
- Can Create Files
- Can Import Files
- Can Export Files
- Can Create Jobs
- Can Schedule Watches
- Can Access Probe Files

Changing user passwords

You can change a user's password from the Users and Groups page, as follows:

Users And Groups

| User Name | Is Administrator | Is Locked | Group Memberships | |
|---------------------------------------|------------------|----------------|-------------------|-----------------|
| admin | Yes | Not Applicable | Administrators | Change Password |
| <input type="checkbox"/> GeorgeSegrim | No | No | NormalUsers | Change Password |
| <input type="checkbox"/> normaluser | No | Not Applicable | NormalUsers | Change Password |

1. Click to bring up the Change Password dialog.

Change Password

User Name: **GeorgeSegrim**

Enter New Password:

Enter New Password (Repeat):

2. Enter new password.

Save Cancel

Unlocking a locked-out user

If a user gets locked out due to exceeding the allowed number of unsuccessful login attempts, they will see a message on the login screen like this:

riverbed
SteelCentral™ NetShark

Username:

Password:

User account has been disabled. Contact a security administrator.

Login

This interface is supported on Mozilla Firefox 24.1 ESR and Microsoft Internet Explorer 7/8 and 9.
The software included on or with this product is owned by Riverbed Technology, Inc. and/or its licensors and any use of this product is subject to the end user license agreement located at <http://riverbed.com/license>. Any unauthorized use, reproduction or distribution is strictly prohibited.

A user with administrator privileges can unlock the account from the Users and Groups page by clicking the Unlock User button for that user.

Users And Groups

| User Name | Is Administrator | Is Locked | Group Memberships | |
|---------------------------------------|------------------|----------------|-------------------|-----------------------------|
| admin | Yes | Not Applicable | Administrators | Change Password |
| <input type="checkbox"/> GeorgeSegrim | No | Yes | NormalUsers | Change Password Unlock User |
| <input type="checkbox"/> normaluser | No | Not Applicable | NormalUsers | Change Password |

Click to unlock.

Add A New User Remove Selected

Setting up the login screen

Entries on the Authentication Settings page determine the layout of the login screen for the appliance. Click the Settings tab, then Authentication Settings to go to that screen. Then fill in the screen as follows:



Authentication Settings

General Settings

Specify Purpose At Login Click to generate a Purpose box on the login screen.

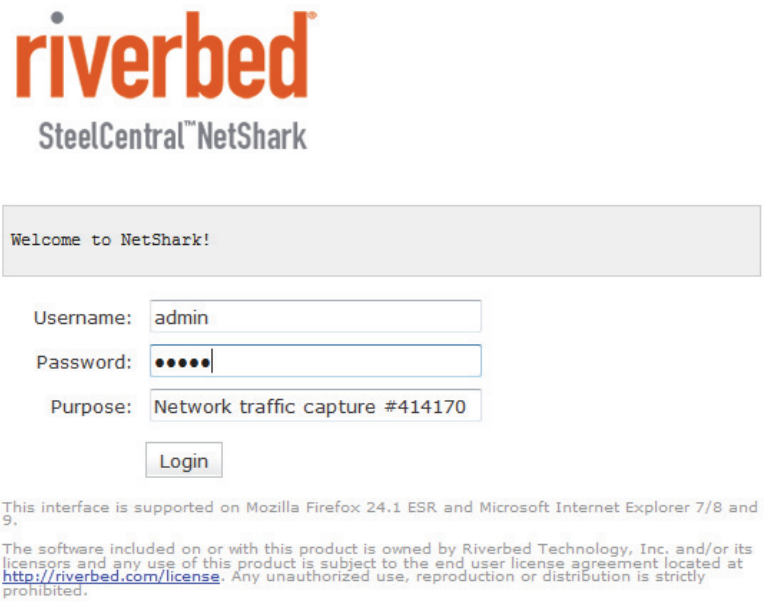
Login Banner: Enter a message to be displayed at login.

Web UI Session Timeout (minutes): Set an inactivity limit after which the session ends.

Allow Packet Analyzer to remember NetShark's password

Uncheck to require password entry at each log in. Any cached passwords in Packet Analyzer are wiped out.

The entries in the screen above produce the login screen shown below.



Information in the Purpose field may be logged to a local/remote syslog and/or to a TACACS+ or RADIUS server, depending on the AUTHENTICATION information category's audit settings. See the section on "Setting up logging" for information on those settings.

Authenticating users

Use the Authentication Settings page to set up the type of authentication used on your appliance. Select an authentication method by checking its check box in the Authentication Methods list. (Details for configuring each authentication method are given below.)

Authentication Type

Authentication Methods: Local Password File Authentication Check the box(es) for the authentication method(s) you want to use.

TACACS+ Authentication

RADIUS Authentication

Authentication Sequence:

Note: Specify the primary and fallback sequence of authentication based on the authentication methods selected.

You can choose more than one authentication method. If first method (primary) fails to authenticate, the second method (fallback) is tried, and so on. The first method to succeed is the one that is used for the session. Use the Authentication Sequence drop-down list to choose the order for authentication attempts.

Authentication Type

Authentication Methods: Local Password File Authentication

TACACS+ Authentication If you choose more than one authentication method...

RADIUS Authentication

Authentication Sequence: ...use this drop-down list to specify the order in which they are tried.

Note: Specify the primary and fallback sequence of authentication based on the authentication methods selected.

Remote Authentication Settings

If you have selected a remote authentication method (TACACS+ or RADIUS), the user interface presents additional authentication settings:

Default Remote Group

When using a remote authentication method, this lets you specify a default group assignment if a remote server (TACACS+ or RADIUS) does not assign an authenticated user to a group.

When a remote server successfully authenticates a user, it sends attribute/value pairs to the appliance to identify the group to which the user belongs; the user receives the capabilities assigned to that group. (These capabilities are set in the Users and Groups page under the Settings tab.) The Default Remote Group parameter gives you the option to specify a default group to use if the server does not return a group; in that case the user receives the capabilities of the default group. The drop-down box for the parameter lets you choose from all the groups on the appliance; if you choose “none”, no capabilities are assigned to the user.

Fallback only when servers are unavailable

When using a remote authentication method you can limit server fallback actions based on the reason for an authentication failure.

An attempt to authenticate might fail because the user does not present proper credentials or it might fail for technical reasons, such as a server being unreachable. If you leave the “For RADIUS/TACACS+, fallback only when servers are unavailable” box unchecked, any failed authentication attempt causes the appliance to try the next authentication method in the sequence (if there is one). But if you do check the box, the fallback procedure continues only if the failure is due to technical reasons; an authentication failure due to improper credentials stops the authentication process and prevents authentication of the user.

Note that if you have specified multiple TACACS+ or RADIUS servers, a failure to authenticate for technical reasons causes the appliance to try to authenticate with the next server of the same type. A failure due to improper credentials ends the authentication attempt for that authentication method; the setting of the “Fallback only when servers are unavailable” box determines whether the appliance tries to authenticate using a different method (local, TACACS+, or RADIUS).

Authentication Type

Local Password File Authentication

Authentication Methods: TACACS+ Authentication
 RADIUS Authentication

Authentication Sequence: RADIUS Only

Note: Specify the primary and fallback sequence of authentication based on the authentication methods selected.

Remote Authentication Settings

Default Remote Group: (None)

For RADIUS/TACACS+, fallback to the next authentication mechanism in the sequence above only when remote servers are unavailable

Default Remote Group: (None)
 Administrators
 NormalUsers
 Viewers

Click to allow fallback to next authentication method only in case of technical problem with server (does not fall back if authentication fails due to improper credentials).

Click to choose default group to use when server assigns authenticated user to non-existent group.

For each authentication method you choose, select its tab in the Authentication Parameters section and fill in the parameters (described below). When you have finished, click the Apply button in the lower left corner.

Click a tab, then fill in the authentication parameters.

Authentication Parameters

Local TACACS+ RADIUS

When you have finished filling in the parameters, click the Apply button in the lower left corner.

Apply

Click when done.

Local Password File authentication

This authentication type uses the user information you set up in the Add New User screen (see Adding Users and Groups). If the username and password match a username and password combination stored in the NetShark, you are logged in to the appliance. The appliance grants you the capabilities of the group you are assigned to.

The Local tab of the Authentication Parameters lets you set various password parameters. Click the Default Settings button to set all parameters to 0 (unconstrained); click the STIG Compliant Settings button to set parameters to values that comply with the Security Technical Implementation Guides (STIG) of the Joint Interoperability Test Command (JITC) of the U.S. Department of Defense.

The image displays two screenshots of the 'Authentication Parameters' configuration interface for Local authentication. Both screenshots show the 'Local' tab selected, with 'TACACS+' and 'RADIUS' tabs also visible. The left screenshot shows the 'Default Settings' configuration, where all parameters are set to 0. A red arrow points to the 'Default Settings' button with the text 'Click to disable all constraints.' The right screenshot shows the 'STIG Compliant Settings' configuration, where parameters are set to 3, 90, 8, 1, 1, 1, 1, and 10. A red arrow points to the 'STIG Compliant Settings' button with the text 'Click to apply STIG-compliant settings.'

| Parameter | Default Settings (Left) | STIG Compliant Settings (Right) |
|---|-------------------------|---------------------------------|
| Number of unsuccessful attempts before user is locked out | 0 | 3 |
| Number of days after which password expires | 0 | 90 |
| Minimum password length | 0 | 8 |
| Minimum number of upper-case letters | 0 | 1 |
| Minimum number of lower-case letters | 0 | 1 |
| Minimum number of numeric characters | 0 | 1 |
| Minimum number of special characters | 0 | 1 |
| Number of previous user passwords stored in history | 0 | 10 |

TACACS+ authentication

If you select TACACS+ Authentication on the Authentication Settings screen, click the TACACS+ tab under Authentication Parameters and fill in the parameters.

Click here to add a new server.

Authentication Parameters

Local TACACS+ RADIUS

| Server Mappings: | IP Address | Port | Shared Secret |
|------------------|----------------------|----------------------|----------------------|
| | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Client Port:

Authorization Attribute:

Authorization Value:

Authorization Response Attribute:

Note: If set to "", only the first attribute-value pair returned by the server will be considered during authorization.*

TACACS+ Accounting: Enable TACACS+ Accounting

Accounting Attribute:

Accounting Value:

Accounting Terminator:

——— Fill in parameters as desired, then click **Apply**.

For servers, specify the IP address and Shared Secret. You can enter up to eight TACACS+ servers.

| IP Address | Port | Shared Secret |
|--------------------------------------|------|---------------|
| <input type="checkbox"/> 10.143.17.5 | 49 | •••••••• |

Fill in IP address and Shared Secret for each server you add (up to 8).

Fill in the parameters as follows:

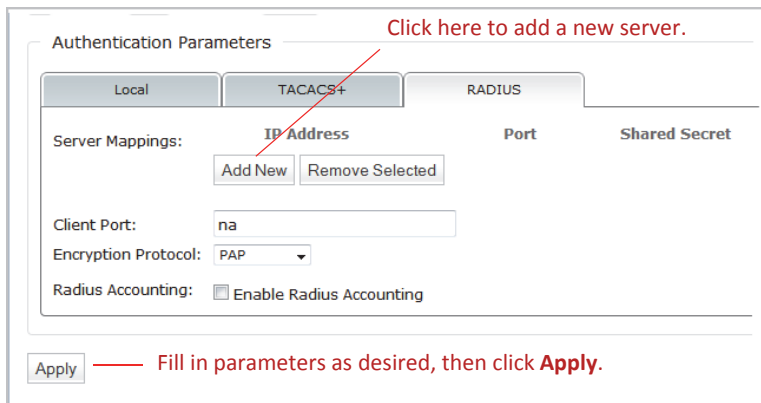
- **Server IP address**—IP address of the TACACS+ server. This field accepts only numeric IP addresses; host names are not supported.
- **Server Port**—TCP port the TACACS+ server is listening on. This is preconfigured to port 49.
- **TACACS+ Shared Secret**—Shared secret configured by the TACACS+ protocol, used to protect the communication between NetShark and the TACACS+ server.
- **Client Port**—This field is part of the TACACS+ protocol and it contains the name of the client port used on the NAS server. Please consult the documentation for the TACACS+ server for details on the correct client port to use.
- **Authorization Attribute and Authorization Value**—These two fields are used in the authorization step to specify the attribute-value pair used to request a specific service to the TACACS+ server. During the TACACS+ protocol authorization step, NetShark sends the attribute-value pair “Authorization-Authorization-Value” to the TACACS+ server. The server uses the pair together with the user-name to identify the user group.
- **Enable TACACS+ accounting**—Enables the remote data accounting on the TACACS+ server.
- **Accounting Attribute and Accounting Value**—These two values are used to create an attribute-value pair that NetShark sends to the TACACS+ server together with the accounting data to trace the accounting communication.
- **Accounting Terminator**—This field is specified as the last value in the attribute-value pairs list, and its value may change based on the TACACS+ server in use.

During the authentication process, NetShark sends the user name and password credentials to the TACACS+ server to validate the credentials and indicate the group that the user is a member of. If the credentials are invalid or if the authorized group name received from the TACACS+ server does not match any of the local groups on the NetShark, the authentication will fail. If, however, the user is successfully authenticated and the appliance has been configured with a Default Remote Group, the user receives the capabilities assigned to the default group.

Please note that you must configure the authentication and authorization parameters on the TACACS+ server as well as on the NetShark. These values must be coordinated between the server and the appliance. If they are not, authentication will fail and users will not be able to log in to the appliance.

RADIUS authentication

If you select RADIUS Authentication on the Authentication Settings screen, click the RADIUS tab under Authentication Parameters and fill in the parameters.



Authentication Parameters

Local TACACS+ RADIUS

Server Mappings:

| IP Address | Port | Shared Secret |
|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> |

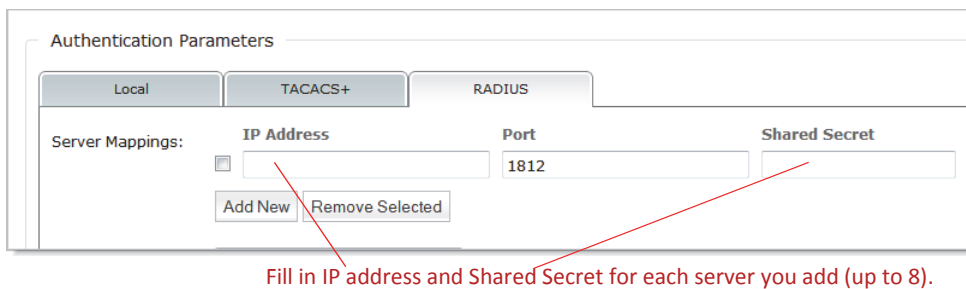
Client Port:

Encryption Protocol:

RADIUS Accounting: Enable RADIUS Accounting

Apply — Fill in parameters as desired, then click **Apply**.

For servers, specify the IP address and Shared Secret. You can enter up to eight RADIUS servers.



Authentication Parameters

Local TACACS+ RADIUS

Server Mappings:

| IP Address | Port | Shared Secret |
|---|-----------------------------------|----------------------|
| <input type="checkbox"/> <input type="text"/> | <input type="text" value="1812"/> | <input type="text"/> |

Fill in IP address and Shared Secret for each server you add (up to 8).

Fill in the parameters as follows:

- **Server IP address**—IP address of the RADIUS server. This field accepts only numeric IP addresses; host names are not supported.
- **Server Port**—TCP port the RADIUS server is listening on. This is preconfigured to port 1812.
- **RADIUS Shared Secret**—Shared secret configured by the RADIUS protocol, used to protect the communication between NetShark and the RADIUS server.
- **Client Port**—This field is part of the RADIUS protocol and it should contain the name of the client port used on the NAS server. Please consult the documentation for your RADIUS server for details on the client port to use.
- **Encryption protocol**—Specifies the protocol used to encrypt data in the path between NetShark and the authentication server. Four protocols are supported:
 - **PAP**—Basic RADIUS encryption; uses MD5 hashes and XOR
 - **CHAP**—Challenge-Handshake Authentication Protocol
 - **MSCHAP1**—MS CHAP version 1
 - **MSCHAP2**—MS CHAP version 2
- **Enable RADIUS Accounting**—Enables remote data accounting on a RADIUS server.

During the authentication process the NetShark sends the user name and password credentials to the RADIUS server. If the authentication is successful, the RADIUS server responds with a one or more attribute-value pairs associated with the local group the user belongs to. The appliance attempts to match the first of these pairs with the configured local groups, and if there is a match the user is authorized with the capabilities assigned to that group.

If the credentials are invalid or if the authorized group name received from the RADIUS server does not match any of the local groups on the appliance, the authentication process will fail. If, however, the user is successfully authenticated and the appliance has been configured with a Default Remote Group, the user receives the capabilities assigned to the default group.

Please note that you must configure the authentication and authorization parameters on the RADIUS server as well as on the appliance. These values must be coordinated between the server and the appliance. If they are not, authentication will fail and users will not be able to log in to the appliance.

Managing security functions

Setting up logging

The Logging Settings page lets you control which system events get logged for auditing purposes. There are 11 categories of information that can be logged, and you can log to local/remote syslogs, to a RADIUS/TACACS+ log, or both. You can find the Logging Settings page at Settings > Logging Settings.

Logging Settings

Click to set logging for a single category. Click to set logging for all categories.

Logging Category Information

| Name | Description | Local/Remote Syslog Settings | RADIUS/TACACS+ Log Settings |
|---------------------|---|--|--|
| | | <input type="button" value="Set All"/> | <input type="button" value="Set All"/> |
| AUTHENTICATION | Audits login attempts to the system and modifications to the authentication settings. | All Events | Disabled |
| CAPTURE JOBS | Audits any modification to capture jobs and data extraction operations from a capture job. | All Events | Disabled |
| COMMUNICATIONS | Audits connections initiated and terminated by NetShark such as HTTPS requests and connections to NetProfiler systems. | Disabled | Disabled |
| CRYPTOGRAPHY | Audits the use of FIPS compliant cryptographic algorithms and failures in the cryptographic functions used for hashing. | All Events | Disabled |
| FILE OPERATIONS | Audits file operations triggered from Packet Analyzer such as add / remove directories, copy / delete / move files and export of pcap data to file and wireshark. | All Events | Disabled |
| LICENSING | Audits addition and removal of licenses. | All Events | Disabled |
| SETTINGS | Audits modifications to various system configuration items from the Web Interface such as networking, time and NTP synchronization, capture ports and auditing. | All Events | Disabled |
| SSL DECRYPTION KEYS | Audits operations on or with SSL private keys (add, remove, edit, decrypt traffic). | All Events | Disabled |
| SYSTEM OPERATIONS | Audits system-level operations such as shutdown, reboot, probe restart, formatting packet storage, and requests to download the audit trail. | All Events | Disabled |
| USER MANAGEMENT | Audits user management operations such as addition and deletion of user and groups along with user lock / unlock operations and password modifications. | All Events | Disabled |
| VIEWS | Audits any operation performed on a view (creation, deletion, locking, unlock, modification). | All Events | Disabled |
| WATCHES | Audits the creation/deletion of watches. | All Events | Disabled |

Remote Logging Servers

Syslog
TACACS+
RADIUS

| Servers: | Host | Port | Protocol | Minimum Severity |
|--|------|------|----------|------------------|
| <input type="button" value="Add New"/> <input type="button" value="Edit Selected"/> <input type="button" value="Remove Selected"/> | | | | |

Click when done.

To set the logging for an information category, click the drop-down list that corresponds to the category and logging location and select which types of events in that category—all events, errors only, or no events—you want to have logged. To set all information categories for a logging location (local/remote syslog or

RADIUS/TACACS+ log) at once, click the drop-down list at the top of the column for that location.



Local logging

Events logged on the local system can be seen by examining the log file at System > Maintenance. Click the Download Log button to save a .TGZ archive of the logs. Once you download and unpack the archive, the syslog files are the files named messages and messages-<datetime>.

Remote Syslog logging

Release 10.6 (and later) supports sending syslog messages to external servers, including Security Information and Management (SIEM) tools. Configure syslog servers on the syslog tab under Remote Logging Servers. Click Add New to add a new server. Click Apply when finished to save your changes.

Remote Logging Servers

Syslog TACACS+ RADIUS

Servers:

| <input type="checkbox"/> | Host | Port | Protocol | Minimum Severity |
|--------------------------|-----------|------|----------|------------------|
| <input type="checkbox"/> | 10.1.10.1 | 514 | UDP | ERROR |
| <input type="checkbox"/> | 10.1.10.2 | 514 | TCP | WARNING |

Server DNS name or IP address.

Add New Server

| Host | Port | Protocol | Minimum Severity |
|----------------------|------|----------|------------------|
| <input type="text"/> | 514 | UDP | Info |

Add Cancel

Add New Edit Selected Remove Selected

Apply

Click when done to apply changes.

Existing servers can be edited or removed using the same screen. Attempts to add a server a second time are flagged as errors and the existing server entry is preserved.

The TACACS+ and RADIUS tabs provide information on the current accounting configuration on those servers. Accounting changes can be made on the Settings > Authentication Settings page of the Web interface.

RADIUS/TACACS+ logging

Events are logged to the TACACS+ or RADIUS server used for authentication. The Accounting configuration, found on the TACACS+ or RADIUS server tabs under Authentication Parameters on the Settings > Authentication Settings page, determines where the logs are located on the server. Note, however, that if you have multiple Authentication Methods set up, only the first one in the Authentication Sequence can be used for remote logging. (See “Authenticating users” for a description of the Authentication Methods and Authentication Sequence settings.)

Consider, for instance, an authentication configuration that sets up both TACACS+ and RADIUS as Authentication Methods and specifies an Authentication Sequence of “RADIUS; TACACS+”. Assume that your Remote Log Settings are enabled for All Events.

Authentication Type

Local Password File Authentication

Authentication Methods: TACACS+ Authentication
 RADIUS Authentication

Authentication Sequence: RADIUS; TACACS+ **RADIUS first, then TACACS+**

Note: Specify the primary and fallback sequence of authentication based on the authentication methods selected.

Remote Authentication Settings

Default Remote Group: (None)

For RADIUS/TACACS+, fallback to the next authentication mechanism in the sequence above only when remote servers are unavailable.

If an authentication attempt succeeds with the RADIUS server, the logging occurs as expected: events are logged to the RADIUS server.

But if the authentication attempt fails with the RADIUS server and then falls back to the TACACS+ server and succeeds, events are not logged to the TACACS+ server since TACACS+ was not the first authentication method specified in the Authentication Sequence setting.

Setting up a firewall

The Firewall Settings page, available at Settings > Firewall Settings, lets you set up an inbound-only firewall to control access to the appliance. This firewall applies to management interfaces; it does not apply to capture interfaces. The same settings are applied to all management interfaces.

The firewall is disabled by default; check the Enable Firewall Protection check box to enable it. The default configuration for an enabled firewall allows access through the Web UI from a Web browser or a Packet Analyzer console (using HTTPS) or through an SSH console, and allows the appliance to respond to ICMP messages (such as a ping). All other access is denied by default.

Firewall Settings

General Settings

Enable Firewall Protection Click to enable firewall.

Default Action: Deny

Firewall Rules

| | Action | Protocol:Port | Source | Description |
|---|--------|---------------|--------|-------------------------------|
| Delete Edit ▼ | Allow | TCP:443 | ALL | Allow HTTPS for all the hosts |
| Delete Edit ▲ ▼ | Allow | TCP:22 | ALL | Allow SSH for all the hosts |
| Delete Edit ▲ | Allow | ICMP | ALL | Allow ICMP for all the hosts |

Add New Rule

- The Default Action tells the firewall what to do with a packet that does not match any of the rules. You can set the Default Action to either Allow or Deny.

Firewall Settings

General Settings

Enable Firewall Protection

Default Action: Deny Click to set default action.

Allow

Deny

You can edit existing rules or add new ones. Click the Edit button to edit an existing rule; click the Add New Rule button to add a new rule.

Delete Edit ▲ ▼ Allow IC Click to edit existing rule.

Add New Rule Click to add new rule.

The firewall rule parameters are the same when rules are added or edited.

Actions can be:

- Allow
- Deny
- Allow And Log

Tasks

■ Deny And Log

Logged actions show up in the syslog files. You can download these files using the Download Log button on the System > Maintenance page. After you unpack the archive, you can find logged actions in the messages and messages-<datetime> files.

Protocols can be:

- ALL
- TCP
- UDP
- ICMP

If no protocol is specified the rule applies to all protocols.

- For TCP and UDP protocols, the port number can range from 0 to 65535; if no port number is specified, the rule applies to all ports. Service names (HTTP, FTP, and so on) are not allowed in this field.
- Sources can be IP addresses in:
 - CIDR notation (192.168.1.0/24)
 - complete IP/mask format (192.168.1.0/255.255.255.0)
 - single host IP address with no mask (192.168.1.23)

If no IP address is specified, the rule applies to all IP addresses.

Hostnames are not allowed in this field.

The screenshot shows a web form titled "Adding A New Rule". It contains the following fields and controls:

- Action:** A dropdown menu with "Allow" selected.
- Protocol:** A dropdown menu with "TCP" selected.
- Port:** A text input field containing "80".
- Source:** An empty text input field.
- Description:** A text area containing "Allow HTTP for all the hosts".
- Buttons:** "Update Table" and "Cancel Add".

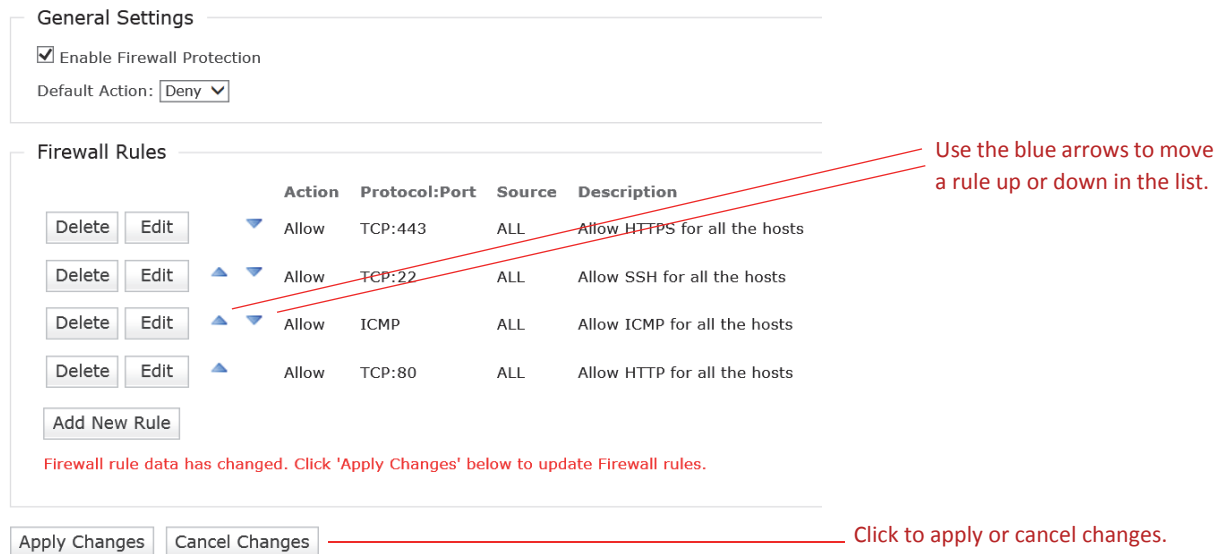
Red lines and arrows point from the "Action", "Protocol", "Port", and "Source" fields to the text "Fill in parameters." on the right. A red line and arrow point from the "Cancel Add" button to the text "Click when done." below it.

Note: A source may be specified as single IP (w.x.y.z), CIDR notation (a.b.c.d/24), IP/mask (1.2.3.4/255.255.255.0) or 'ALL'.

Note that clicking the Update Table button enters the rule in the Firewall Rules table, but that no changes are effective until you click the **Apply Changes** button at the bottom of that table.

- Rules are evaluated from top to bottom. As soon as a rule is matched, the action for that rule is applied and processing for that packet stops. You can change the order of evaluation by using the blue arrows to move a rule up or down in the list.

Firewall Settings



General Settings

Enable Firewall Protection

Default Action: Deny

Firewall Rules

| | Action | Protocol:Port | Source | Description |
|---|--------|---------------|--------|-------------------------------|
| Delete Edit ▼ | Allow | TCP:443 | ALL | Allow HTTPS for all the hosts |
| Delete Edit ▲ ▼ | Allow | TCP:22 | ALL | Allow SSH for all the hosts |
| Delete Edit ▲ ▼ | Allow | ICMP | ALL | Allow ICMP for all the hosts |
| Delete Edit ▲ | Allow | TCP:80 | ALL | Allow HTTP for all the hosts |

Add New Rule

Firewall rule data has changed. Click 'Apply Changes' below to update Firewall rules.

Apply Changes Cancel Changes

Changes are not effective until you click the Apply Changes button at the bottom of the page.

It is possible to configure the firewall in such a way that you lock yourself out of the appliance. If this occurs, you can make a direct connection to the NetShark through the serial port or the keyboard/monitor ports and disable the firewall using the system firewall disable CLI command. (See the System commands section in “Reference.”) Once the firewall is disabled, you can reconfigure it to avoid the problem, and then re-enable it.

Managing certificates

You can manage certificates from the SSL Certificate Management page: Settings > SSL Certificate Management.

There are three types of certificate:

- Web Interface-This certifies the appliance's identity to a Web browser or to Packet Analyzer. The default Web Interface certificate is a self-signed certificate generated after the first boot of the appliance. Any subsequent boot uses the same certificate. Each appliance has a unique certificate.
- NetProfiler Export-This certifies the appliance's identity to a NetProfiler when using the NetProfiler Export feature. It is a self-signed certificate. The default certificate is the same on all NetShark and NetProfiler appliances.
- Trusted NetProfilers-This certifies the identity of a NetProfiler connecting to this NetShark. By default there are two default Trusted NetProfiler certificates, which allows trusting any NetProfiler using the default certificates.

The SSL Certificate Management page lets you view and replace the certificates. Any changes you make to the configuration are applied after a NetShark Probe service restart.

SSL Certificate Management

Click a tab to choose a certificate.

The screenshot shows the 'SSL Certificate Management' page with three tabs: 'Web Interface', 'NetProfiler Export', and 'Trusted NetProfilers'. The 'Web Interface' tab is selected. Below the tabs is the 'Certificate Details' section, which includes the following information:

- Issued To:** Common Name: shark.lab.nbttech.com, Email: [redacted], Organization: Riverbed Technology, Organization Unit: Cascade, Locality: San Francisco, State: California, Country: US
- Issued By:** Common Name: shark.lab.nbttech.com, Email: [redacted], Organization: Riverbed Technology, Organization Unit: Cascade, Locality: San Francisco, State: California, Country: US
- Validity:** Issued On: Sat, 12 Jul 2014 21:39:36 GMT, Expires On: Sun, 12 Jul 2015 21:39:36 GMT
- Fingerprint:** Algorithm: SHA1, Value: EB:00:D0:E4:51:D4:BB:03:82:59:93:4B:0D:91:00:0B:84:FC:39:D8
- Key:** Algorithm: RSA, Size: 2048
- PEM:** View PEM

Below the details is the 'Replace Certificate' section with three buttons: 'Import Certificate', 'Generate Certificate', and 'Use NetProfiler Export Certificate'.

Click to view the PEM file for the certificate.

On the Web Interface tab, click to re-use the NetProfiler Export certificate/key pair as the Web Interface certificate/key pair.

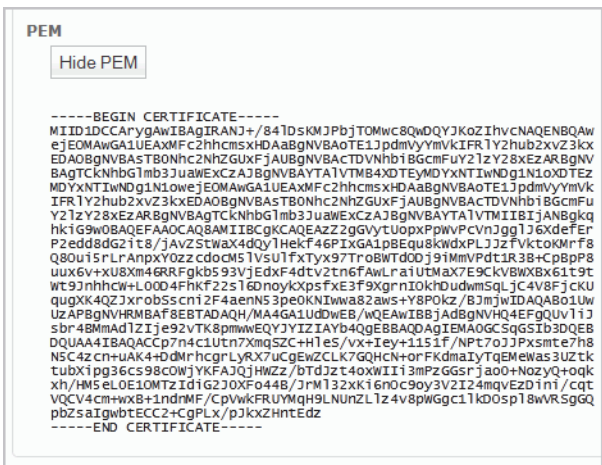
Click to generate a new certificate/key pair.

Click to import an existing certificate/key pair.

On the NetProfiler Export tab, click to re-use the Web Interface certificate/key pair as the NetProfiler Export certificate/key pair.

This close-up shows the 'Replace Certificate' section with three buttons: 'Import Certificate', 'Generate Certificate', and 'Use Web Interface Certificate'. A red arrow points to the 'Use Web Interface Certificate' button.

To view the PEM file for a certificate, click the View PEM button.

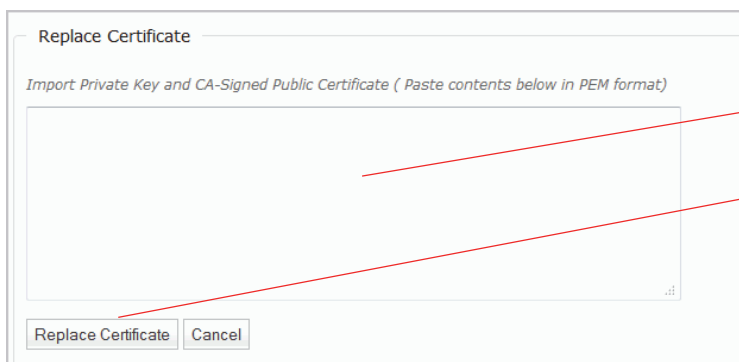


You can import existing certificates that are in PEM format and have either PKCS1 or PKCS8 headers. The general format of these certificates is:

```
-----BEGIN PRIVATE KEY-----
(Base64 encoded data goes here.)
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Base64 encoded data goes here.)
-----END CERTIFICATE-----
```

The two sections can appear in either order. For Web Interface and NetProfiler Export, include both certificate and key. For Trusted NetProfilers, include only the certificate section.

To import an existing certificate, click the Import Certificate button and paste the certificate (and key, if appropriate) in the space provided. Then click the Replace Certificate button.



Paste existing certificate here.

Click when done.

To generate a new certificate/key pair, click the Generate Certificate button and fill in the parameters.

It is important to make sure that the hostname and domain name are properly configured before generating the new certificate, as the new certificate contains hostname.domainname as the Common Name record. The hostname and domain name are specified on the Settings > Basic Settings page. The Certificate Details for each certificate type on the Settings > SSL Certificate Settings page show the Common Name record and other records encoded into the certificate.

Click the Replace Certificate button to generate the new certificate/key pair.

Replace Certificate

Generate New Private Key and Self-Signed Public Certificate

Organization Name:

Organization Unit Name:

Locality:

State:

Country: (two-letter code)

Email Address:

Validity Period: Days (60 to 3650 days)

To use an existing certificate and private key that are stored on the appliance, click the **Use NetProfiler Export Certificate** button (from the Web Interface tab) or **Use Web Interface Certificate** button (from the NetProfiler Export tab). Click the **Replace Certificate** button to accomplish the replacement.

Replace Certificate

Replace NetProfiler Export Certificate with a copy of the Web Interface Certificate.

The default NetProfiler Export certificate for the NetShark appliance is the default_profiler certificate if the appliance is running version 9.5 or earlier software or if the software is version 9.6 or later but the appliance has never been booted in FIPS mode. Once the appliance has been booted in FIPS mode (in version 9.6 or later software), the default_profiler_fips certificate becomes the default NetProfiler Export certificate; it remains the default NetProfiler Export certificate even if the appliance returns to non-FIPS mode, unless you upload a new certificate or generate a new certificate. FIPS mode is described in the section on “Setting basic appliance parameters” on page 8.

Note that if you replace the default NetProfiler Export certificate with a new one (either by importing a certificate or by generating a new one), you need to add that new certificate to the trusted certificates in any NetProfiler to which you will be exporting data. If you change the certificate on the NetShark but not on a NetProfiler, the NetShark will no longer be able to export data to that NetProfiler.

There are two default certificates under the Trusted Profilers tab: default_profiler and default_profiler_fips. These allow trusting NetProfiler appliances connecting to the NetShark. Buttons on the Trusted NetProfilers tab allow you to view or remove these certificates, or to add new certificates.

SSL Certificate Management

Web Interface | NetProfiler Export | Trusted NetProfilers

Existing Certificates

| | | |
|---------------------------------------|-------------------------------------|-----------------------|
| <input type="button" value="Remove"/> | <input type="button" value="View"/> | default_profiler_fips |
| <input type="button" value="Remove"/> | <input type="button" value="View"/> | default_profiler |

Add Certificate

Managing the appliance: SNMP and Notifications

Enabling SNMP management

From the NetShark Web interface go to Settings > SNMP Settings. The NetShark can act as a Simple Network Management Protocol (SNMP) agent, allowing you to access some management information using an SNMP client. The appliance supports the v1, v2c, and v3 versions of the SNMP protocol. The agent allows polling and exports some standard MIBs. For information on available SNMP traps, see “Setting up notifications.”

Check the Enable SNMP box to enable the SNMP agent. Next, choose an SNMP version and fill in the Location, Description, and Contact parameters. If you use v1 or v2c, you can leave the Community string at its default value of “public”; for more security, you can choose a different value.

SNMP Settings

The screenshot shows the 'SNMP Settings' page in the NetShark web interface. It is divided into two sections: 'Common Settings' and 'SNMPv3 Settings'. Red lines and text annotations point to specific elements:

- Common Settings:**
 - Enable SNMP**: Check the box to enable SNMP operation.
 - Downloads:**
 - [RBT-MIB](#): Click a link to view MIB; right-click to save a copy locally.
 - [SHARK-MIB](#): Click a link to view MIB; right-click to save a copy locally.
 - SNMP Version:**
 - SNMPv1
 - SNMPv2c**: Select a protocol version.
 - SNMPv3
 - Location:** : Fill in parameters.
 - Description:** : Fill in parameters.
 - Contact:** : Fill in parameters.
 - Community:** : Change the default Community string.
- SNMPv3 Settings:**
 - Username:**
 - Security Level:**
 - Authentication Passphrase:**
 - Authentication Protocol:**
 - Privacy Passphrase:**
 - Privacy Protocol:**
 - Note: Authentication and privacy passphrases must be at least 8 characters long.*
- Apply**: Click **Apply** to save changes.

NetShark 10.5 introduced custom metrics specific for NetShark:

- Job configuration and status
- Flow export configuration and statistics
- Packet storage hardware status

You can read or download the two MIB description files. The RBT-MIB is a MIB common to many Riverbed products. You need not download it if you already have a copy. The SHARK-MIB is the MIB for NetShark appliances. Both MIB files are needed by a MIB browser. Right-click a MIB and save the file locally to enable OID/field-name mapping on your SNMP client.

SNMP v3 does not use a Community string, but offers additional parameters for more security. There are three levels of security for SNMP v3; as you increase the security level, you specify additional passphrases and protocols, as follows:

Tasks

- **Username**—SNMP security name that the application attempting to browse the MIB must use.
- **Security level**—Choose among:
 - **No Authentication/No Privacy**—SNMP transactions are not authenticated and the SNMP traffic is transmitted in plain text.
 - **Authentication/No Privacy**—SNMP transactions are authenticated and the SNMP traffic is transmitted in plain text.
 - **Authentication/Privacy**—SNMP transactions are authenticated and encrypted.
- **Authentication passphrase**—password associated with the username. It must be at least 8 characters long.
- **Authentication protocol**—algorithm used by the authentication protocol. This can be MD5 or SHA.
- **Privacy passphrase**—string used to encrypt SNMP data exchanges. It must be at least 8 characters long.
- **Privacy protocol**—algorithm used to encrypt the SNMP data exchanges. This can be DES or AES.

Note: Certain SNMP configurations are modified when the appliance is switched into FIPS mode (set FIPS mode in “Security Configuration” at Settings > Basic Settings).

SNMP Settings

Common Settings

Enable SNMP

Downloads

- [RBT-MIB](#)
- [SHARK-MIB](#)

SNMP Version: SNMPv1 SNMPv2c SNMPv3

Location:

Description:

Contact:

Community:

SNMPv3 Settings

Username:

Security Level:

Authentication Passphrase:

Authentication Protocol:

Privacy Passphrase:

Privacy Protocol:

Note: Authentication and privacy passphrases must be at least 8 characters long.

Security levels: No authentication or privacy Authentication, but no privacy Both authentication and privacy

Setting up notifications

You can configure the NetShark to alert you by email or SNMP trap when certain events occur. Alert notifications are delivered to recipients. A recipient is one email address and/or one or more trap receiver addresses.

In the Settings > Notification Settings page, start by selecting how the alerts are sent to recipients: email, SNMP trap, or both.

NetShark can alert you when the following events occur:

- Notify every time the system clock is modified.
Some errors might occur when a time synchronization protocol modifies the clock. A notification is sent.
- Notify whenever the up/down state of a link changes.
A notification is sent when a network or management port changes state.
- Notify every time this NetShark is rebooted.
A notification is sent every time the NetShark reboots, normally or unexpectedly.
- Notify whenever there is a disk pressure event.
When the amount of space available in system storage is getting low and views might be closed, a notification is sent.
- Notify whenever there is a job status change.
For example, a notification is sent when a new job is started.
- Notify whenever there is a memory pressure event.
When running out of memory and views might be closed, a notification is sent.
- Notify whenever there is an SSL key added.
- Notify whenever there is an SSL key edited.
- Notify whenever there is an SSL key removed.
- Notify whenever a view uses an SSL key to decrypt traffic.
A notification is sent the first time a view uses an SSL key. If a second view uses the key, another notification is sent. Each notification includes the title of the view that used the key.
- Notify whenever there is a view killed.
When a large amount of disk space or memory is being used, a NetShark will close views to free up some disk space or memory. Should this occur, this notification is sent.
- Notify whenever there is a watch event.
You can use Packet Analyzer to set up watches on views that trigger events and notifications. A notification is sent when a watch triggers an event.
- Notify whenever there is a change in the storage status.
A notification is sent every time something goes wrong with the packet storage. The notification will include further details about what disk/s are experiencing problems.

Adding Email Notifications

Notification Settings

The screenshot shows the 'Notification Settings' page in NetShark. It is divided into three main sections: 'Recipient', 'Notifications', and 'Email Settings'. The 'Recipient' section has two radio buttons: 'Email' (checked) and 'SNMP trap'. The 'Notifications' section contains a table of events with checkboxes. The 'Email Settings' section has input fields for SMTP Server Address, SMTP Server Port (25), To Address, and From Address, along with a 'Test Email Settings' button. An 'Apply' button is at the bottom. Red lines and text boxes provide instructions: 'Select method of event notification delivery.' points to the 'Email' radio button; 'Select events for notification.' points to the list of events; 'Enter Email parameters.' points to the SMTP fields; 'Click to test Email configuration.' points to the 'Test Email Settings' button; and 'Click **Apply** to save changes.' points to the 'Apply' button.

Recipient

Email
 SNMP trap

Notifications

| Enabled | Description |
|--------------------------|---|
| <input type="checkbox"/> | Notify every time the system clock is modified |
| <input type="checkbox"/> | Notify whenever the up/down state of a link changes |
| <input type="checkbox"/> | Notify every time this NetShark is rebooted |
| <input type="checkbox"/> | Notify whenever there is a disk pressure event |
| <input type="checkbox"/> | Notify whenever there is a job status change |
| <input type="checkbox"/> | Notify whenever there is a memory pressure event |
| <input type="checkbox"/> | Notify whenever there is an SSL key added |
| <input type="checkbox"/> | Notify whenever there is an SSL key edited |
| <input type="checkbox"/> | Notify whenever there is an SSL key removed |
| <input type="checkbox"/> | Notify whenever a view uses an SSL key to decrypt traffic |
| <input type="checkbox"/> | Notify whenever there is a view killed |
| <input type="checkbox"/> | Notify whenever there is a watch event |
| <input type="checkbox"/> | Notify whenever there is a change in the storage status |

Email Settings

SMTP Server Address:

SMTP Server Port:

To Address:

From Address:

You can test the configuration by clicking the **Test Email Settings** button; the NetShark will try to send you a test email to verify that the configuration is correct. Click **Apply** to save changes.

Adding SNMP Trap Receivers

Click the SNMP trap tab to add and edit SNMP trap receivers.

The screenshot shows the 'SNMP trap' tab in a configuration interface. It features a list of 'SNMP Trap Recipients' with three entries: 192.168.10.101 (SNMPv1), 192.168.20.202 (SNMPv2c), and 192.168.30.301 (SNMPv3). Each entry has 'Test' and 'Delete' buttons. A red box highlights these three entries, with a line pointing to the text 'Currently configured trap recipients.' Below the list is an 'Add' button, with a line pointing to 'Click to add new trap recipients.' At the bottom left is an 'Apply' button, with a line pointing to 'Click **Apply** to save changes.'

Be sure to click **Apply** to save any revisions or additions you make to SNMP recipients.

Click **Add** to configure a new trap recipient. Choose the SNMP Version used by the recipient. Your choice determines what fields must be entered. Fields that do not apply are grayed out.

The screenshot shows the 'Add Snmp Trap Recipient' dialog box. It is divided into two sections: 'Common Settings' and 'SNMPv3 Settings'. In 'Common Settings', there are radio buttons for 'SNMPv1', 'SNMPv2c', and 'SNMPv3' (which is selected). Below are 'Address:' and 'Community:' text boxes. A red line points from the 'Address:' box to the text 'Enter Hostname or IP address.' In 'SNMPv3 Settings', there are text boxes for 'Username:', 'Engine Id', 'Authentication Passphrase:', and 'Privacy Passphrase:'. There are also dropdown menus for 'Security Level:' (set to 'No Authentication / No Privacy'), 'Authentication Protocol:' (set to 'MD5'), and 'Privacy Protocol:' (set to 'DES'). A red line points from the 'Username:' box to the text 'Alphanumeric string (up to 32 characters).' Another red line points from the 'Engine Id' box to the text 'A hexadecimal string between 5 and 32 characters long.' At the bottom, there are 'Save', 'Delete', and 'Cancel' buttons. A red line points from the 'Save' button to the text 'Click **Save** to return to SNMP trap tab. On that page you click **Apply** to save the new recipient.'

Every SNMPv3 Agent has an engine ID that uniquely identifies the agent in an administrative domain. The engine ID is used by the authentication and privacy algorithms when communicating with a client. Check with your network management team for an SNMPv3 trap receiver's engine id.

Clicking Save returns you to the SNMP trap tab. You can now:

- Click Add to enter more trap recipients.
- Click an existing trap recipient's IP address to edit it.
- Click Test to test the parameters of a specific trap recipient by sending it a test trap.
- Click Delete to remove a trap recipient.

You must save any change (new, revised, or deleted trap recipients) by clicking **Apply**. If you navigate away from this page before clicking **Apply**, your changes are lost. After clicking **Apply**, a message appears at the top of the page, confirming that your settings have been updated.

Using Traps with SNMPv3

You can set the security level used for traps sent to SNMPv3 recipients using the Security Level setting. Your choices are:

- No authentication/No Privacy
- Authentication/No Privacy
- Authentication/Privacy

If you choose Authentication, you must enter a passphrase of eight characters or more and select an authentication protocol (MD5 or SHA1). If you choose Privacy, you must enter a passphrase of eight characters or more and select a privacy protocol (AES or DES).

Note: If you enable FIPS 140-2 Compatible Cryptography (in Security Configuration at Settings > Basic Settings) some settings may change.

Using the Packet Analyzer Concurrent License server

In addition to purchasing licenses for features and capacities on a NetShark, you can purchase a license pack for multiple SteelCentral Packet Analyzer instances. This is activated from the Riverbed licensing Web site the same as NetShark licenses. Once it is added to the NetShark, you can license Packet Analyzer instances by configuring the Packet Analyzer to obtain a concurrent license from the NetShark.

This is useful for situations where operators on different shifts may all be using Packet Analyzer at different times. Instead of buying enough licenses for each person to have their own, you might prefer to purchase only enough licenses to cover the largest number of concurrent Packet Analyzer users you anticipate. These serve as a license pool that users can draw from as needed.

Packet Analyzer licenses expire 48 to 72 hours after they are issued. The expiration time is based on UTC and therefore the actual number of hours depends on the time zones of the Packet Analyzer and NetShark. They are automatically renewed if the Packet Analyzer is connected to a NetShark that has Packet Analyzer licenses available.

When you install a license for multiple Packet Analyzer instances, the System > Licenses page adds the number of licenses in the Packet Analyzer Concurrent Licenses section at the bottom. This section lists the total number of Packet Analyzer licenses available and the number currently in use for each concurrent license.

Licenses

Current Licensed Feature Set

| Feature | Licensed Value |
|--------------------------------|----------------|
| NetProfiler Export: | Enabled |
| NetProfiler Export Flow Limit: | 50 K |
| Packet Storage Size Limit: | 2000 GB |

License Updates

Updates successfully retrieved last time on 12/11/2014 10:09:13 Fetch Updates now

Enable Automatic License Download from Riverbed

Valid Licenses

| | License Key | Status | Description | Start Date | End Date |
|---|--|--------------|--|------------|----------|
| Delete | LK1-VBASE#V96VX0000E6F1-0000-0000-1-523D-F0BB-9149 | VALID | NetShark Virtual Edition Base | -- | -- |
| Delete | LK1-SHKDSK2000-0000-0000-1-E7C7-4FAA-2FC7 | VALID | Packet Storage Disk 2TB | -- | -- |
| Delete | LK1-SHKPROFLR2-0000-0000-1-8577-4A29-409B | VALID | NetProfiler Export 2 destinations | -- | -- |
| Delete | LK1-SHKEXPCAP50-0000-0000-1-8E21-D9C6-CD74 | VALID | NetProfiler Export Capacity 50K flows | -- | -- |
| Delete | LK1-CPEL#10+00000000-0000-0000-1-0668-39DA-EF16 | VALID | Concurrent license for Packet Analyzer | -- | -- |

Add New Licenses

Packet Analyzer Concurrent Licenses

Total: **16** Available: **16** In use: **0**

License Request

Enter a valid license token, which you should have obtained from Riverbed.

License request token:

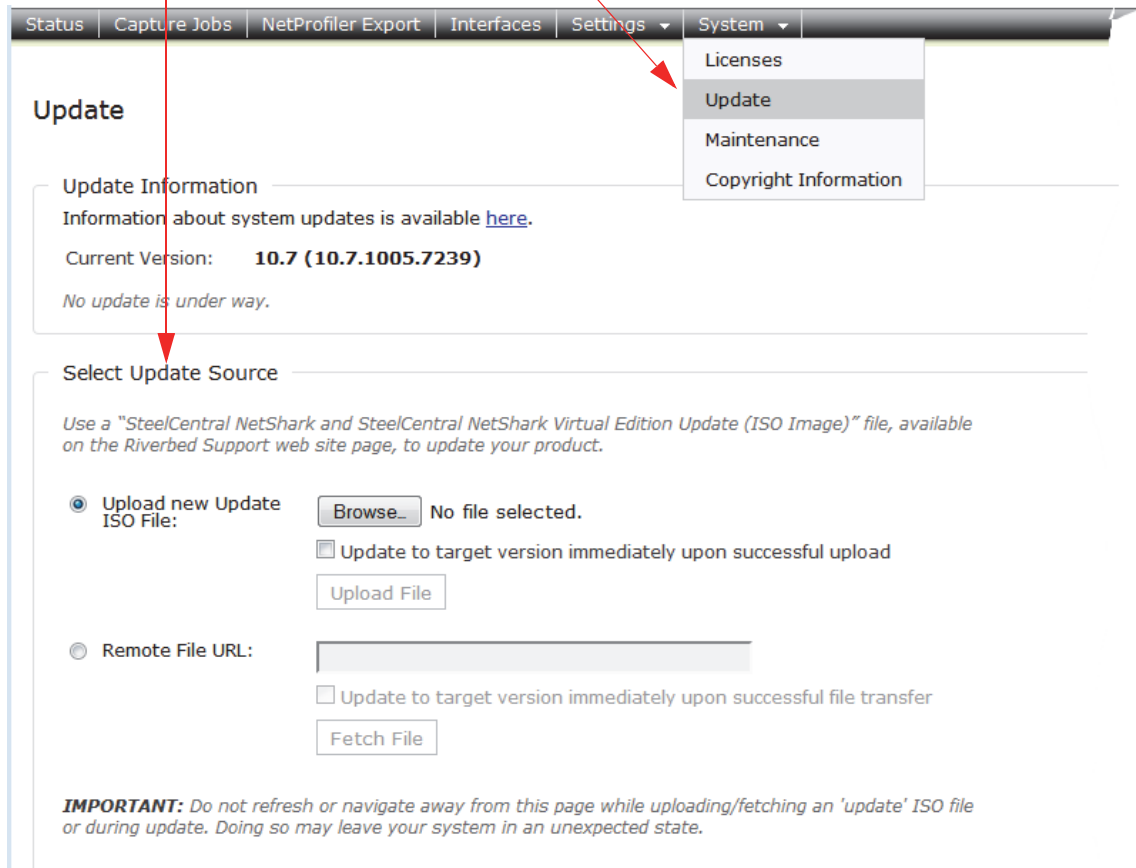
Generate License Request Key

Updating system software

From time to time, Riverbed may make software updates available for the appliance. You can install these updates by uploading an update ISO file that is saved on the local system or by fetching the update ISO file from the Riverbed Support site. Use the screen shown below:

1) Click System > Update to open the Update page.

2) Specify the update source and perform the update.



Update

Update Information
Information about system updates is available [here](#).

Current Version: **10.7 (10.7.1005.7239)**

No update is under way.

Select Update Source

Use a "SteelCentral NetShark and SteelCentral NetShark Virtual Edition Update (ISO Image)" file, available on the Riverbed Support web site page, to update your product.

Upload new Update ISO File: No file selected.

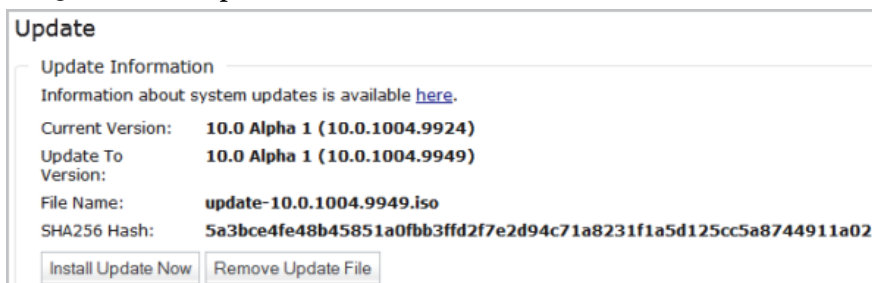
Update to target version immediately upon successful upload

Remote File URL:

Update to target version immediately upon successful file transfer

IMPORTANT: Do not refresh or navigate away from this page while uploading/fetching an 'update' ISO file or during update. Doing so may leave your system in an unexpected state.

If you check the “Update to target version immediately...” box, the update is performed as soon as the update file has been transferred to the NetShark. Otherwise the file is saved on the appliance and you perform the update manually by clicking the **Install Update Now** button.



Update

Update Information
Information about system updates is available [here](#).

Current Version: **10.0 Alpha 1 (10.0.1004.9924)**

Update To Version: **10.0 Alpha 1 (10.0.1004.9949)**

File Name: **update-10.0.1004.9949.iso**

SHA256 Hash: **5a3bce4fe48b45851a0fbb3ffd2f7e2d94c71a8231f1a5d125cc5a8744911a02**

See Appendix B for instructions on installing NetShark software on an appliance using a USB memory stick.

Performing maintenance functions

Click System > Maintenance to bring up the Maintenance screen.

Status | Capture Jobs | NetProfiler Export | Interfaces | Settings | System

Maintenance

System Info

SteelCentral NetShark Version: **10.8 (10.8.1005.8757)**

REST API Version: **5.3**

Serial Number: **K91KY00000000**

Log Download

Current
(Includes current NetShark Probe and NetShark Packet Recorder logs.)

NetShark Probe
(Includes all NetShark Probe logs.)

Select Log: **Packet Recorder**
(Includes all NetShark Packet Recorder logs.)

Complete
(Includes all NetShark Probe logs and all NetShark Packet Recorder logs.)

Case ID:

Storage Status

System Storage Status: **OK**

Packet Storage Status: **OK**


Packet Storage RAID level: **0**

Packet Storage Total Space: **3.63 TB**

Packet Storage Available Space: **2.54 TB**

Packet Storage Used Space: **1.08 TB**

Model: CSK-01100 Serial: K91KY00000000 Status: **OK**



New Reserved Space: %

Write speed tends to be slower at the end of hard drives. By setting the 'New Reserved Space' parameter, you can prevent the appliance from writing at the end of packet storage. This will reduce the available storage size, but it will make disk write performance more uniform.

Important: *Reinitializing or reformatting packet storage will cause all packets in the capture jobs to be lost.*

System Halt

From this screen you can perform the tasks listed below.

Gathering system information

The System Info section of the screen presents version information that will be useful when troubleshooting with the assistance of Riverbed Support.

Downloading logs

This section allows you to download various system logs to your local system. It is normally used under the direction of Riverbed Support. There is also a field where you can enter a support case number. If you have opened a support case with Riverbed Support, entering a case number here causes the case number to be inserted into the file name of downloaded archive files.

Note: Starting with Release 10.8.0 core dumps for the two main services, Shark Probe and Packet Recorder can be forced using the NetShark CLI. The generated core dumps are automatically gzipped and can be uploaded to Riverbed or a 3rd party FTP/SFTP server. See the `service <service> coredump <operation>` commands in “CLI Commands” in the Reference chapter for more information.

Viewing storage status

The Storage Status section of the UI screen shows aggregate status information for system storage and packet storage. It also displays status information for each individual disk drive, by drive number.

If you hover the cursor over one of the drives, you will see a tooltip that gives the size, type, model number, and serial number for that drive:



System storage status

NetShark system storage uses RAID technology to provide redundancy. The NetShark 2170 system storage uses RAID 1. The NetShark 4170 and 6170 system storage use RAID 10.

- **OK**—All disks are working properly.
- **FAILING**—At least one disk is about to fail and all the others are OK or REBUILDING.
- **DEGRADED**—While some disks have failed, the array is still working but the failed disks need to be replaced.
- **REBUILDING**—A failed disk was replaced and parity is being rebuilt. If a disk is being rebuilt and another one is failing, the overall status will be FAILING. If at least one drive is FAILED the overall status is DEGRADED.

Packet storage status

NetShark packet storage uses RAID technology to provide redundancy. By default the packet storage uses RAID 0. The NetShark CLI can be used to switch from RAID 0 to RAID 5 or RAID 6 (or back to RAID 0). A 6170 uses up to 8 storage units for packet storage. Disk redundancy is per storage unit. When using RAID 5 one disk can fail in each storage unit; when using RAID 6 two disks can fail in each storage unit.

- **OK**—All disks or all disks across the storage units re working properly.
- **FAILING**—At least one drive is about to fail and all the others are OK or REBUILDING.
- **INOPERABLE**—At least one drive has failed (RAID 0) or has been moved, or the packet recorder is down; the RAID array is malfunctioning or not even there, even if all of the disks are OK. For RAID 5 or 6 it means that too many drives have failed in a 4170 or a 6170 storage unit and the array can no longer be restored.
- **DEGRADED**—(for RAID 5 or 6 arrays) While some disks have failed, the array is still working but the failed disks need to be replaced.
- **REBUILDING**—(for RAID 5 or 6 arrays) A failed drive was replaced and parity is being rebuilt or Packet Storage was switched to RAID 5 or 6. If a disk is being rebuilt and another one is failing, the overall status will be FAILING. If at least one drive is FAILED the overall status will be INOPERABLE or DEGRADED, depending on the RAID level being used.
- **INITIALIZING**—Packet Storage is undergoing a reinitialization.
- **CORRUPTED**—Internal file system is damaged.

Status for an individual disk drive

- **OK**—The drive is working properly.
- **FAILING**—The drive is still working, but will probably fail soon.
- **FAILED**—The disk is either missing or failed (the system cannot detect it).
- **NEW**—The disk has been replaced and it is working (RAID 0).
- **INCOMPATIBLE**—A disk of the wrong size or connectivity has been inserted.
- **MOVED**—A disk has been replaced by one that was previously sitting in a different slot (RAID 0).
- **REBUILDING**—The disk is part of a RAID 5 or 6 array and is currently being rebuilt.

Note: The amber Fault LED on a disk drive blinks while a disk is being rebuilt.

Status for a NetShark 6170 storage unit

- **OK**—All drives are working properly.
- **NEW**—The storage unit is not the one expected (another storage unit was previously enrolled).
- **FAILED**—The storage unit has already been enrolled but it is not reachable (either offline or failed).
- **UNCONFIGURED**—The storage unit has been detected but not has not been previously enrolled.

For more information on storage units, see “Configuring and managing 6170 storage units.”

Reinitializing and reformatting packet storage

Reinitializing or reformatting packet storage destroys all data on the packet storage system. If you are uncertain about performing either action, contact Riverbed Support for assistance.

Clicking the **Reinitialize Packet Storage** button performs a low-level format of the packet storage subsystem. Capture job configurations are retained. The existing packet storage RAID level also is restored. This format takes a considerable amount of time and destroys all data on the system. It ignores the **Reserved Space** setting (see below) and formats the entire packet storage system. It is typically used when a drive fails and is replaced.

Note: Packet storage for a 6170 is reinitialized to the RAID level being used, for example, RAID 5 is reinitialized to RAID 5.

Clicking the **Reformat Packet Storage** button performs a fast, light wipe of the data; it destroys all data on the packet storage system. Capture job configurations are retained however. The **Reformat** option honors the **Reserved Space** setting (see next paragraph). Use reformat to wipe packet data but retain capture job configurations.

The **Reserved Space** parameter is available only on physical NetShark appliances, not on NetShark virtual editions. Setting the **Reserved Space** parameter prevents the use of inner tracks of hard disks that can have slower transfer rates. Setting this value to something other than 0% can in some cases provide more uniform write-to-disk speeds, although it reduces the amount of storage available for packet capture.

Halting and rebooting the system

Clicking **Shutdown SteelCentral NetShark** shuts down the operating system and powers down the appliance. Clicking **Reboot SteelCentral NetShark** shuts down the operating system and then reboots the appliance.

Configuring and managing 6170 storage units

A NetShark 6170 base unit has no internal packet storage. Up to eight external storage units *of the same model* (SCAN-SU-48TB or SCAN-SU-72TB) can be connected to a base unit for packet storage. A base unit runs an enrollment process to identify connected and powered on storage units and then formats packet storage.

- If a base unit has no enrolled storage units, for example, when first installed or after an enroll-reset command has been issued, an automatic enrollment is performed when it is rebooted.
- Enrollment is a global operation, that is, all storage units are enrolled whenever an enrollment occurs.
- An individual storage unit cannot be enrolled separately.
- Enrollment fails
 - if there is a mix of storage unit models attached to the base unit
 - if an invalid storage unit is detected
 - if a disk fails
 - If an incompatible disk is found
- The enrollment process formats packet storage as RAID 0 storage by default. After enrollment, packet storage can be reinitialized as RAID 5 or RAID 6 for packet storage redundancy, using the NetShark CLI.

If a storage unit fails or is removed, packet storage is inoperable.

Note: Enrollment, reinitialization and reformatting destroy all existing captured packet data.

NetShark CLI Packet Storage and Service commands

- `packet-storage status`—displays packet storage status and details
- `packet-storage reinitialize raid[0 | 5 | 6]`—changes packet storage RAID level
- `storage-unit rescan`—restores a storage unit that has lost its connection to the base unit
- `storage-unit enroll-reset`—removes all previous storage unit enrollments; must be followed by a `storage-unit enroll-force` command or a NetShark reboot.
- `storage-unit enroll-force`—starts an enrollment procedure; all storage units are enrolled and all packet storage data is lost

NetShark Web interface storage information and management

- On the Status page view the following detailed system information:
 - User Data Storage status and use
 - Packet Storage status and use
 - Memory status and use

Tasks

- On the System > Maintenance page view the following system and packet storage information:
 - System and Packet Storage status
 - Packet Storage RAID level
 - Packet Storage total space and use
 - Detailed information on and status of:
 - o Each NetShark model
 - o Each storage unit
 - o Each disk drive
- On the System > Maintenance page the following storage maintenance actions are available:
 - **Reinitialize Packet Storage**—Used when packet storage has failed; all packet storage data is lost. Capture job configurations are preserved and the existing RAID level is recreated.
 - **Reformat Packet Storage**—Used for a fast, light wipe of packet storage data; reserved space and capture job settings are preserved.

Enrolling storage units

When a base unit powers on, if there are no enrolled storage units or after an enroll-reset command is issued, it detects connected and powered up storage units. It then automatically enrolls the identified storage units and formats them for packet storage. Each storage unit's identity is stored by the base unit and the storage units are formatted as RAID 0 packet storage.

If other storage units are connected and powered on after this enrollment, they are not used for packet storage and their status is UNCONFIGURED. To include unconfigured storage units in packet storage a new enrollment must be started from the NetShark CLI. This new enrollment deletes all packet data in packet storage.

For NetShark installation instructions and troubleshooting see the *NetShark Quick Start Guide, Models xx70* available on the Riverbed Support site.

Adding storage units to packet storage

- 1) Connect one or more storage units to the base unit configuration using the supplied 1 M SAS cables.
 - a) Connect the cable to Port A in slot 4 of the new storage unit. Connect the other end to Port B in slot 4 on the last storage unit in the existing single linear daisy chain of storage units. Repeat as necessary.
- 2) Power on the storage units.
- 3) Open the NetShark Web interface and check the status of the storage units on the System > Maintenance page. The status should be UNCONFIGURED. If not, the unit is not successfully connected to the base unit.
- 4) Using a terminal emulator such as PuTTY or Tera Term, SSH to the NetShark CLI.
- 5) Enter `storage-unit enroll-reset` to clear all references to any previously enrolled storage units.

- 6) Enter `storage-unit enroll-force`. All existing packet data is lost when the new enrollment occurs.

Changing the packet storage RAID level

By default packet storage is formatted as RAID 0 when storage units are enrolled by a 6170 base unit. For redundancy packet storage can be reformatted to RAID 5 or RAID 6 using the NetShark CLI.

When changing the format of packet storage:

- All existing packet data is lost.
- Changing packet storage to RAID 5 or RAID 6 starts a background rebuilding process that can take several hours. While packet storage is available within seconds, storage performance is degraded, particularly by concurrent packet write-to-disk operations, until rebuilding is complete.
- Packet storage is available immediately when changing the RAID level back to RAID 0.

Note: The amber Fault LED on a hard disk drive blinks while a hard disk is being rebuilt.

Changing packet storage to RAID 5 or RAID 6

Follow the steps below.

- 1) Using a terminal emulator such as PuTTY or Tera Term, SSH to the NetShark CLI.
- 2) Enter `packet-storage reinitialize <raid5|raid6>`
- 3) Packet storage is available within seconds; packet storage status on the System > Maintenance page is REBUILDING until it completes.

When the packet storage is reinitialized in RAID 5 or RAID 6, the rebuild process starts after a few minutes. The status is shown as OK until the rebuilding starts.

Changing packet storage to RAID 0

Follow the steps below.

- 1) Using a terminal emulator such as PuTTY or Tera Term, SSH to the NetShark CLI.
- 2) Enter `packet-storage reinitialize raid0`
- 3) Packet storage is available immediately.

Packet storage status on the System > Maintenance page is OK.


Maintaining a Storage Unit

Periodically NetShark automatically tests storage unit disk drives and reports their status on the NetShark Web interface System > Maintenance page. The example Storage Status below shows a base unit and two storage units formatted as RAID 0 packet storage. All storage units and disk drives show an OK status.


Storage Status

System Storage Status: **OK**
 Packet Storage Status: **OK**
 Packet Storage RAID level: **0**
 Packet Storage Total Space: **87.31 TB**
 Packet Storage Available Space: **74.47 TB**
 Packet Storage Used Space: **12.83 TB**


Model: SCAN-06170 Serial: LD5KY00000000 Status: OK



Model: SCAN-SU-48TB Serial: LD84000 Status: OK



Model: SCAN-SU-48TB Serial: LD84001 Status: OK



New Reserved Space: %

Write speed tends to be slower at the end of hard drives. By setting the 'New Reserved Space' parameter, you can prevent the appliance from writing at the end of packet storage. This will reduce the available storage size, but it will make disk write performance more uniform.

Important: Reinitializing or reformatting packet storage will cause all packets in the capture jobs to be lost.

When a disk is failing or fails its status changes in the Storage Status information. The Fault LED on the disk drive is On. If enabled, a notification also is sent or logged, reporting a change in storage status.

The action needed to recover from a failed disk drive is determined by the format of the packet storage. For a NetShark 6170, this table applies on a per storage unit basis. The formats and recovery action to be taken are summarized in the table below.

Table 2

| Packet Storage Format | No. of Failed Disks | Packet Data Status | Packet Storage Status | Recovery Action |
|-----------------------|---------------------|--------------------|-----------------------|---|
| RAID 0 | 1 | Lost | INOPERABLE | 1. Replace failed disks. 2. Click Reinitialize Packet Storage . |
| RAID 5 | 1 | No Change | DEGRADED | Replace failed disk. |
| | 2 or more | Lost | INOPERABLE | 1. Replace failed disks. 2. Click Reinitialize Packet Storage . |
| RAID 6 | 1 or 2 | No Change | DEGRADED | Replace failed disks. |
| | 3 or more | Lost | INOPERABLE | 1. Replace failed disks. 2. Click Reinitialize Packet Storage . |

Reinitializing packet storage

To reinitialize packet storage:

- 1) Open the NetShark Web interface to the System > Maintenance page.
- 2) Replace all failed disk drives. The mounting process takes about a minute to complete.
- 3) Click **Reinitialize Packet Storage**. For RAID 0, packet storage is immediately available. For RAID 5 or 6, packet storage is available within seconds, but storage performance is degraded until rebuilding is complete.

Note: When packet storage is reinitialized the previous RAID level is used. For example, when an INOPERABLE RAID 5 packet storage is reinitialized, the new packet storage is RAID 5.

Replacing a failed system storage hard disk drive

To replace a System Storage disk drive:

- 1) Open the NetShark Web interface to the System > Maintenance page.
- 2) Replace all failed disk drives. The mounting process takes about a minute to complete.
- 3) REBUILDING starts automatically within a few seconds.

Replacing a base unit or a storage unit

The replacement or reinstallation of a base or storage unit requires a new enrollment process. All packet storage data is lost when a new base unit enrolls existing storage units. See “Enrolling storage units” for installation instructions.

A new storage unit (shown as UNCONFIGURED until enrolled) must be enrolled by a base unit. Enrollment is a global process, so existing storage units also are enrolled and existing packet storage data is lost. The packet storage is formatted as RAID 0 by default. See “Adding storage units to packet storage” for installation instructions.

Restoring a storage unit to its base unit

An unplugged cable or a loss of power can result in a storage unit losing its connection with its base unit. For example, a previously enrolled storage unit may have been power cycled or was not connected when the base unit last booted. When the storage unit is connected and powered on its status is FAILED. Packet recording stops and packet storage status is INOPERABLE. A rescan is needed.

The base unit must have enrolled the storage unit(s) previously. If so, a rescan can restore their connection to the base unit and packet recording resumes for active capture jobs.

To restore a previously enrolled storage unit to operation:

- 1) Using a terminal emulator such as PuTTY or Tera Term, SSH to the NetShark CLI.
- 2) Enter **storage-unit rescan**

Following a successful rescan, the storage unit is again available and packet recording resumes. The status of the storage unit and packet storage is OK.

Advanced Configuration Settings

These are the paths to the settings discussed in the following topics:

The screenshot shows the SteelCentral NetShark interface with the 'Settings' menu open. The 'Advanced Settings' option is highlighted at the bottom of the menu. Red arrows point from the 'Advanced Settings' menu item to the 'Advanced Settings' text in the 'System Information' section of the main interface.

| Job | Status | Packet |
|-------------------------|----------------|-------------|
| Traffic Monitor #518130 | RUNNING | 4.91 |

| User Data Storage | | Packet |
|--------------------|--------------------------|---------|
| Status: | OK | Status |
| Total: | 425.94 GB | Total |
| Used: | 270.10 MB (0.06%) | Used |
| Allocated (Index): | 11.16 GB (2.76%) | Allocat |

Updating Predefined Port and Port Group Definitions

The default port and port group definitions listed below are used in some views. Deleting or renaming these definitions can result in unreliable results when the views are applied. These definitions can be added to or revised to match your network. For example, if you also use a nonstandard port to carry SIP traffic in your network, you can add that port to the `sip` port name in the port definitions. Or, if none of your SIP traffic runs on the default port, you can replace the default port with the port that you do use. This ensures that views will reliably report the SIP traffic on your network.

Table 3

| Name | Type | Used by |
|-----------------|-----------|--------------|
| cisco-sccp | Port Name | VoIP Views |
| citriximaclient | Port Name | Citrix Views |
| h323hostcall | Port Name | VoIP Views |
| ica | Port Name | Citrix Views |
| microsoft-ds | Port Name | CIFS Views |
| ms-sql-s | Port Name | SQL Views |
| mysql | Port Name | SQL Views |
| netbios-ssn | Port Name | CIFS Views |

Configuring Service Response Time in Port Definitions

For TCP connections carrying request/response application layer protocols, the following additional Service Response Time (SRT) metrics can be captured:

- Request Transfer Time
- Response Transfer Time
- Request Retransmission Delay
- Response Retransmission Delay
- Server Response Time

Web, Email, and SSH are examples of TCP connections with such request/response application layer protocols.

Application layer protocols carried by TCP that do not support these metrics include:

- Pipelining, for example, HTTP pipelining or CIFS
- Two-way communication, for example, H.323, Citrix, or chat applications

Click the Service Response Time box for a new or existing port definition to include the above SRT metric calculations for an application. SRT metrics are automatically included in TCP flows exported to a NetProfiler. These metrics can be viewed in Packet Analyzer using views in the “Advanced Time Metrics” folder, located under “TCP” in the “Performance and Errors” view folder. Note: The Service Response Time setting can be updated when synchronization of Ports, Port Groups and Application Definitions with a NetProfiler is enabled on the “NetProfiler Export” tab of the Web interface.

The following default port definitions have the Service Response Time box checked:

Table 4

| Port Name | TCP Port | Port Name | TCP Port |
|----------------------|----------|-------------|----------|
| ftp-data | 20 | ldaps | 636 |
| ftp | 21 | rsync | 873 |
| smtp | 25 | ftps-data | 989 |
| tftp | 69 | ftps | 990 |
| http | 80 | imaps | 993 |
| pop3 | 110 | pop3s | 995 |
| sftp | 115 | ms-sql-s | 1433 |
| nntp | 119 | ms-sql-m | 1434 |
| epmap | 135 | ncube-lm | 1521 |
| netbios-ns | 137 | pdap-np | 1526 |
| netbios-dgm | 138 | sms-rcinfo | 2701 |
| imap | 143 | sms-xfer | 2702 |
| ldap | 389 | sms-chat | 2703 |
| https | 443 | sms-remctrl | 2704 |
| urd | 465 | mysql | 3306 |
| Ibm-db2 | 523 | postgresql | 5432 |
| Imap4-ssl-deprecated | 585 | http-alt | 8080 |
| submission | 587 | bacula-dir | 9101 |
| ipp | 631 | bacula-fd | 9102 |

Notes:

- a) A NetShark must see both directions of traffic flow on the same physical port (or vNIC on NetShark virtual edition) to calculate and export the metrics to a NetProfiler.
- b) NetProfiler appliance can provide Round Trip Times if it receives both directions of the connection (from two different NetShark interfaces or from two different NetShark appliances).
- c) TCP connection history expires on a NetShark when a long-lived connection is silent for more than five minutes. No SRT metrics are available for that connection.
- d) No SRT metrics are available for optimized connections.

Important: If you include ports with TCP connections that do not use request/response application layer protocols, the reported metrics can be distorted and of little value.

Port definitions

Important: Before making changes to default port and port group definitions, please review “Updating Predefined Port and Port Group Definitions” to avoid causing inaccurate views of your network traffic. Use the Port Definitions page to:

- Add a mapping of a port to a TCP and/or UDP protocol and assign a name.
- Edit or delete an existing port definition.
- Select Service Response Time metric compilation for a port.
- View, sort, and filter existing port definitions.

Port Definitions

| Name | Port ▲ | Protocol | Service Response Time | Delete |
|-------------|--------|----------|-------------------------------------|--------|
| tcpmux | 1 | tcp/udp | <input type="checkbox"/> | ✖ |
| compressnet | 2 | tcp/udp | <input type="checkbox"/> | ✖ |
| compressnet | 3 | tcp/udp | <input type="checkbox"/> | ✖ |
| rje | 5 | tcp/udp | <input type="checkbox"/> | ✖ |
| echo | 7 | tcp/udp | <input type="checkbox"/> | ✖ |
| discard | 9 | tcp/udp | <input type="checkbox"/> | ✖ |
| systat | 11 | tcp/udp | <input type="checkbox"/> | ✖ |
| daytime | 13 | tcp/udp | <input type="checkbox"/> | ✖ |
| qotd | 17 | tcp/udp | <input type="checkbox"/> | ✖ |
| msp | 18 | tcp/udp | <input type="checkbox"/> | ✖ |
| chargen | 19 | tcp/udp | <input type="checkbox"/> | ✖ |
| ftp-data | 20 | tcp/udp | <input checked="" type="checkbox"/> | ✖ |
| ftp | 21 | tcp/udp | <input checked="" type="checkbox"/> | ✖ |
| ssh | 22 | tcp/udp | <input type="checkbox"/> | ✖ |
| telnet | 23 | tcp/udp | <input type="checkbox"/> | ✖ |
| smtp | 25 | tcp/udp | <input checked="" type="checkbox"/> | ✖ |
| nsw-fe | 27 | tcp/udp | <input type="checkbox"/> | ✖ |
| msg-icp | 29 | tcp/udp | <input type="checkbox"/> | ✖ |
| msg-auth | 31 | tcp/udp | <input type="checkbox"/> | ✖ |
| dsp | 33 | tcp/udp | <input type="checkbox"/> | ✖ |

Add Cancel Apply

Modification of port group definitions is disabled when synchronizing their configuration with a NetProfiler. You can continue to search, sort, and filter the definitions.

Adding a port definition

To create a port definition:

- 1) Go to the Settings > Port Definitions page and click the Add button at the bottom of the page. A new row with no name appears at the top of the list (scroll up to the top of the list if you don't see it).
- 2) Enter the name for a port as you want it to appear in views and reports. A name can contain alphanumeric, dot (.), and underscore (_) characters.
- 3) Enter a unique port number. The port number must be between 1 and 65535. If an error is shown for a valid port number, the port definition is a duplicate and not allowed.
- 4) Click in the Protocol column and choose the protocols that the name applies to from the drop-down list.
- 5) Select or deselect the Service Response Time check box to enable or disable the calculation of the service response time metrics for TCP ports.
- 6) Click Update to complete your entry, or Cancel to remove it. Unsaved changes are highlighted with a light-yellow background.
- 7) To enter additional definitions, click the Add button at the bottom of the page.
- 8) Review new and revised definitions that have not yet been saved. Use the Cancel button to remove all changes before saving. Revised definitions require use of the Cancel button to retain the original definition. Click the red "x" in the Delete column to remove a single new definition.
- 9) Click Apply at the bottom of the page to save your changes.

Sorting and filtering definitions

Do the following to sort and filter the list of port definitions:

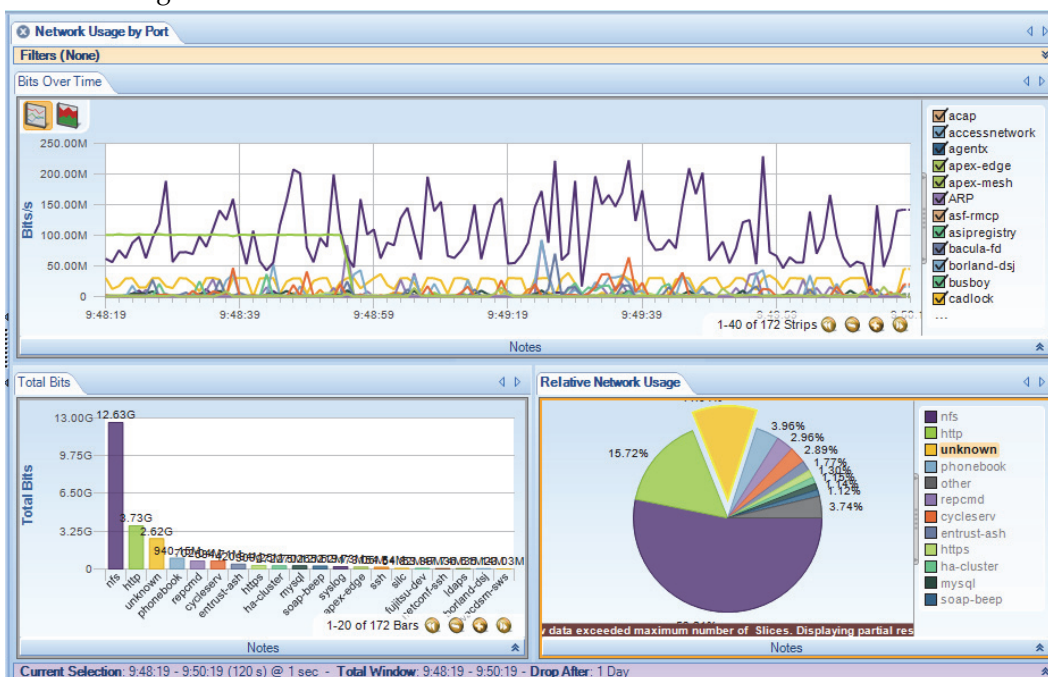
- Hover over the right edge of a column and click the down arrow to select available sort orders or filters from a drop-down menu.
- To search an alphanumeric field, hover over Filters and enter a search term in the field that appears. The check box is automatically checked and the search result is displayed.
- To search a numeric field, hover over Filters and enter a number in the appropriate search type. The check box is automatically checked and the search result is displayed.

Note: Filters and searches can be applied to the results of a previous search or filtering.

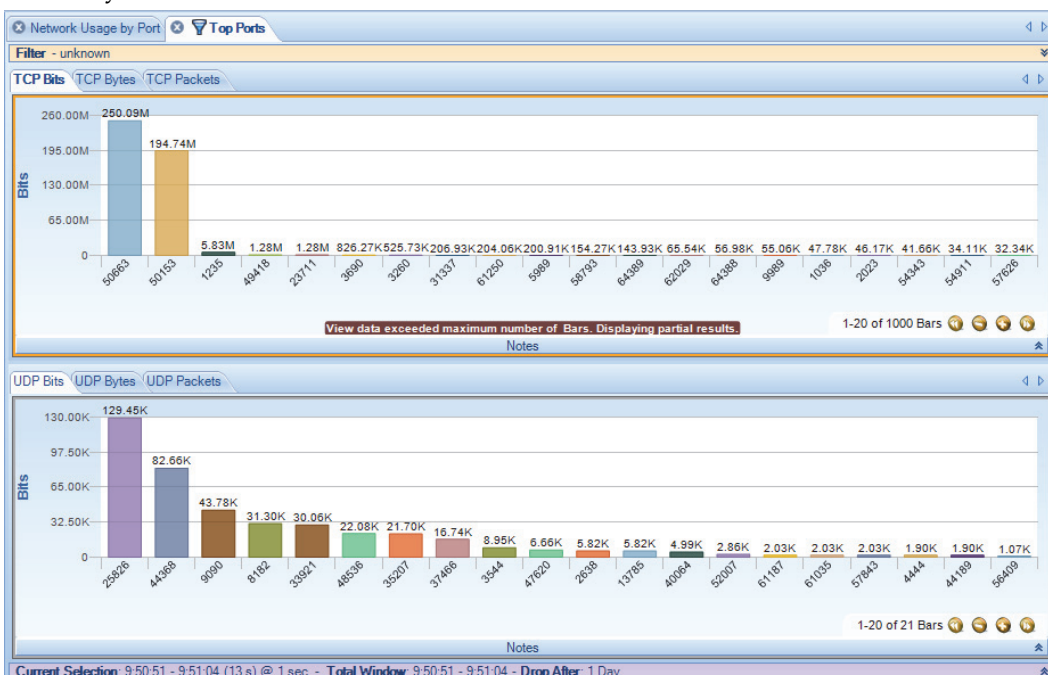
| Name | Port ^ | Protocol | Service Response Time | Delete |
|-------------|--------|----------|--------------------------|-------------------------------------|
| tcpmux | 1 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| compressnet | 2 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| compressnet | 3 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| rje | 5 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| echo | 7 | tcp/udp | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| discard | 9 | tcp/udp | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| systat | 11 | tcp/udp | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| daytime | 13 | tcp/udp | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Identifying unknown ports

The Network Usage by Port view applied to a live interface shows “unknown” ports in the “Relative Network Usage” tab.



Drill down by applying the Talkers and Conversations > Top Ports view to the selected unknown traffic wedge in the Relative Network Usage chart. The new charts identify TCP and UDP ports by traffic volume. This provides a starting point for updating or making additions to your Port Definitions to better identify traffic in your network.



Port group definitions

The NetShark Web interface Settings > Port Group Definitions page enables you to map a number of related ports into categories, such as, Email, or Web, providing a more detailed look at traffic on your network. This page allows you to:

- Define a new category of related TCP and UDP ports.
- Edit existing port group definitions.
- View and filter existing port group definitions.
- Delete existing port group definitions.
- Display or hide columns.

Note: A port may appear in more than one port group definition. Starting with release 10.6 (and later), there is no priority in port group definitions. Packets with a port in multiple port groups are mapped to each port group now, not just one. For example, in a bar chart showing port groups, if a packet uses a port that appears in three port groups, three bars are displayed, not one.

Port Group Definitions

| Name | TCP Ports | UDP Ports | Delete |
|--------------------|--|---|--------|
| Web | 80, 8080, 443, 3128 | 80, 443 | ✗ |
| Email | 25, 109, 110, 174, 209, 220, 465, 587, 995, 143, 585, 9... | 25, 109, 110, 174, 209, 220, 587, 995, 143, 993, 119 | ✗ |
| DataTransfer | 20, 21, 115, 69, 989, 990, 873, 9101, 9102, 9103 | 20, 21, 115, 69, 989, 990, 9101, 9102, 9103 | ✗ |
| SSH_Telnet | 22, 23, 514 | | ✗ |
| MSNetworking | 137, 138, 139, 445, 135, 389, 636, 631, 2701, 2702, 27... | 137, 138, 139, 445, 135, 389, 636, 631, 2701, 2702, 27... | ✗ |
| NetworkManagement | 161, 162 | 161, 162 | ✗ |
| VPN_Tunnel | 1723, 1701, 1194 | 1723, 1701, 1194, 8472 | ✗ |
| RemoteDesktop | 3389, 5800, 5801, 5900-5905, 5631, 5632, 6000-6063, 1... | 3389, 5631, 5632, 6000-6063, 1494, 1604, 4172 | ✗ |
| Voice_Video | 1270, 1503, 5060, 5061, 1718, 1719, 1720, 1731, 1300, ... | 1503, 5060, 5061, 1718, 1719, 1720, 1731, 1300, 1935, ... | ✗ |
| Authentication | 1645, 1646, 49, 65 | 1645, 1646, 49, 65 | ✗ |
| DHCP | 67, 68 | 67, 68 | ✗ |
| DNS | 53 | 53, 5353 | ✗ |
| Database | 3306, 1433, 1434, 66, 1521, 1526, 523, 5432 | 3306, 1433, 1434, 66, 1521, 1526, 523 | ✗ |
| Pilot | 61898, 61899 | | ✗ |
| Routing | 179, 521, 698, 1985 | 179, 520, 521, 698, 1985 | ✗ |
| IM | 194, 1863, 5190, 5191, 5192, 5193, 5222, 5223, 5269, 6... | 194, 5190, 5191, 5192, 5193, 4000, 5010 | ✗ |
| SteelheadRBTProtos | 7744, 7800, 7801, 7810, 7820, 7821, 7830, 7840, 7850, ... | | ✗ |
| P2P | 1214, 2234, 2254, 4661, 4662, 6257, 6346, 6699, 6881, ... | 4665, 4672, 7674 | ✗ |

Note: Modification of port group definitions is disabled when synchronizing with a NetProfiler.

Adding a port group definition

A port can appear in more than one port group definition. A port is mapped to each port group it is a member of.

- 1) Go to the Settings > Port Group Definitions page and click the Add button at the bottom of the page. An empty new row appears at the bottom of the list.
- 2) Enter the name for the port group as you want it to appear in views and reports. A name can contain alphanumeric, dot (.), and underscore (_) characters.

3) Enter the TCP and UDP ports for this definition. A port number must be between 1 and 65535.

A list of comma separated ports and port ranges can be entered, for example, 1718-1720, 1731, 1300, 1310-1325

4) Click Update to complete your entry, or Cancel to remove it. Unsaved changes are highlighted with a light-yellow background.

5) To enter additional definitions, click the Add button at the bottom of the page.

6) Review new and revised definitions that have not yet been saved. Use the Cancel button to remove all changes before saving. Revised definitions require use of the Cancel button to retain the original definition. Click the red "x" in the Delete column to remove a single new definition.

7) Click Apply at the bottom of the page to save your changes.

Filtering definitions

Do the following to filter the list of port group definitions:

Hover over the right edge of a column and click the down arrow to select available sort orders or filters from a drop-down menu.

- Alphanumeric fields can be searched by hovering over Filters and entering a search term in the field that appears. The check box is automatically checked and the filter result is displayed. Uncheck the Filters check box to return to the previous list. Checking the box again repeats the last filter.
- "Columns" allows you to select which columns are displayed. Uncheck a box to hide a column.

Note: Filters can be applied to the results of a previous filter. To return to the original list, all filters must be unchecked.

Port Group Definitions

| Name | TCP Ports | UDP Ports | Delete |
|------|---------------------|-----------|--------|
| Web | 80, 8080, 443, 3128 | | ✘ |

Application definitions

Application definitions examine flows to identify and report application traffic. The following types of application definitions can be made:

- **L4 Mappings** - A user-defined mapping of a specific host or group of hosts using a specific port or group of ports to an application.
- **L7 Fingerprints** - A user-defined mapping of an HTTP request URL or SSL/TLS hostname fingerprint to an application.
- **System Applications** - A read-only predefined list of applications that are identified by SteelCentral NetShark and SteelHead.

Deploying a consistent set of definitions for ports, port groups, and applications across Riverbed products ensures uniform reporting and analysis of your network traffic. When synchronization is enabled on a NetShark, a NetProfiler that receives exports from a NetShark can share its definitions. Synchronization replaces the definitions on a NetShark with those on the NetProfiler, enabling a NetProfiler to manage and maintain a master list of ports, port groups, and application definitions. See “NetProfiler Export” for information on how to configure NetProfiler synchronization.

L4 Mappings

Application traffic can be identified by the IP addresses of the hosts where an application runs and the ports that an application uses. Using this information you can assign a name to this traffic using an L4 mapping. Traffic on any host or group of hosts specified in the Hosts field is classified as belonging to an application if it uses any port or group of ports specified in the TCP Ports or the UDP Ports fields in a mapping. The name identifies this traffic in Views and reports. NetProfiler also uses the name when reporting that application traffic.

For example, suppose there are two hosts in your network running the same application but using two different ports. You can create multiple mappings for the same application name, one identifying application traffic coming from the first host and port and the other mapping identifying the second host and port.

Table 5 Layer 4 Mapping Example

| Example Mapping #1 | Example Mapping #2 |
|---------------------|---------------------|
| Name: My App | Name: My App |
| Hosts: 172.16.0.100 | Hosts: 172.16.0.120 |
| TCP Ports: 40430 | TCP Ports: 40440 |

The above mappings identify the application traffic with only particular host-port combinations (i.e., not 172.16.0.100 on TCP port 40440). You can also specify a list of hosts using any of a list of ports as one mapping and a second list of hosts using any of a second list of ports as another mapping.

Note: Hosts and ports can appear in more than one L4 mapping. In this case, priority is based on the position of the mapping in the L4 Mappings list. The mapping closest to the top of the list has the highest priority. In addition, priority can be given to an L4 mapping over Layer 7 Signatures and System Applications by selecting Override in the mapping. When Override is selected, the L4 mapping is evaluated before Layer 7 Signatures, System Applications and other L4 mappings. When Override is not selected, an L4 mapping's priority is determined by its position in the L4 Mappings list.

Application Definitions

| L4 Mappings | | L7 Fingerprints | System Applications | | | |
|-------------|-----------------|---|------------------------|--------------------------------------|--------------------------|-------------------------------------|
| Priority | Name | Hosts | TCP Ports | UDP Ports | Override | Delete |
| 1 | CIFS | 0.0.0.0/0 | 139, 445 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2 | FTP | 0.0.0.0/0 | 20-21 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3 | H.323 | 0.0.0.0/0 | 1718-1720, 1300, 11720 | 1718-1720, 2517, 1300 | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 4 | HTTP | 0.0.0.0/0 | 80 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 5 | LotusNotes | 0.0.0.0/0 | 1352 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 6 | MSExchange | 0.0.0.0/0 | 7830 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 7 | MSSQL | 0.0.0.0/0 | 1433 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 8 | NFS | 0.0.0.0/0 | 2049 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 9 | OracleInitiator | 0.0.0.0/0 | 9000 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 10 | SIP | 0.0.0.0/0 | 5060-5061 | 5060 | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 11 | SSL | 0.0.0.0/0 | 443 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 12 | Skinny | 0.0.0.0/0 | 2000 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 13 | SnapMirror | 0.0.0.0/0 | 10565-10569 | | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 14 | LSE_ITCH | 224.4.0.0/22, 224.4.4.0/23, 224.4.6.0/24, 224.4.10.0/2... | | 60000, 60300, 60400, 61000, 61100... | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Add Cancel Apply

Adding an L4 Mapping

To add an L4 application mapping, do the following:

- 1) Go to the Settings > Application Definitions page and click the L4 Mappings tab.
- 2) Click the Add button at the bottom of the page. An empty new row appears at the bottom of the list.
- 3) Enter the name for the application as you want it to appear in views and reports. A name can contain alphanumeric, dot (.), and underscore (_) characters.
- 4) Enter the IP addresses or range of addresses for the Hosts.

Add a comma-separated list of IP addresses. Addresses can include IP addresses using CIDR notation or a subnet mask. For example,

192.168.1.0/24, 192.168.1.1/255.255.255.0, 192.168.9.12

A host or group of hosts can appear in more than one mapping. Priority is based on the mapping's position in the L4 Mappings list. A mapping conflict can be resolved by dragging a mapping up or down in the list, changing its priority. Click Apply to save a new list order.

- 5) Enter the TCP and UDP ports for this mapping. A port number must be between 1 and 65535.

A list of comma separated ports and port ranges can be entered. For example,

1024-1029, 1731, 1300, 1310-1325

A port can appear in more than one mapping. Priority is based on the mapping's position in the L4 Mappings list. A mapping conflict can be resolved by dragging a mapping up or down in the list, changing its priority. Click Apply to save a new list order.

- 6) Click Update to complete your entry, or Cancel to remove it. Unsaved changes are highlighted with a light-yellow background.
- 7) To enter additional mappings, click the Add button at the bottom of the page.
- 8) Review new and revised mappings that have not yet been saved. Use the Cancel button to remove all changes before saving. Revised mappings require use of the Cancel button to retain the original mapping. Click the red "x" in the Delete column to remove a single new mapping.
- 9) Click Apply at the bottom of the page to save your changes.

L7 Fingerprints

An L7 Fingerprint identifies application traffic based on a user-defined HTTP request URL or an SSL/TLS hostname fingerprint. A Uniform Resource Identifier (URI) string is specified for each HTTP request URL or SSL/TLS hostname fingerprint.

Creating an HTTP URI

Wildcards can be used at the beginning or the end of a URL fingerprint. When used at the end, a wildcard must appear after the hostname in the URL. For example:

L7FB `somedomain.com/index.html`

L7FE `somedomain.com/index.*`

Wildcards also can appear at both the beginning and end of a URI string, subject to the restrictions above.

Matching is done using a longest match rule. For example:

When DPI is enabled, the URL `http://www.facebook.com/hello/hi.a` is analyzed and identified as Facebook traffic.

Next, two L7 Fingerprints are added, using the URI strings below.

L7F1 `www.facebook.com/hi.a` or `*/hi.a`

L7F2 `www.facebook.com/hello/hi.a` or `*/hello/hi.a`

Now when the URL `http://www.facebook.com/hello/hi.a` is analyzed it is identified as L7F2 traffic as the L7F2 URI has the longest match. Note: L7 Signatures have a higher priority than System Applications or L4 Mappings. If Override is selected in an applicable L4 Mapping it would have the highest priority, ahead of L7 Signatures.

Creating an SSL/TLS URI

A definition must include `https://`. In an SSL/TLS URI, only the hostname is used for traffic classification, so, for example, `https://www.foo.com/` and `https://www.foo.com/live` are exactly the same fingerprint. In addition:

- The first fingerprint in the list that matches is used.
- A wildcard character can be used at the beginning of the hostname.
- Port specifications are ignored.
- There is no longest match rule used to select a fingerprint.

Here are some examples of valid SSL/TLS URIs:

SSLTLS1https://www.secure.server.com

SSLTLS2https://*.mysecureserver.com

SSLTLS3https://192.168.25.2:443 (port is not processed)

Application Definitions

| L4 Mappings | | | L7 Fingerprints | | | System Applications | | |
|-------------------|-------------------------------|--------|-----------------|--|--|---------------------|--|--|
| Name | URI | Delete | | | | | | |
| Personnel_App | https://*.private.com | ✘ | | | | | | |
| Payroll_App | https://www.mysite.com | ✘ | | | | | | |
| Manufacturing_App | *parts.com/list | ✘ | | | | | | |
| Project_Scheduler | http://192.168.1.7/projects.* | ✘ | | | | | | |

Add Cancel Apply

Adding an L7 Fingerprint

To add an L7 application fingerprint, do the following:

- 1) Go to the Settings > Application Definitions page and click the L7 Fingerprints tab.
- 2) Click the Add button at the bottom of the page. A new empty row appears at the bottom of the list.
- 3) Enter the name for the application as you want it to appear in views and reports. A name can contain alphanumeric, dot (.), and underscore (_) characters.
- 4) Enter the URI string for the HTTP request URL or SSL/TLS hostname fingerprint in the URI column. For example:

http://192.168.1.7/projects.*

*parts.com/list

https://www.mysite.com/

Note: Matching is done using a longest match rule for HTTP URIs; for SSL/TLS URIs, the first matching fingerprint in the list is used.

- 5) Click Update to complete your entry, or Cancel to remove it. Unsaved changes are highlighted with a light-yellow background.
- 6) To enter additional L7 application fingerprints, click the Add button at the bottom of the page.
- 7) Review new and revised fingerprints that have not yet been saved. Use the Cancel button to remove all changes before saving. Revised fingerprints require use of the Cancel button to retain the original fingerprint. Click the red "x" in the Delete column to remove a single new fingerprint. Click Apply at the bottom of the page to save your changes.

System Applications

A NetShark is preconfigured with a read-only set of system applications that can be identified when DPI is enabled on a capture job or a NetProfiler export. The name and a description of each application can be viewed on the Settings > Applications > System Applications tab.

To sort by Name or Description, click on a column heading. A second click reverses the sort order. Alternatively, hover over the right edge of a column and click the down arrow to select the sort order or the columns to display from a drop-down menu.

Application Definitions

| Application Definitions | |
|--|--|
| L4 Mappings L7 Fingerprints System Applications | |
| Name | Description |
| 12306.cn | 12306.cn is the only China Railway customer service center |
| 126.com | 126.com is a free webmail service of Netease |
| 2345.com | General browsing of navigation portal 2345.com |
| 39.net | 39.net is China's leading health web portal |
| 3COM-TSMUX | 3COM-TSMUX Queuing Protocol |
| 4399.com | General browsing and game play on Chinese casual gaming website 4399.com |
| 4Shared | A file sharing service that provides search functions, allows users to upload and download files to their accounts and share links with other people. |
| 56.com | General browsing and streaming media from Chinese video sharing website 56.com |
| 914CG | Texas Instruments 914C/G Terminal |
| about.com | English source for original information and advice |
| ACA-Services | DEC's Application Control Architecture Services |
| ACI | Application Communication Interface |
| ACR-NEMA | A standard for handling, storing, printing, and transmitting information in medical imaging. |
| Active-Directory-Protocol | Microsoft Active Directory |
| ActiveSync | ActiveSync Notifications, IANA port 1034/tcp and 1034/udp |
| AD-Backup | Microsoft Active Directory Backup Service. |
| AD-DRS | Microsoft Active Directory Replication Services. |
| AD-DSAOP | Active Directory DSAOP services |
| AD-DSROL | Microsoft Active Directory Domain Services helps administrators securely manage users, computers, and other devices on the network and facilitates resource sharing and collaboration between users. |
| AD-File-Replication-Service | Microsoft Active Directory File Replication Services used to replicate files and changes between domain controllers |
| AD-NSP | Microsoft Active Directory Name Service Provider |
| AD-Restore | Microsoft Active Directory Restore Service. |

Advanced settings

The Advanced Settings page allows modification of the NetShark Probe configuration file and should only be used with the assistance of Riverbed Support personnel.

Troubleshooting an initial installation

If you have gone through the initial configuration of your NetShark or NetShark virtual edition and it does not seem to function properly, try the troubleshooting steps below. Remember that the default username and password are `admin` and `admin`.

After each step, check again to see whether your appliance is functioning properly.

- 1) Using the appliance's console, enter `wizard` at the console prompt and check that you have the right values for:
 - a) IP address
 - b) IP subnet mask
 - c) IP default gateway
 - d) DNS servers
 - e) Domain name

If you don't want to change any of the entries, you can cancel by typing `c` at the end of the list of questions.

If you used DHCP to provision your IP address, you can find the IP address by entering `interface show primary` at the console prompt.

- 2) Try to ping the appliance at the IP address you set up in using the configuration wizard. If that doesn't work, it indicates a possible network problem. Check your network connections and make sure that your firewall and proxy configurations are correct.
- 3) Try using your Web browser to connect to the Web UI of the appliance.
- 4) If you configured SSH, try connecting with an SSH program like PuTTY.

If those steps fail, contact Riverbed technical support:

Email: <http://support.riverbed.com>

Phone (U.S. and Canada): 1-888-782-3822

Phone (outside U.S. and Canada): 1-415-247-7381

Securing your appliance configuration

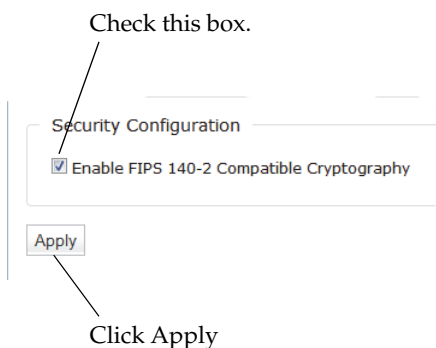
Use the following procedures to make your NetShark appliance compliant with:

- Common Criteria certification (certificate #1747)
- JITC hardened
- FIPS 140-2 compliant cryptography

Common Criteria initial setup

1) Enable FIPS-compliant cryptographic algorithms by putting the appliance into FIPS mode.

- In the CLI: `system fips enable`
- In the Web interface:
 - a) Go to Settings > Basic Settings
 - b) Put a check mark in the Enable FIPS 140-2 Compatible Cryptography box at the bottom of the page.

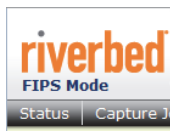


c) Click Apply.

A reboot is required:

- In the CLI: Use `system reboot`.
- In the Web interface: Go to System > Maintenance and click the Reboot SteelCentral NetShark button at the bottom of the page.

After the reboot the appliance shows "FIPS Mode" in the banner in the Web interface.



1) Make sure that the Web Interface certificate and private key are compliant:

- Private key algorithm must be RSA.
- Key length should be at least 2048 bits.
- Certificate hashing algorithm should be one of:
 - SHA1
 - SHA224
 - SHA256
 - SHA384
 - SHA512

In the CLI: The certificate and private key can be replaced using `certificate web set`.

In the Web interface: To view the certificate, go to Settings > SSL Certificate Management and click the Web Interface tab. If you need to import or generate a new certificate, use the buttons at the bottom of the page.

The default certificate and any self-signed certificates generated by the appliance are compliant.

A NetShark Probe service restart (CLI: `service probe restart`; Web interface: a Restart Probe button pops up) is required for the certificate change to be effective.

2) Make sure that the NetProfiler Export certificate and private key are compliant:

- Private key algorithm must be RSA.
- Key length should be at least 2048 bits.
- Certificate hashing algorithm should be one of:
 - SHA1
 - SHA224
 - SHA256
 - SHA384
 - SHA512

In the CLI: The certificate and private key can be replaced using `certificate profiler-export set`.

In the Web interface: To view the certificate, go to Settings > SSL Certificates and click the NetProfiler Export tab. If you need to import or generate a new certificate, use the buttons at the bottom of the page.

When booted in FIPS mode, the default certificate and any self-signed certificates generated by the appliance are compliant.

A NetShark Probe service restart (CLI: `service probe restart`; Web interface: a Restart Probe button pops up) is required for the certificate change to be effective.

Note—A NetShark appliance that has never booted in FIPS mode uses a default NetProfiler Export certificate that is compatible with NetProfiler appliances of version 9.5 or earlier. The first time the NetShark appliance boots in FIPS mode, this certificate is replaced with a certificate that is FIPS and Common Criteria compliant and that is compatible only with NetProfiler appliances of version 9.6 or later. If you revert to non-FIPS mode on the NetShark appliance, the version 9.6 certificate remains active; it does not revert to the version 9.5 certificate.

3) Make sure that the Trusted NetProfiler certificate and private key are compliant:

Tasks

- Private key algorithm must be RSA.
- Key length should be at least 2048 bits.
- Certificate hashing algorithm should be one of:
 - SHA1
 - SHA224
 - SHA256
 - SHA384
 - SHA512

In the CLI: The certificate and private key can be managed using the `certificate profiler-trusted ...` commands.

In the Web interface: To view the certificate, go to Settings > SSL Certificates, click the Trusted Profilers tab, and click the View button for one of the listed certificates. If you need to import a new certificate, use the Add button at the bottom of the page.

By default the NetShark appliance contains two Trusted NetProfiler certificates: `default_profiler` and `default_profiler_fips`. The `default_profiler` certificate is compatible with appliances with software version 9.5 or earlier, or appliances with version 9.6 or later software that have never been booted in FIPS mode; this certificate is not compliant. The `default_profiler_fips` certificate is compliant. For operation in FIPS mode, you must remove the `default_profiler` certificate. In the CLI: Use `certificate profiler-trusted del`. In the Web interface: Use the Remove button next to `default_profiler` in the list of certificates.

If you make any changes to the certificates, you must restart the NetShark Probe service (CLI: `service probe restart`; Web interface: a Restart Probe button pops up).

- 4) Make sure that authentication is set to Local Authentication. (The TACACS+ and RADIUS implementations use algorithms that are not FIPS compliant.)\

In the Web interface: On the Settings > Authentication Settings page, make sure the Local Password File Authentication check box is checked and the TACACS+ and RADIUS check boxes are unchecked.

Authentication Type

Authentication Methods: Local Password File Authentication This box should be checked.

Tacacs+ Authentication These boxes should be unchecked.

Radius Authentication

Authentication Sequence: Local Only

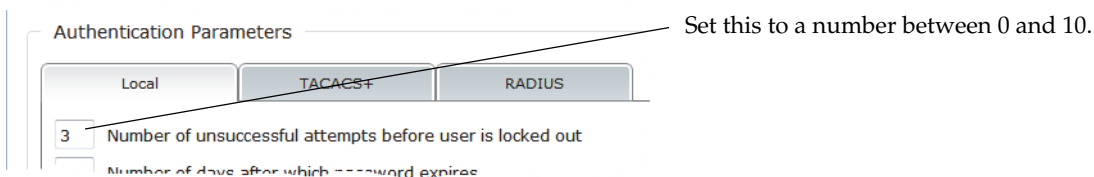
Note: Specify the primary and fallback sequence of authentication based on the authentication methods selected.

If you make any changes, click the Apply button at the bottom of the page.

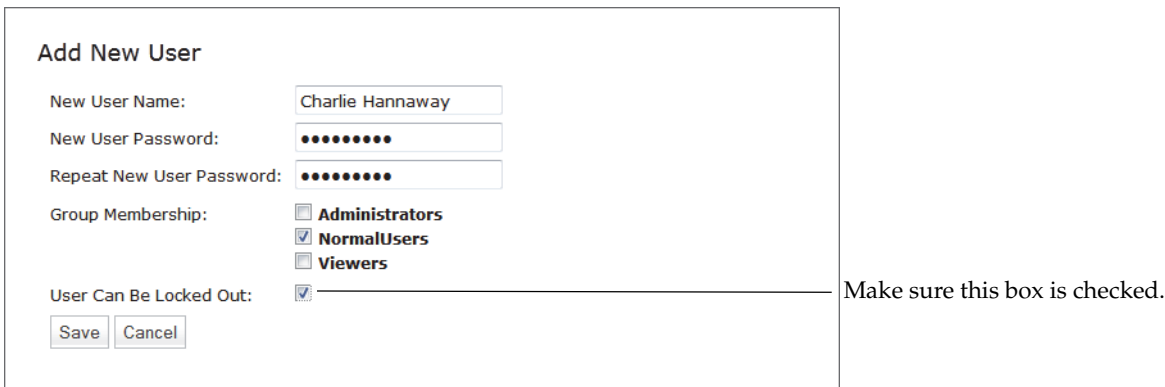
- 5) Configure all users, including the administrator, to have a lockout policy.

In the Web interface:

- a) From Settings > Authentication Settings, on the Local tab, make sure that the “Number of unsuccessful login attempts before user is locked out” is set to a number between 0 and 10.



- b) When creating a user (in Settings > Users and Groups, click the Add A New User button), make sure that the “User Can Be Locked Out” check box is checked.

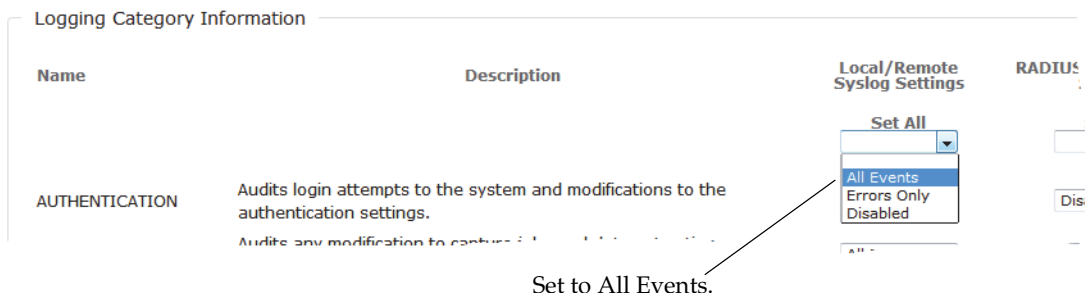


Note—The default users (admin, normaluser) do not have the lockout property enabled. Since it is not possible to change that property on an existing user, you must delete the existing user entry and recreate it with the lockout property enabled. For the “admin” user, first create another, temporary, admin user (say, “admin2”) and use that temporary admin user to delete and recreate the “admin” user.

- 6) Change the Logging Settings to log all events to the local syslog.

In the Web interface: Go to Settings > Logging Settings. In the Local/Remote Syslog Settings column, set the top drop-down box to All Events. This sets all categories of events to be logged locally. (There is no need to change the RADIUS/TACACS+ Log Settings box, as remote logging to TACACS+ and RADIUS servers is not officially supported in the Common Criteria compliant mode of operation.)

Logging Settings



7) Make sure that these specific Advanced Settings have appropriate values.

In the Web interface: From Settings > Advanced Settings, make sure that the following settings are configured as described. Once the appliance is booted in FIPS mode these settings cannot be changed.

- `webui.legacy_port=0`
- `connection.ports.https=443`
- `connection.ports.http=80`
- `connection.ports.http_redirect=True`
- `webui.enabled=True`
- `profilerexport.profiler.port=41018`
- `profilerexport.profiler.ssl.enabled=True`
- `profilerexport.profiler.ssl.port=41017`
- `actions.enable_run_program=False`

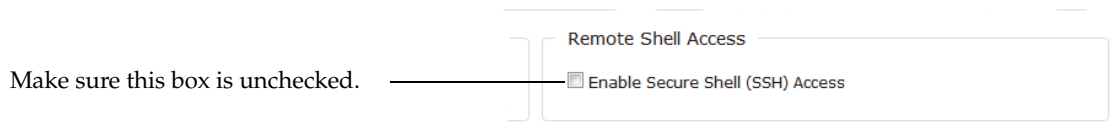
Note that any setting that is not listed under Advanced Settings has a value corresponding to the list above. (This applies to `actions.enable_run_program`, which is not listed.)

8) Enable FIPS mode on the Windows client system running Packet Analyzer. Details are at <http://technet.microsoft.com/en-us/library/cc750357.aspx>.

9) Enable FIPS mode on the Windows client system running Packet Analyzer. Details are at <http://technet.microsoft.com/en-us/library/cc750357.aspx>.

10) Disable SSH access, as its use has not been certified for Common Criteria.

In the Web interface: Go to Settings > Basic Settings and make sure that the Enable Secure Shell (SSH) Access box is unchecked. If you make a change, click the Apply button in the lower left corner of the page.



Common Criteria operation

Packet Analyzer

- Do not use Packet Analyzer to analyze local files or to analyze traffic from local interfaces. There is no authentication and auditing when analyzing local files and traffic.
- Do not tick the “Remember password” check box when connecting to a NetShark appliance. Starting with version 10.7, the password is encrypted and saved on the client system running Windows.
- Do not use SMTP with authentication when configuring a watch that sends an email. The password would be saved in clear text on the Shark appliance.
- Do not use the SSL protocol when configuring a watch that sends an email. There is no auditing on this cryptographic functionality.

NetShark appliance

- Do not change any of the settings listed below. Changing any of the following settings when FIPS mode is enabled is prohibited.
 - `webui.legacy_port=`
 - `connection.ports.https=`
 - `connection.ports.http=`
 - `connection.ports.http_redirect=`
 - `webui.enabled=`
 - `actions.enable_run_program=`
 - `profilerexport.enabled=`
 - `profilerexport.profiler.port=`
 - `profilerexport.ssl.enabled=`
 - `profilerexport.profiler.ssl.port=`
 - `profilerexport.profilers.address.*=`

Changing any of these settings when FIPS mode is enabled results in a failure, as it would violate either secure communication or auditing requirements.

JITC-hardened initial setup

1) Put the appliance into Common Criteria compliant mode. Refer to the list of instructions under [Common Criteria initial setup](#), above.

2) Disable the IPMI port. The IPMI port does not use secure channels. Note that this does not apply to a NetShark virtual edition, as a NetShark virtual edition does not have IPMI ports

In the CLI: Use `system ipmi disable`.

3) Set compliant password requirements.

In the Web interface: Go to Settings > Authentication Settings. In the Local tab, click the STIG Compliant Settings button, then click Apply.

The screenshot shows the 'Authentication Parameters' web interface. It has three tabs: 'Local', 'TACACS+', and 'RADIUS'. Under the 'Local' tab, there are several input fields for password constraints:

- Number of unsuccessful attempts before user is locked out: 3
- Number of days after which password expires: 90
- Minimum password length: 8

Below these are 'Password Constraints' with the following settings:

- Minimum number of upper-case letters: 1
- Minimum number of lower-case letters: 1
- Minimum number of numeric characters: 1
- Minimum number of special characters: 1
- Number of previous user passwords stored in history: 10

A note states: 'Note: Specify '0' to disable the constraint.' At the bottom of the form, there are two buttons: 'Default Settings' and 'STIG Compliant Settings'. An arrow points from the 'STIG Compliant Settings' button to the text 'Click to set password requirements.' Below the form is an 'Apply' button with an arrow pointing to the text 'Click to apply settings.'

4) Change the default boot password.

In the CLI: Use `system boot password`.

5) Change the default BIOS password. See the section “How to change the BIOS password” in Appendix A for more information.

6) Change the Web/CLI default user passwords.

In the Web interface: Go to Settings > Users and Groups and for each user click the Change Password button and change the password.

7) Set up a login banner.

In the Web interface: Go to Settings > Authentication Settings and configure a login banner. Click the Apply button when done.

Authentication Settings

Web UI Settings

Specify Purpose At Login

Session Timeout (minutes):

Login Banner:

Enter text for login banner.

8) Enable the firewall. The default settings are compliant.

In the Web interface: Go to Settings > Firewall Settings and make sure the Enable Firewall Settings box is checked. If you make a change, click the Apply Changes button when done.

Firewall Settings

General Settings

Enable Firewall Protection ————— Check this box.

Default Action:

9) Configure the idle timeout for the Web interface to 10 minutes or less.

In the Web interface: Go to Settings > Authentication Settings and set the Session Timeout to 10 minutes or less. Then click the Apply button at the bottom of the page.

Authentication Settings

Web UI Settings

Specify Purpose At Login

Session Timeout (minutes): ————— Set to 10 minutes or less.

10) Configure authentication for your NTP servers. You need to use a secure hashing algorithm and key for each NTP server to be compliant.

By default, NTP server listings show only the server (as a URL):

```
server1
server2
server3
server4
```

To use secure hashing, add an index, an algorithm, and a key for each server:

```
server1:index1:algorithm1:key1
server2:index2:algorithm2:key2
```

Tasks

```
server3:index3:algorithm3:key3
```

```
server4:index4:algorithm4:key4
```

Note that:

- When using NetProfiler Export, the NetShark appliance uses the NetProfiler appliance as the NTP source, and no additional configuration is required.
- You can configure NTP servers only when export to NetProfiler appliances is disabled.
- The index field must be unique within the NetShark appliance. It is provided by the administrator of the NTP server.
- Valid values for the algorithm are MD5 and SHA1. These values are not case sensitive.

Note also that:

- When in non-FIPS mode the NetShark appliance uses MD5-based NTP authentication with the NetProfiler appliance.
- When in FIPS mode the NetShark appliance uses SHA1-based NTP authentication with the NetProfiler appliance.

In the CLI: Use the `wizard` command, and in the NTP server specification step enter the server, index, algorithm, and key information for each server.

In the Web interface: Go to Settings > Basic Settings and enter the NTP server information in the NTP Server Addresses box. Then click the Apply button.

The screenshot shows the 'Basic Settings' page in a web interface. Under the 'Host Information' section, there are fields for 'Host Name' (Shark11) and 'Timezone' (America/Los_Angeles). The 'NTP Server Addresses' field is a text area containing four lines of configuration: '0.riverbed.pool.ntp.org:1:MD5:Key1', '1.riverbed.pool.ntp.org:2:MD5:Key2', '2.riverbed.pool.ntp.org:3:SHA1:Key3', and '3.riverbed.pool.ntp.org:4:SHA1:Key4'. An arrow points from the text 'Enter server information here.' to the NTP Server Addresses field.

When the settings have been updated, the keys will be hidden.

The screenshot shows the 'Basic Settings' page after the NTP server addresses have been updated. The 'NTP Server Addresses' field now contains the same four lines of configuration, but the keys are replaced with asterisks: '0.riverbed.pool.ntp.org:1:MD5:***', '1.riverbed.pool.ntp.org:2:MD5:***', '2.riverbed.pool.ntp.org:3:SHA1:***', and '3.riverbed.pool.ntp.org:4:SHA1:***'.

- 11) Change the BIOS settings to disallow booting from removable media. See “How to disable booting from removable media” in the Appendix Changing System Settings.

CHAPTER 3 Reference

CLI commands

The commands available through the NetShark console interface are listed below:

Table 3-1

| | |
|--|--|
| <code>certificate profiler-trusted add</code> | Add a new trusted NetProfiler certificate |
| <code>certificate profiler-trusted del</code> | Remove the given trusted NetProfiler certificate |
| <code>certificate profiler-trusted list</code> | List all trusted NetProfiler certificates |
| <code>certificate profiler-export set</code> | Replace the encryption key used by NetProfiler export |
| <code>certificate web set</code> | Replace the encryption key used by the Web UI |
| <code>challenge create</code> | Create a new challenge |
| <code>challenge response</code> | Validate the response of a challenge |
| <code>interface show primary</code> | Print network settings for primary |
| <code>interface show aux</code> | Print network settings for aux |
| <code>interface show ipmi</code> | Print network settings for the IPMI interface |
| <code>license add</code> | Add a new license |
| <code>license del</code> | Delete a license |
| <code>license clear</code> | Clear all licenses |
| <code>license list</code> | List all licenses |
| <code>packet-storage status</code> | Show the Packet Storage status |
| <code>packet-storage reinitialize</code> | Reinitialize the Packet Storage with RAID 0, RAID 5, or RAID 6 |

Table 3-1

| | |
|--|--|
| <code>service probe restart</code> | Restart the NetShark Probe service |
| <code>service probe coredump enable</code> | Enable the NetShark Probe core dump |
| <code>service probe coredump disable</code> | Disable the NetShark Probe core dump |
| <code>service probe coredump status</code> | Status of the NetShark Probe core dump functionality |
| <code>service probe coredump upload</code> | Upload the NetShark Probe core dump |
| <code>service probe coredump force</code> | Force the NetShark Probe to do a core dump |
| <code>service packetrecorder restart</code> | Restart the Packet Recorder |
| <code>service packetrecorder coredump force</code> | Force the Packet Recorder to do core dump |
| <code>service packetrecorder coredump enable</code> | Enable the Packet Recorder core dump |
| <code>service packetrecorder coredump disable</code> | Disable the Packet Recorder core dump |
| <code>service packetrecorder coredump status</code> | Status of the Packet Recorder core dump functionality |
| <code>service packetrecorder coredump upload</code> | Upload the Packet Recorder core dump |
| <code>service mgmt restart</code> | Restart the Management Daemon |
| <code>storage-unit enroll-force</code> | Start an enrollment procedure |
| <code>storage-unit enroll-reset</code> | Reset all previous enrollments |
| <code>storage-unit rescan</code> | Rescan storage units |
| <code>system boot password</code> | Reset the boot password |
| <code>system fipsmode enable</code> | Enable FIPS mode |
| <code>system fipsmode disable</code> | Disable FIPS mode |
| <code>system fipsmode show</code> | Show the current FIPS status and the status at the next reboot |
| <code>system firewall disable</code> | Disable the system firewall |
| <code>system firewall status</code> | Show the current status of the firewall |
| <code>system ipmi enable</code> | Enable the IPMI interface |
| <code>system ipmi disable</code> | Disable the IPMI interface |

Table 3-1

| | |
|--|---|
| <code>system ipmi root password</code> | Update the IPMI root password |
| <code>system log upload</code> | Upload system logs to an FTP server |
| <code>system poweroff</code> | Power off the NetShark |
| <code>system reboot</code> | Reboot the NetShark |
| <code>system serial show</code> | Show the NetShark serial number |
| <code>system vault wipe</code> | Wipe and re-initialize the secure key vault |
| <code>system version show</code> | Show the software version and build numbers |
| <code>system wipe</code> | Wipe off all the data from the disks |
| <code>uptime-report enable</code> | Enable the uptime reports |
| <code>uptime-report disable</code> | Disable the uptime reports |
| <code>uptime-report status</code> | Check on the uptime reports status |
| <code>clock set</code> | Set the system date and time on a physical NetShark |
| <code>wizard</code> | Start a wizard to enter basic NetShark settings |
| <code>help</code> | Display this help |
| <code>exit</code> | Exit the shell |

Certificate commands

certificate profiler-trusted add <trusted-key-name>

Adds a new Trusted NetProfiler certificate. The <trusted-key-name> appears as the name of the certificate when you list the Trusted NetProfiler certificates using the `certificate profiler-trusted list` command (described below) or when listing them in the Web interface.

certificate profiler-trusted del <trusted-key-name>

Deletes the specified Trusted NetProfiler certificate.

certificate profiler-trusted list

Lists all Trusted NetProfiler certificates.

certificate profiler-export set

Replaces the certificate and private key used for NetProfiler Export. When you run this command, the CLI prompts you to type (copy and paste) the PEM version of the certificate and private key into the command line.

certificate web set

Replaces the certificate and private key used by the Web Interface. When you run this command, the CLI prompts you to type (copy and paste) the PEM version of the certificate and private key into the command line.

Interface commands

These commands show useful information about the appliance's various Ethernet interfaces.

An example of the output:

```
shark> interface show primary

mac address   : 00:25:90:0E:2E:82
ip address    : 10.5.16.59
netmask       : 255.255.255.0
broadcast     : 10.5.16.255
dhcp          : enabled
link status   : up (1000Mbps full duplex)

[OK]
```

interface show primary

interface show aux

interface show ipmi

License commands

license add <license-key>

Adds a new license to the appliance.

license del <license-key>

Deletes the specified license from the appliance.

license clear

Deletes all licenses from the appliance.

license list

Lists all licenses on the appliance.

To make the changes effective, you must restart the Shark Probe service after issuing these commands:

- license add <license-key>
- license del <license-key>
- license clear

You can use the `service probe restart` command for this purpose.

Packet Storage commands

packet-storage status

Shows the current status of the packet storage.

packet-storage reinitialize <raid0> <raid5> <raid6>

Reinitializes the Packet Storage with RAID 0, RAID 5, or RAID 6. All packet storage data is lost.

Service commands

The service commands act on the main services running on the NetShark. They do not reboot the appliance. If you want to reboot the appliance, use the `system reboot` command.

service probe restart

Restarts the NetShark Probe service.

service probe coredump enable

Enables the NetShark Probe core dump.

service probe coredump disable

Disables the NetShark Probe core dump.

service probe coredump status

Shows the current status of the NetShark Probe core dump functionality.

service probe coredump upload <CaseNumber> [server <ServerPath>]

Uploads the NetShark Probe core dump. The uploaded file cannot be larger than 50 MB. The default FTP address is: <ftp://anonymous:anonymous@ftp.riverbed.com/incoming>. The uploaded file name uses this format:

```
case-XXXXXX-sharkcoredump- [tccaptureserver | PilotServer] - [HostName] -yyyymmdd-hh  
mmss.gz
```

service probe coredump force

Forces the NetShark Probe to do a core dump.

service packetrecorder restart

Restarts the Packet Recorder service.

service packetrecorder coredump force

Forces the Packet Recorder to do a core dump.

service packetrecorder coredump enable

Enables the Packet Recorder core dump.

service packetrecorder coredump disable

Disables the Packet Recorder core dump.

service packetrecorder coredump status

Shows the current status of the Packet Recorder core dump functionality.

service packetrecorder coredump upload <CaseNumber> [server <ServerPath>]

Uploads the Packet Recorder core dump. The uploaded file cannot be larger than 50 MB. The default FTP address is: <ftp://anonymous:anonymous@ftp.riverbed.com/incoming>. The uploaded file name uses this format:

```
case-XXXXXX-sharkcoredump- [tccaptureserver | PilotServer] - [HostName] -yyyymmdd-hh  
mmss.gz
```

service mgmt restart

Restarts the Management Daemon.

storage-unit enroll-force

Starts an enrollment procedure. All storage units are enrolled and all packet storage data is lost.

storage-unit enroll-reset

Resets all previous storage unit enrollments. A `storage-unit enroll-force` command then must be used to create new packet storage.

storage-unit rescan

Rescans storage units. Rescanning can restore a base unit's communication with previously enrolled storage units. Packet capture resumes.

System commands**system boot password**

Resets the system boot password. You will be asked to enter a password and to confirm it.

system fipsmode enable

Enables the use of FIPS 140-2 compliant cryptography. This change takes place at the next system reboot.

system fipsmode disable

Disables FIPS mode. This change takes place at the next system reboot.

system fipsmode show

Shows the current FIPS status and the status after the next system reboot.

system firewall disable

Disables the system firewall. This is the emergency command you can use if you lock yourself out of the NetShark. You would enter it from a terminal (or terminal emulator) connected through the serial port or the keyboard/monitor ports, and then reconfigure the firewall from the Web interface to fix the problem.

system firewall status

Shows the current status of the system firewall.

system ipmi enable {dhcp}|{ipaddr <addr> netmask <mask> [gateway <ipaddr>]}

Enables the IPMI interface. You must specify DHCP address assignment or specify an IP address and subnet mask. You can also specify a gateway IP address if you wish.

system ipmi disable

Disables the IPMI interface. Note: The IPMI interface is disabled by effectively setting its IP address to 0.0.0.0.

system ipmi root password

Updates the IPMI root password. The root account cannot be deleted. Up to 16 user accounts can be created using the BMC Web interface.

system log upload [<case_number>] [server <server_path>] [level <log_level>]

Uploads a .tgz file of system logs to FTP or SCP server. If called without parameters it generates the logs with log level "current," case number "000000" and uploads them to <ftp://anonymous:anonymous@ftp.riverbed.com/incoming>. Confirmation is asked before command is processed.

- <case_number> must be numeric.
- <server_path> must include protocol (ftp:// or scp://), credentials, the server name and the path where the logs will be stored. Example: ftp://user:password@my.ftp.server/path/to/file.
- <log_level> can be current, probe, packetrecorder, or complete.

Log file's name is case-XXXXXX-sharkdebug-LLLLLL-shark-yyyymmdd-hhmmss.tgz

system poweroff

Powers off the appliance.

system reboot

Reboots the appliance.

system serial show

Shows the serial number of the appliance.

system vault wipe

Reinitializes the secure key vault. This erases all data in the vault, recreates the folder structure, and generates SSH keys. In the process, the Web Interface certificate, the NetProfiler Export certificate, and the Trusted NetProfiler certificates are all erased and reset to their default values. A reboot is required after this operation.

system version show

Displays the current software version and build numbers.

system wipe {dod|dodshort|short}

Restarts the appliance with a custom kernel that securely wipes all data from the disks. Choose one of three wipe options:

- `dod` - 7 passes, random data (most secure), DoD 5220.22-M standard wipe
- `dodshort` - 3 passes, random data, DoD 5220-22-M short wipe (passes 1, 2, and 7 of the standard wipe)
- `short` - 1 pass, all zeros

Note that:

- It takes a long time for the wipe operation to complete, during which time the appliance is reachable only from the monitor and keyboard. Therefore, it is strongly recommended that you run this command locally from the monitor/keyboard.
- After the wipe operation is complete, the appliance software needs to be reinstalled, as system storage has been wiped during the operation.

Uptime-report commands

uptime-report enable

Enables the uptime ping service. It is enabled by default.

uptime-report disable

Disables the uptime ping service.

uptime-report status

Shows the status of the uptime ping service.

For more information on the uptime ping service, see <https://support.riverbed.com/announce/dns.htm>.

Clock command

clock set {<yyyy/mm/dd> <hh:mm:ss>}

Sets the system time and date for a physical NetShark by specifying the date (year, month, day) and the time (hour, minutes, seconds). A system reboot is required to set the date and time.

Example:

```
NetShark> clock set 2014/07/15 14:20:00
Ready to set system time to 2014-07-15 14:20:00.000000
A reboot is required in order to set the system time.
Are you sure? [y|n]
```

A NetShark virtual edition uses the date and time set in the host.

Wizard command

wizard

Runs the setup wizard for a NetShark. This leads you through setting up initial configuration parameters, including:

- hostname
- IP addressing for the primary and aux ports
- DNS servers
- domain name for the appliance
- time zone
- SSH daemon
- PTP and management port used
- NTP servers

You can find details on the wizard in the Quick Start Guide for the NetShark or the NetShark virtual edition.

Help command

help

Displays the list of CLI commands.

Exit command

exit

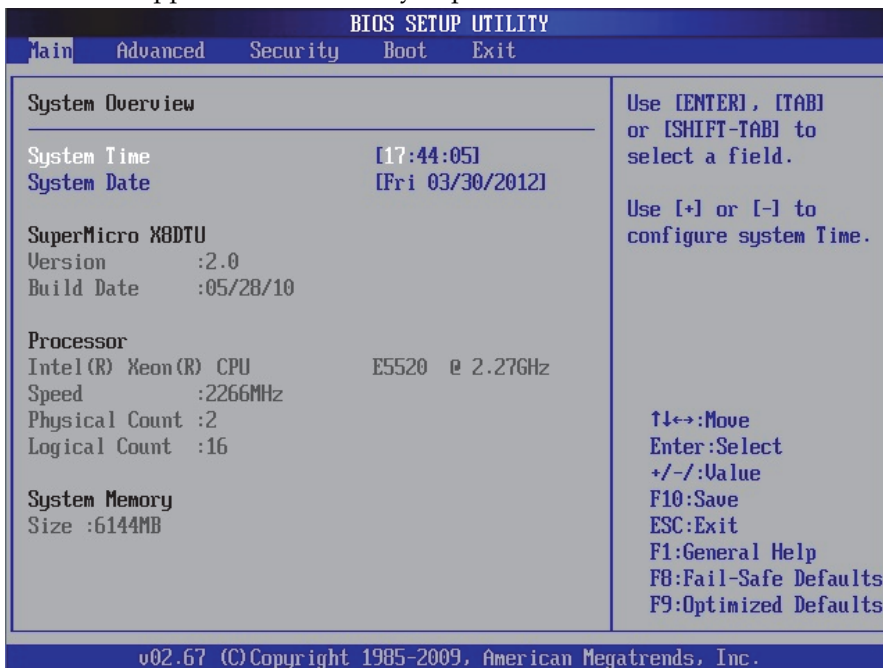
Exits the CLI.

APPENDIX A Changing System Settings

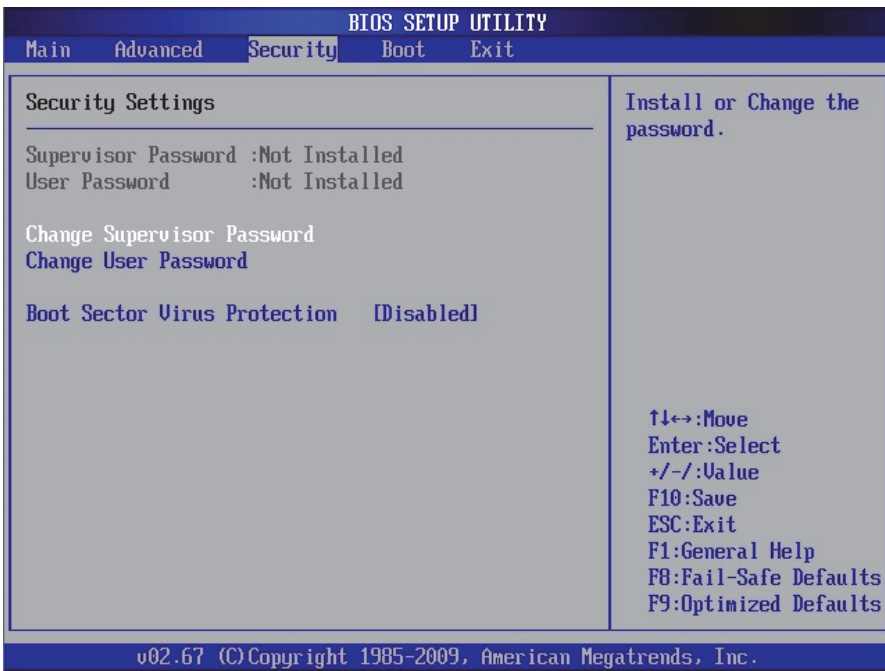
Changing BIOS settings for NetShark Model xx00 appliances

How to change the BIOS password

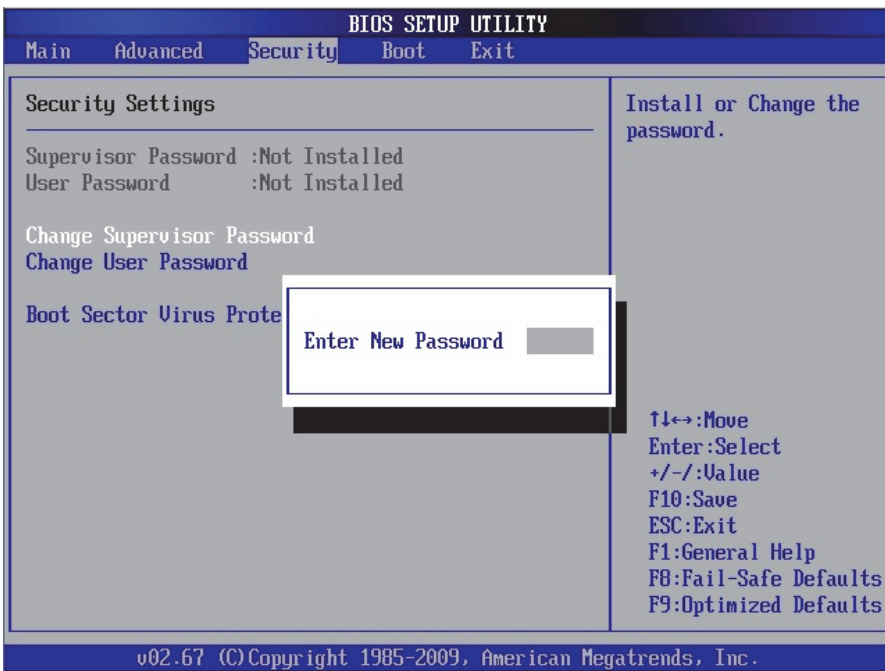
- 1) Reboot the appliance and be ready to press DEL in order to enter the BIOS SETUP UTILITY.

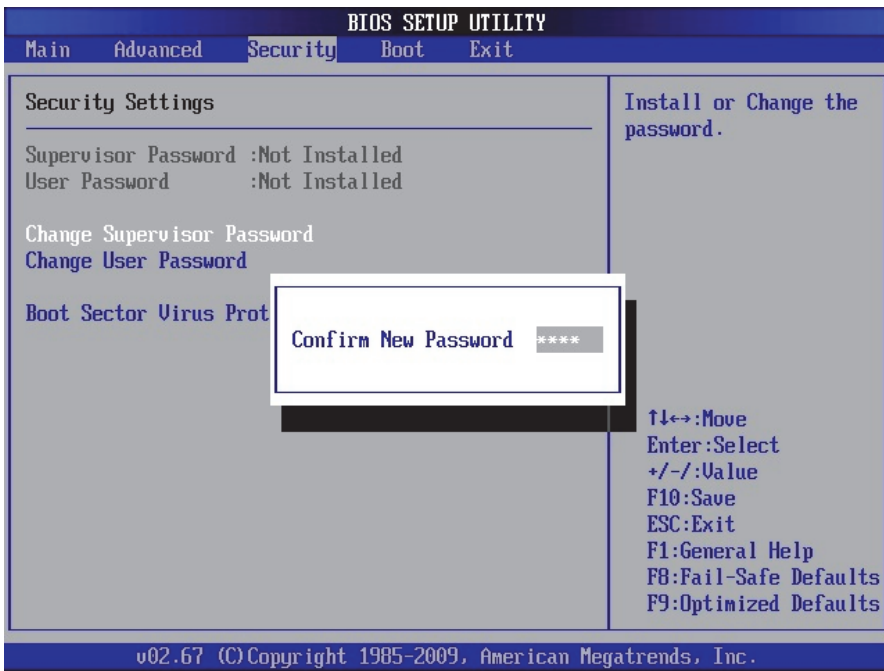


2) Move to the 'Security' tab and select the option 'Change Supervisor Password'.

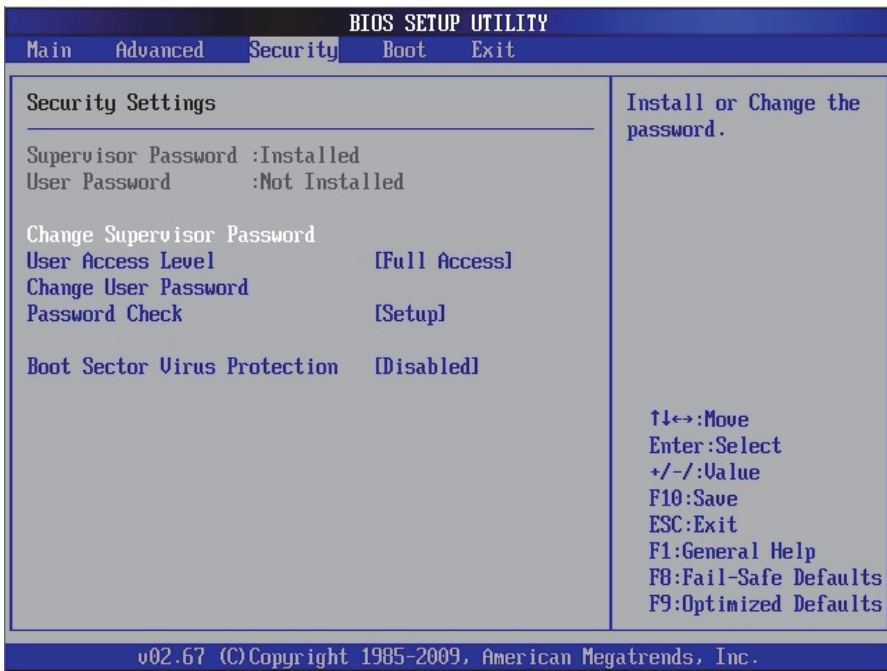


3) Enter a password at the prompt and confirm it.

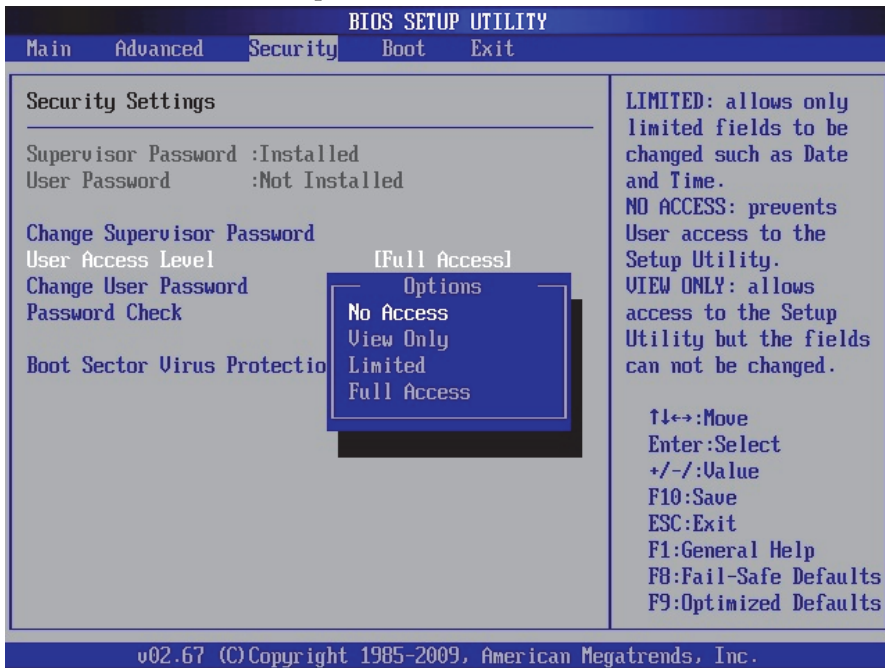




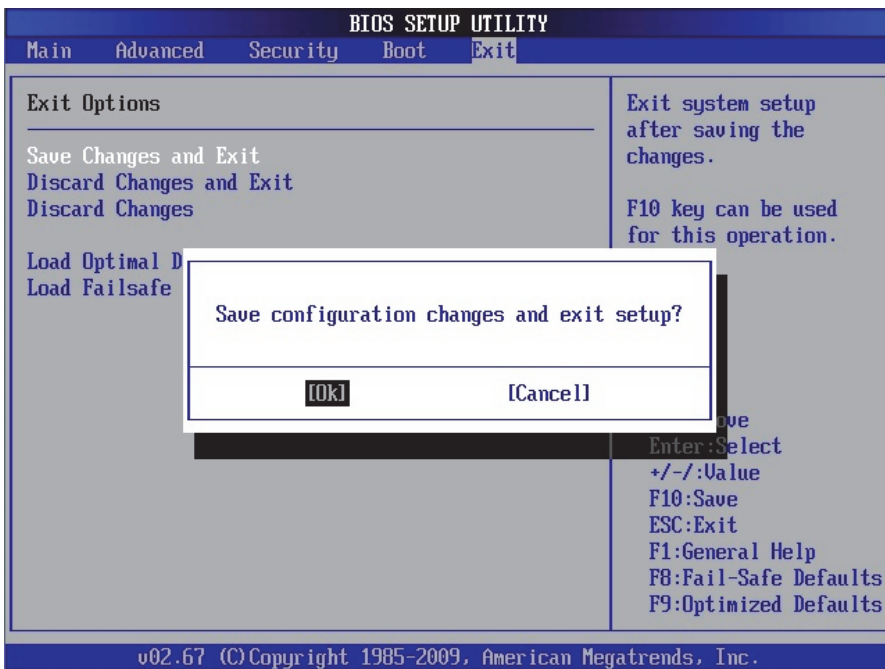
4) Once the Supervisor Password has been enabled, the User Access Level may be set to 'Full Access'. This must be disabled since only the Supervisor can access the BIOS SETUP UTILITY.



5) Select 'User Access Level', press Enter and select 'No Access'.

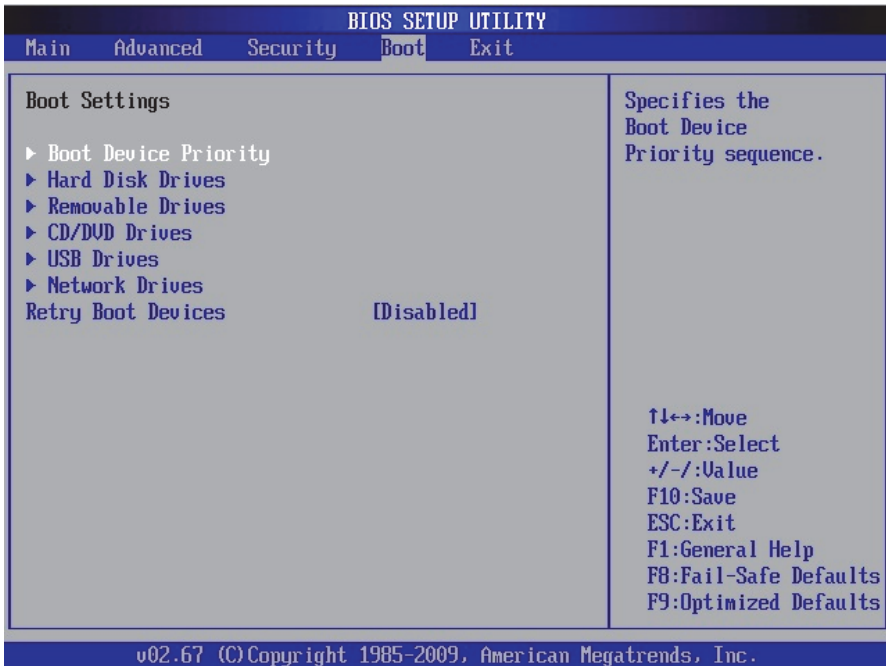


6) Move to the 'Exit' tab and save the settings.

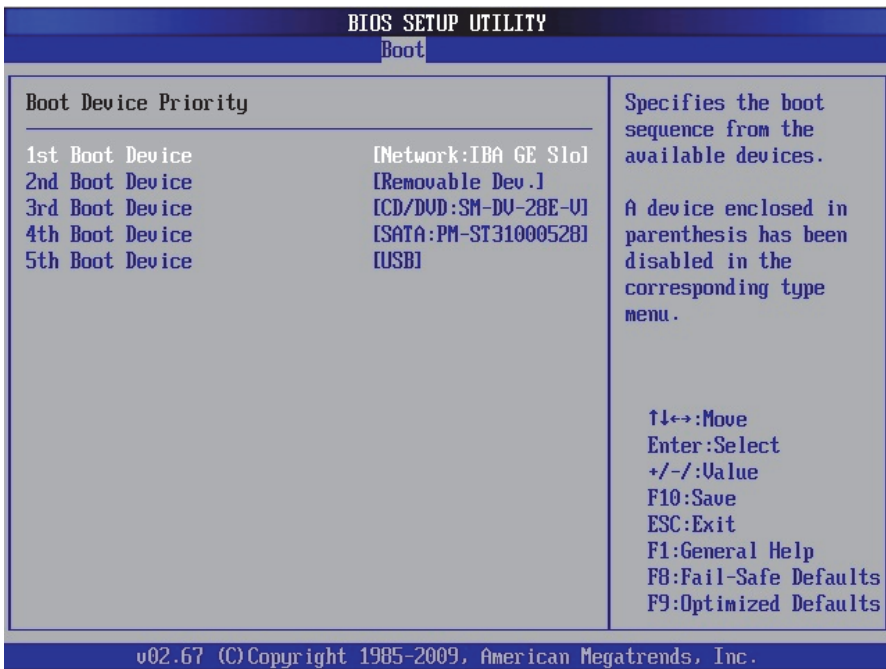


How to disable booting from removable media

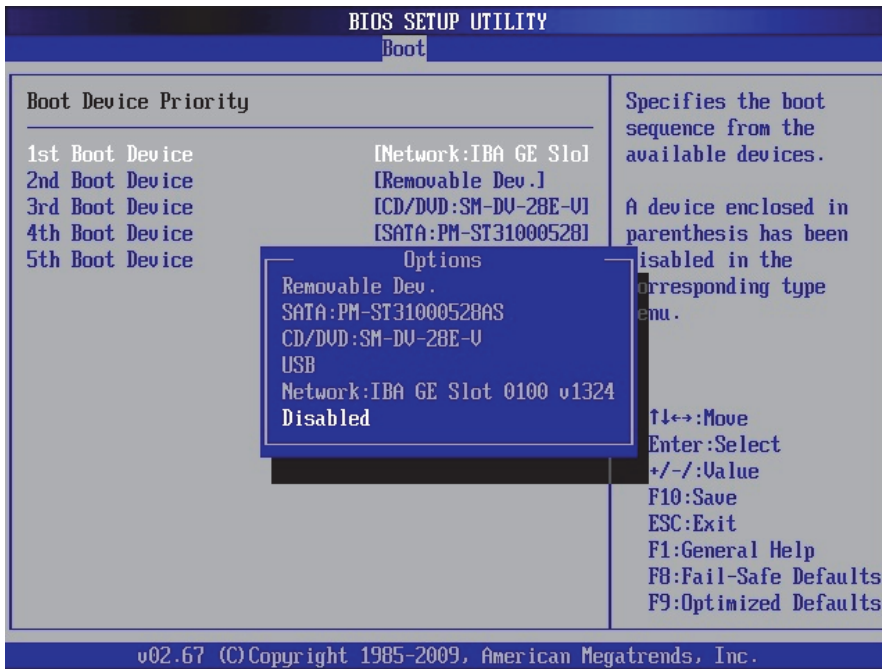
1) In the BIOS SETUP UTILITY, move to the 'Boot' tab.



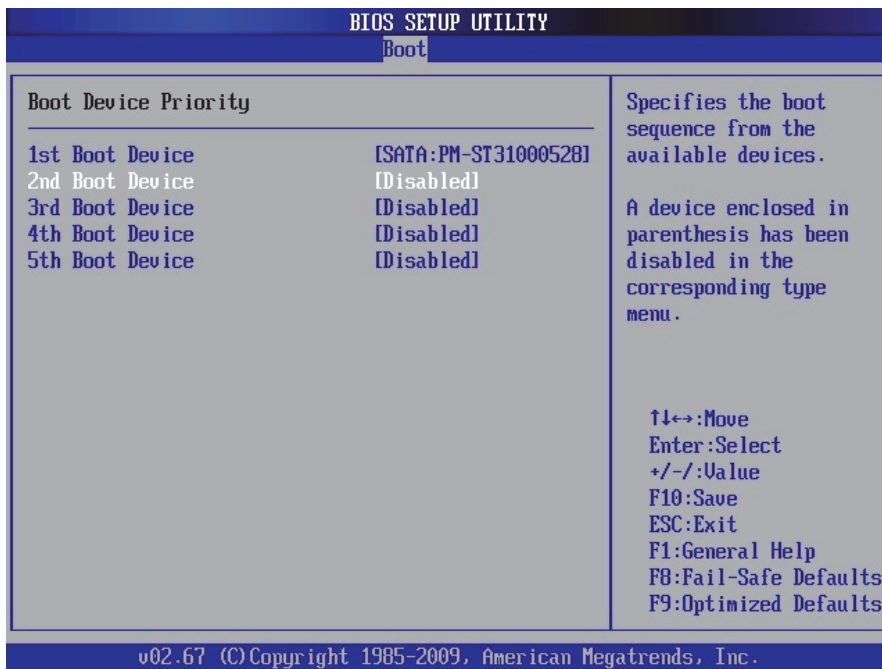
2) Select the option 'Boot Device Priority'. Removable (and network) devices may be listed.



3) To disable a device, select it, press enter and select 'Disabled' in the drop-down menu.



4) Make sure that all removable drives are disabled.



5) Save settings and exit the BIOS SETUP UTILITY.

APPENDIX B Installing NetShark Software

Installing NetShark from a USB memory stick

NetShark is shipped from the factory with its software already installed. You can configure the factory-installed software and begin using the product, or, beginning with software version 10.8.0, you can perform a complete installation of software downloaded from the Riverbed Support site using a USB memory stick.

To configure and run the factory-installed software, refer to *SteelCentral NetShark Quick Start Guide*. To download and install a new version of the software from the Riverbed Support site, follow the instructions below.

Step 1 - Download the software

Download the installation software from the Riverbed Support site: <https://support.riverbed.com>. Be sure to download the Install (ISO Image) software.

An account is required to access the Support site. If you do not have an account, follow the directions on the Support site to set one up.

Step 2 - Create bootable USB memory sticks

You can use a universal USB installer tool to transfer the downloaded NetShark software .iso file to a bootable USB memory stick. For example, in a Microsoft Windows environment, the program Universal-USB-Installer.exe was used to successfully create a bootable USB memory stick in testing. Note: when using Universal-USB-Installer.exe, the Try Unlisted Linux ISO (at the bottom of the list of choices) was selected in Step 1 of the creation process.

Step 3 - Insert the bootable USB memory stick into the system

USB connectors are located on the back of the NetShark chassis. The Model 2170 1U chassis also has USB connectors on the front. Insert the memory stick into any USB connector.

Step 4 - Connect to the console port

If you have not already connected to the console port as part of cabling,

- 1) Connect a laptop or other device to the console connector using the RJ45 to 9-pin D-subminiature cable supplied in the accessory kit and any necessary connector converter. The cable wiring is available under "Specifications" in the *NetShark Quick Start Guide*.
- 2) Set the device's terminal emulator to 9600 Baud, 8 data bits, 1 stop bit, no parity bit, and no flow control.

Step 5 - Configure the BIOS

The default BIOS configuration causes the product to boot the factory-installed software from an internal disk. To boot from an external USB memory stick, you must change the BIOS configuration as follows:

- 1) Use the power switch to power-cycle the system. The power switch is in the upper right corner of the front of the chassis.
- 2) During the POST (power-on self-test) sequence, press F2 to start the BIOS configuration tool.
- 3) On the Advanced menu:
 - Select "USB Configuration" and press Enter.
 - Select "Make USB Devices Non-bootable" and press Enter.
 - Select "Disabled" and press Enter.
 - Press Esc to go back to the previous menu.
- 4) On the Boot Options menu:
 - Select "USB Boot Priority" and press Enter.
 - Select "Enabled" and press Enter.
 - Press Esc and then select "No" and press Enter to go back to the previous menu.
- 5) From the EXIT menu, select "Save Changes and Exit" and press Enter.
- 6) Select "Yes" and press Enter in the resulting screen to save the changes and exit the BIOS configuration tool. The system reboots.

Step 6 - Install the software

When the system finishes booting from your USB memory stick, enter "install" at the prompt.

Software installation requires approximately 20 minutes. After the installation process completes, the USB memory stick can be removed. If it is not removed, the system boots from the USB and presents the "boot" prompt again.

Step 7 - Remove the USB memory stick and power-cycle the appliance

When the software installation has completed and the "boot" prompt is displayed, remove the USB memory stick and power-cycle the appliance. After the system reboots, the login prompt is displayed.

Step 8 - Run the configuration wizard

Open the *NetShark Quick Start Guide* and start at “Configuration” to finish the installation.

