Release Notes:
Version J.08.03 Software
for the ProCurve Secure Routers 7000dl Series

Release J.08.03 supports these routers:

- ProCurve Secure Router 7102dl (J8752A)
- ProCurve Secure Router 7203dl (J8753A)

These release notes include information on the following:

Boot Code Update Recommendations for J.08.03

With any major software update, ProCurve recommends that you update your Boot Code if an update is available. If you are updating to J.08.03 from a software version earlier than J.03.01, a Boot Code update to Boot Code version J.06.06 is required. If you are updating from software version J.03.01 or later, a Boot Code update is recommended, but not required.

The J.06.06 Boot Code image is installed in a separate operation, before loading the J.08.03 software. See page 2 for more information.

Publication Number

Part Number 5991-2124
August 2007B

Applicable Product

ProCurve Secure Router 7102dl	(J8752A)
ProCurve Secure Router 7203dl	(J8753A)

Trademark Credits

Microsoft®, Windows®, and Windows NT® are US registered trademarks of Microsoft Corporation. Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated. Java™ is a US trademark of Sun Microsystems, Inc.

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
http://www.procurve.com

Contents

Software Management

Enhancements

Software Fixes

Known Software Issues and Limitations

Software Management

Software Updates

Check the ProCurve Networking Web site frequently for free software updates for the various ProCurve products you may have in your network.

Downloading Documentation and Software from the Web

You can download software updates and the corresponding product documentation from ProCurve Networking's Web site as described below.

To Download a Software Version:

1. Go to the ProCurve Networking Web site at:

   http://www.procurve.com.

2. Click on **Software updates**.
3. Under **Latest software**, click on **Secure Router 7000dl Series**.

To Download Product Documentation: You will need the Adobe® Acrobat® Reader to view, print, and/or copy the product documentation.

1. Go to ProCurve Networking's Web site at **http://www.procurve.com**.
2. Click on **Technical support**, then **Product manuals**.
3. Click on the name of the product for which you want documentation.
4. On the resulting Web page, double-click on a document you want.
5. When the document file opens, click on the disk icon  in the Acrobat® toolbar and save a copy of the file.

Downloading Software to the Router

Caution

The startup-config file generated by the latest software release is compatible with the same file generated by earlier software releases. HP recommends that you backup your current configuration to compact flash or a TFTP server before performing any software update. See "Saving the Current or Start-Up Configuration to Compact Flash" or "Saving the Current or Start-Up Configuration to a TFTP Server".

ProCurve Networking periodically provides software updates through the ProCurve Networking Web site **http://www.procurve.com**). After you acquire the new software file, use the ProCurve Secure Router GUI, TFTP, XModem, FTP, or compact flash to update the router software. See the *Upgrading SROS Software Configuration Guide* (5991-2123) for instructions and more information.

Notes

Downloading new software does not change the current router configuration. The router configuration is contained in a separate file that can also be transferred, for example, for archive purposes or to be used in another router of the same model.

Saving Configurations While Using the CLI

The router operates with two configuration files:

- **Running-Config File:** Exists in volatile memory and controls router operation. Rebooting the router erases the current running-config file and replaces it with an exact copy of the current startup-config file. To save a configuration change, you must save the current configuration in the running-config file to the startup-config file.
- **Startup-Config File:** Exists in flash (non-volatile) memory and preserves the most recently-saved configuration as the "permanent" configuration. When the router reboots for any reason, an exact copy of the current startup-config file becomes the new running-config file in volatile memory.

You may use the **write memory** command to save changes made to the running-config file to the startup-up config file. Also, the system prompts you to save any unsaved changes when you leave the configuration level.

Saving the Current Configuration as the Start-Up Configuration

When you use the CLI to make a configuration change, the router places the change in the running-config file. If you want to preserve the change across reboots, you must save the change to the startup-config file. Otherwise, the next time the router reboots, the change will be lost.

To save configuration changes while using the CLI:

1. From the Enable prompt enter:

   #**copy running-config startup-config**

2. Verify that the Configuration built message displays, indicating that the download is complete. The current configuration is now saved as the startup configuration file, and the router will execute the file at each power-up.

The current configuration in the running-config file also may be saved to compact flash or a TFTP server as a **.txt** file (to allow it to be opened in a text editor). You also may use the **write memory** command in place of the above steps to save the running configuration after a change.

Saving the Current or Start-Up Configuration to Compact Flash

1. To save a configuration file to compact flash, from the Enable prompt enter:

   #copy <*config-file*> cflash <*filename*>

   where **<*config-file*>** is either **running-config** or **startup-config** and **<*filename*>** is a name that you choose, ending in **.txt.**

2. Verify that the `Percent Complete 100%` message displays, indicating that the download is complete. The current configuration is now saved in compact flash with the specified filename.

Saving the Current or Start-Up Configuration to a TFTP Server

1. To initiate a download of a configuration file to an external TFTP server, from the Enable prompt enter:

   #copy <*config-file*> tftp

   where **<*config-file*>** is either **running-config** or **startup-config.**

2. Enter the IP address of the TFTP server when prompted for the Address of remote host.

3. Enter a filename ending in **.txt** for the saved configuration when prompted for the Destination filename.

All configuration files downloaded from the router should have a .txt extension. Use identifiable names when saving the configuration, such as the name and date, for example, **startup-config-branch-A-042505.txt**.

Managing Router Configurations Remotely

You may not always have direct access to a router, so a console terminal session through the serial port is not possible. The router provides remote console access through Telnet or SSH. However, when using Telnet or SSH to revise the router's configuration, a change could result in loss of network connectivity, without any means of restoring access remotely.

Beginning with software release J.04.01, ProCurve SafeMode solves this problem. When enabled on a router, SafeMode requires a user to periodically reset a reload timer within a specified amount of time. If no reset request is received, the router saves the current, disruptive running configuration to internal flash as **problem-config** and reboots. Once the router reboots, it displays a "reboot cause message" and loads the currently saved **startup-config** file. This startup-configuration file should restore remote access to the router. The user can then review the saved disruptive configuration file, **problem-config**, and correct any problems. For more information, see "SafeMode" in Chapter One of the *Basic Management and Configuration Guide*.

ProCurve Switch, Routing Switch, and Router Software Keys

Software Letter	ProCurve Networking Products
C	1600M, 2400M, 2424M, 4000M, and 8000M
CY	Switch 8100fl Series (8108fl and 8116fl)
E	Switch 5300xl Series (5304xl, 5308xl, 5348xl, and 5372xl)
F	Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324
G	Switch 4100gl Series (4104gl, 4108gl, and 4148gl)
H	Switch 2600 Series, Switch 2600-PWR Series: H.07.81 and earlier, or H.08.55 and greater, Switch 2600-8-PWR requires H.08.80 or greater. Switch 6108: H.07.xx and earlier
I	Switch 2800 Series (2824 and 2848)
J	Secure Router 7000dl Series (7102dl and 7203dl)
K	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, and 5400zl Series (5406zl, 5406zl-48G, 5412zl, and 5412zl-96G)
L	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
M	Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 though M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 though M.08.95, or M.08.99 to M.08.100 and greater.
N	Switch 2810 Series (2810-24G and 2810-48G)
PA/PB	Switch 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)

Software Letter	ProCurve Networking Products
Q	Switch 2510 Series (2510-24)
T	Switch 2900 Series (2900-24G, and 2900-48G)
VA/VB	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
WA	ProCurve Access Point 530
WS	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
numeric	Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.)

Minimum Software Versions for Secure Router 7000dl Modules

ProCurve Secure Router Module	Minimum Supported Software Version
J8451A ProCurve Secure Router 1xT1 Interface Module	J.01.02B
J8452A ProCurve Secure Router 1xT1 + DSX-1 Interface Module	J.01.02B
J8453A ProCurve Secure Router 2xT1 Interface Module	J.01.02B
J8454A ProCurve Secure Router 1xE1 Interface Module	J.01.02B
J8455A ProCurve Secure Router 1xE1 + G.703 Interface Module	J.01.02B
J8456A ProCurve Secure Router 2xE1 Interface Module	J.01.02B
J8457A ProCurve Secure Router 2xISDN BRI S/T dl module	J.04.01
J8458A ProCurve Secure Router 1xSerial Interface Module	J.01.02B
J8459A ProCurve Secure Router 1xADSL2+ Annex A Interface Module	J.01.02B
J8759A ProCurve Secure Router 1xADSL2+ Annex B Interface Module	J.02.01A
J8460A ProCurve Secure Router ISDN BRI U Backup Module	J.01.02B
J8461A ProCurve Secure Router ISDN BRI S/T Backup Module	J.01.02B
J8462A ProCurve Secure Router Analog Modem Backup Module	J.01.02B
J8463A ProCurve Secure Router 8xT1/E1 Wide Module	J.01.02B
J8471A ProCurve Secure Router 7100/7200 IPSec Module	J.01.02B
J9010A ProCurve Secure Router 2xISDN BRI U dl module	J.04.01
J9011A ProCurve Secure Router 8xSerial dl Wide module	J.04.01
J9026A ProCurve Secure Router 7100/7200 IPSec Base Module	J.05.02

Enhancements

Unless otherwise noted, each new release includes the features added in all previous releases.

Release J.02.01 Enhancements

The following enhancements are described in the guides referenced in each enhancement overview. For the latest version of any of these guides, refer to "Downloading Documentation and Software from the Web" on page 1.

Table 1. Summary of J.02.01 EnhancementsSoftware Fixes

J.02.01 Enhancement	Overview
Compact Flash Support	Added capability to copy boot image directly from compact flash to boot sector. Added capability to format compact flash with SROS running. Added capability to boot from a specific file from compact flash. For more information, see **boot config** and **boot system** the section titled "Global Configuration Mode Command Set" in the *SROS Command Line Interface Reference Guide* (April 2005 edition or later).
ADSL Annex B module	Added software support for ADSL Annex B module.
RFC1483 on ADSL/ATM link	Added support for RFC1483 on ADSL/ATM link.
GRE (IP Only)	The current implementation supports IP protocol only. For more information on GRE commands, see the section titled "Tunnel Configuration Command Set" in the *SROS Command Line Interface Reference Guide* (April 2005 edition or later).
HDLC (Cisco)	HDLC is a protocol developed by the International Organization for Standardization (ISO). It is used throughout the world and widely implemented because it supports both half duplex and full duplex communication lines, point to point, and multi-point networks, on both switched or non-switched links. HDLC is designed to permit synchronous, protocol transparent data transmission. HDLC also has many off shoots. Some of these are Synchronous Data Link Control (SDLC) and Link Access Procedure-Balanced (LAP-B), and PPP For more information on HDLC commands, see the section titled "HDLC Command Set" in the *SROS Command Line Interface Reference Guide* (April 2005 edition or later).

J.02.01 Enhancement	Overview (Continued)
Multi-Link Frame-Relay support	Multilink Frame Relay (MFR) for the User-to-Network Interface (UNI) and the Network-to-Network Interface NNI) provides physical interface emulation for frame relay devices. The emulated physical interface consists of one or more physical links, called "bundle links", aggregated together into a single "bundle" of bandwidth. This service provides a frame-based inverse multiplexing function, sometimes referred to as an "IMUX". The bundle provides the same order-preserving service as a physical layer for frames sent on a data link connection. In addition, the bundle provides support for all Frame Relay services based on UNI and NNI standards. For more information, see the *8xT1/E1 Wide Module) Quick Configuration Guide*. Also, see pages 581 and 582 in the section titled "Frame Relay Interface Config Command Set" in the *SROS Command Line Interface Reference Guide* (April 2005 edition).
SNMP Views	Added SNMP Views.For more information, see the **snmp-server view** command in the section titled "Global Configuration Mode Command Set" in the *SROS Command Line Interface Reference Guide* (April 2005 edition or later).
802.1X supplicant mode	Added 802.1X supplicant mode. For more information, see the **port-auth supplicant enable** command in the section titled "Ethernet Interface Configuration Command Set" in the *SROS Command Line Interface Reference Guide* (April 2005 edition or later).
SIP-ALG	Improved the performance through the router.

Release J.02.02A Enhancements

System-Level Enhancement: Default Boot Path Changed

Concurrent with the release of J.02.02A software, ProCurve has changed the default boot path in the ProCurve Secure Router products it builds. Products with the following serial numbers, or later, use compact flash as the primary (default) boot path for the router software and router configuration files.

Table 2. ProCurve Secure Router Serial Numbers That Boot From Compact Flash

Product	Serial Number
ProCurve Secure Router 7102dl (J8752A)	US525TRAP4 or later.
ProCurve Secure Router 7203dl (J8753A)	US522TS252 or later.

The secondary boot path is the router's internal flash memory. Prior to this change, the 7102dl and 7203dl products booted by default from the files installed on internal flash at manufacturing time.

What has changed?

At manufacturing time, two software files are loaded into internal flash: the most recent software and an exact copy of that software, renamed to `SROS.BIZ`.

The default boot path for the software and configuration files is set as follows:

boot system cflash SROS.BIZ flash SROS.BIZ
boot config cflash startup-config flash startup-config

By default, the router tries to boot a file named `SROS.BIZ` from compact flash. If this file or compact flash is not present, the router boots SROS.BIZ from internal flash. In addition, by default, the router tries to use a configuration file named `startup-config` from compact flash. If this file or compact flash is not found, the router uses `startup-config` from internal flash.

Why make this change?

For ease of router deployment. A network administrator can now pre-configure a router using compact flash, without ever physically touching the router. All that is required is a PC equipped with a compact flash reader/writer. First, build a valid `startup-config` file and copy it to compact flash. Next, rename the current software file to `SROS.BIZ` and copy it to compact flash. With these two files loaded on compact flash, a network administrator can drop-ship the compact flash and a router to a remote site. At the remote site, someone inserts the compact flash into the router and attaches the network cables. When finished, the power cord is attached and plugged into a suitable power outlet, powering up the router. The router, by default, uses the software file (`SROS.BIZ`) and configuration file (`startup-config`) on the supplied compact flash to boot the system.

Note

Only routers built with serial numbers in Table 2 on page 7 boot by default from compact flash. Routers with earlier serial numbers can be updated to use compact flash by default. See "Updating Pre-J.02.02A Routers to Boot From Compact Flash" on page 8 for the update instructions.

Updating Pre-J.02.02A Routers to Boot From Compact Flash

ProCurve Secure Routers with serial numbers *below* those in Table 2 on page 7 can be manually configured to use the new default boot path from compact flash. If your router's serial number is later than those shown in Table 2, it already has the new boot path and these instructions can be ignored.

Follow the steps below.

1. Update the router Boot Code to version J.02.02A or later.
2. Load and boot from software version J.02.02A or later.

3. Make any necessary changes to the router's configuration and save the running-config file. You now have a current startup-config file in flash.

   ProCurveSR7203dl>
   ProCurveSR7203dl>enable
   ProCurveSR7203dl#write memory

4. Rename the current software file to `SROS.BIZ`. The file name must be in all capital letters.

   ProCurveSR7203dl#copy flash J02_02A.biz flash SROS.BIZ

5. If you are using compact flash, copy the SROS.BIZ file and the startup-config file to compact flash. If you are not using compact flash, go to step 6.

   ProCurveSR7203dl#copy running-config cflash startup-config
   ProCurveSR7203dl#copy flash J02_02A.biz cflash SROS.BIZ

6. Change the primary boot path to compact flash and the backup to internal flash.

   ProCurveSR7203dl#conf term
   ProCurveSR7203dl(config)# boot system cflash SROS.BIZ flash SROS.BIZ
   ProCurveSR7203dl(config)# boot config cflash startup-config flash startup-config

Release J.03.01 Enhancements

The overviews provided below include pointers to additional information where it is available. For the latest version of ProCurve Secure Router documentation, refer to "Downloading Documentation and Software from the Web" on page 1.

Table 3. Summary of J.03.01 Enhancements

Enhancement	Overview
1:1 NAT Port-translation	Provides translation between a single specific private IP address on the inside network and a single specific public IP address on the outside network.
AutoSynch	Enables fast and efficient deployment or replacement of routers by automatically synchronizing a compact flash software file (**SROS.BIZ**) and a configuration file (**startup-config**) with internal flash. For more information, see the *Updating the Secure Router OS Software Configuration Guide*.
Boot Code Update from CLI	Enables Boot Code updates from the router CLI. Boot Code updates may now be performed from a remote location using a Telnet session. Note: during the Boot Code update process the router ceases to function, that is, it doesn't route once the update has begun and doesn't begin routing again until the Boot Code update is completed.

Enhancement	Overview (Continued)
Class-based Weighted Fair Queuing (CBWFQ)	Allows a user to configure (classify) a specific type of traffic that is put into its own reserved queue or class. Class-based traffic is serviced at a higher priority than plain WFQ traffic but after priority queuing. The classes can be packet matches based on an ACL, an IP precedence or Diffserv priority marking (DSCP), UDP port numbers, or bridged traffic. Up to four specific queues (or classes) are allowed per interface with up to 16 total queues per router. Using the **bandwidth** command, each queue provides a minimum amount of the interface bandwidth needed to support that class of traffic. For more information on CBWFQ, refer to the **match** and **bandwidth** command descriptions in "Quality of Service (QoS) Map Commands" in the *SROS Command Line Interface Reference Guide*.
ECMP (Static Routing and BGP)	Allows proposing up to six BGP or static routes as candidates for multipath routing. Use the **ip load-sharing** command to load share and distribute traffic based on the destination IP or based on a round robin metric for all equal parallel routes (based on administrative distance parameter). For more information, refer to the SROS *Command Line Interface Reference Guide*.
File Copy and Erase Using a Wildcard Character	A wildcard character '*' may now be used in file names to allow groups of files to be copied or erased. For example, from the enable level, the command, **erase flash J02*** removes all files that begin with 'J02' from internal flash.
Multihoming BGP	See "ECMP (Static Routing and BGP)" overview. Note: multihoming BGP is not supported when using NAT.
Real-time Show Commands	Display full-screen output in real time for select **show** commands. Information is continuously updated on the console until you either freeze the data (by pressing the F key) or exit the *realtime* mode (by pressing Ctrl+C). Refer to the **show** commands in the SROS *Command Line Interface Reference Guide* to determine if real-time output is supported.
Secure Copy	Enables secure copy server functionality in the router, providing an encrypted and authenticated method of transferring files, based on the Berkeley r-tools. SSH (Secure Shell) is used for the secure channel. For more information, see the **ip scp server** command in the *SROS Command Line Interface Reference Guide*.
Show Modules Command	Displays a list of the modules currently installed in the router.
Show Tech Command	Creates a file, **showtech.txt**, located in flash memory, containing system information collected from various **show** commands. As an option, the command output can be displayed on the terminal, using the **show showtech terminal** command. In addition, the contents of this file may be viewed using the **show file flash showtech.txt** command. For information on the **show** commands processed to create the output, refer to the SROS *Command Line Interface Reference Guide*.
SNMP Bridge MIB (RFC 1493)	Adds support for the Bridge MIB (in RFC 1493) with the following OID exceptions: BRIDGE-MIB.dot1dTpPortMaxInfo, BRIDGE-MIB.dot1dTpPortInFrames, BRIDGE-MIB.dot1dTpPortOutFrames, BRIDGE-MIB.dot1dTpPortInDiscards
Traffic Shaping and QoS for Ethernet Interfaces	Enables QoS to be applied to VLAN and Ethernet interfaces with traffic shaping applied to them. The bandwidth used for outgoing traffic on an interface is limited, like the rate limiter on QoS Map entries, except that it queues packets instead of deleting them. For more information, see the **bandwidth** command in "Ethernet Interface Configuration Command Set" in the *SROS Command Line Interface Reference Guide*.
Web Browser Interface Revisions	A new QoS wizard is available to allow easy setup of LLQ on a WAN interface. Also, existing wizards have been enhanced. These tools are self-documented and available in the router's Web browser interface.

Release J.04.01 Enhancements

The overviews provided below include pointers to additional information where it is available. For the latest version of ProCurve Secure Router documentation, refer to "Downloading Documentation and Software from the Web" on page 1.

Table 4. Summary of J.04.01 Enhancements

Enhancement	Overview
Dial on Demand Routing	Manages a backup connection so that when traffic needs to be sent and the primary interface is unavailable, the ProCurve Secure Router establishes the dial-up connection. Demand routing also ensures that when the dial-up connection is idle for the amount of time you specify, the ProCurve Secure Router terminates the call. For more information, refer to Chapter Eight "Configuring Demand Routing for Primary ISDN Modules" in the *Basic Management and Configuration Guide*.
ECMP for OSPF	ECMP for OSPF is now supported. For more information, refer to "Configuring Load Sharing" in Chapter Thirteen of the *Advanced Management and Configuration Guide*.
Global Password Encryption	You can now enter one command, **service password-encryption,** to encrypt all the passwords configured on the ProCurve Secure Router, including the passwords configured for Telnet and console access. For more information, refer to "Encrypting All the Passwords Configured on the Router" in Chapter Two of the *Basic Management and Configuration Guide*.
Policy Based Routing	Enables different types of traffic to travel over different paths, even when the traffic is destined to the same network. You can configure your ProCurve Secure Router to route a packet according to its: • IP precedence value • DiffServ value • source IP address • source and destination IP addresses • application data (source and destination ports) • payload size For more information, refer to Chapter Thirteen "IP Routing—Configuring RIP, OSPF, BGP, and PBR" in the *Advanced Management and Configuration Guide*.
ProCurve SafeMode	Allows a user to perform configuration changes in "config" mode without the fear of being disconnected during a Telnet or SSH session and losing access to the router. When enabled, SafeMode requires the user to periodically reset a reload timer within a specified amount of time. If no reset request is received, the router will save the current disruptive running configuration to internal flash as "problem-config" and reboot. Once the router has rebooted, it will display a reboot cause message and load the currently saved startup-configuration file, restoring access to the router. For more information, see "SafeMode" in Chapter One of the *Basic Management and Configuration Guide*.
Protocol Independent Multicast-Sparse Mode (PIM-SM)	Provides a a multicast routing protocol that allows multicast packets received from one network to be routed to hosts in different networks. Working with whatever unicast routing protocols the routers implement, PIM-SM allows routers in a PIM domain to construct a shared, unidirectional tree for each multicast group active in the network. The shared tree is rooted at a rendezvous point (RP) router, which is the router responsible for drawing multicast traffic from a new source to receivers in the associated group. For more information, refer to Chapter Eleven "Configuring Multicast Support with PIM-SM" in the *Advanced Management and Configuration Guide*.

Enhancement	Overview (Continued)
TACACS+ (AAA)	Provides support for authentication, authorization, and accounting (AAA) using a TACACS+ server. For more information, refer to "Configuring the TACACS+ Server" in Chapter Two of the *Basic Management and Configuration Guide*.

Release J.05.02 Enhancements

The overviews provided below include pointers to additional information where it is available. For the latest version of ProCurve Secure Router documentation, refer to "Downloading Documentation and Software from the Web" on page 1.

Table 5. Summary of J.05.02 Enhancements

Enhancement	Overview
IPSec Base Module (J9026A) Support	The ProCurve Secure Router 7100/7200 IPSec Base Module supports the industry standard for VPNs, IP Security (IPSec). As a result, it enables both site-to-site and client-to-site VPNs. With this module installed, you can create VPN site-to-site connections between routers, with up to 10 tunnels. If VPN client connectivity is required, the ProCurve VPN Client is available for purchase. Any pure IPSec client can connect to the router, however, VPN clients with proprietary implementations will not work with the ProCurve Secure Router 7100/7200 IPSec Base Module. Installing this module activates software encryption/decryption and security services for IPSec VPNs in the router. The following software security services in the main processor are enabled: • DES • triple-DES (3DES) • AES • SHA-1 • MD5 • random number generation
CBWFQ Priority Percent Command	Priority queues are intended for constant bit rate traffic. The **priority percent <*percent*>** command specifies the bandwidth allocated to the priority queue on the interface, based on a percentage of the total bandwidth available. For more information, refer to "Priority Command" in the *Understanding SROS Priority Queuing, Class-Based WFQ, and QoS Maps Configuration Guide*.
Fixed (Static) Multicast Routing Support	Use the **ip mcast-stub fixed** command to allow forwarding of multicast traffic on a selected interface (Ethernet, ATM, Demand, Frame Relay, HDLC, Loopback, PPP, and Tunnel) after enabling multicast routing. For more information, refer to the *SROS Command Line Interface Reference Guide*.
RIP Filters	Use the **distribute-list** command to add RIP filtering functionality by assigning inbound and outbound access lists on either a global, per logical interface or type-of-route basis. Only one inbound/outbound pair of access lists can be configured for a particular interface. For more information, refer to the *SROS Command Line Interface Reference Guide*.

Enhancement	Overview (Continued)
Web Browser Interface Updates	New and revised screens are summarized below: • System Summary (revised)—information is refreshed every five seconds; additional system information is displayed, including the File System. Selecting **File System** displays the contents of Flash memory. • ISDN Group (new)—configures and manages ISDN groups, required when configuring demand routing for a primary ISDN connection. • Demand Routing (new)—configure and manage demand routing for dial-up connections. • SNMP (new)—configure and manage SNMP settings. • Additional status information displayed for a selected interface. Refreshed every five seconds (updated). • Event Logging (new)—enable the router's event history and set the priority level. Also set email and syslog forwarding and view event history.
New Interface Range Command	The interface range command, **interface range [e1 | t1] <*slot*>/<*port-port*>**, allows multiple E1 or T1 interfaces to be configured at the same time. The interfaces you want to configure must be contiguous ports on the same module. If you have a ProCurve Secure Router 7203dl with an octal E1 or T1 module, you can configure up to eight E1 or T1 interfaces with the same settings (such as *tdm-groups* and *timeslots*).For more information, refer to the *SROS Command Line Interface Reference Guide*.
New Debug Commands	Additional debug commands have been added. For more information, refer to the *SROS Command Line Interface Reference Guide*.
New Show Commands	**show frame-relay multilink fragment interface frame-relay <*number.subinterface*>** — Displays information about multilink Frame-Relay interfaces that support fragmentation. **show ip policy-class host-session** — Displays maximum number of sessions allowed and the number of active sessions currently open. **show isdn-group <*number*>** — Displays settings configured for the ISDN group used for demand routing. **show sip resources** — Displays information about SIP resources. **show sip statistics** — Displays SIP statistics. For more information, refer to the *SROS Command Line Interface Reference Guide*.

Release J.06.03 Enhancements

The overviews provided below include pointers to additional information where it is available. For the latest version of ProCurve Secure Router documentation, refer to "Downloading Documentation and Software from the Web" on page 1.

Table 6. Summary of J.06.03 Enhancements

Enhancement	Overview
Debug Information in Web Browser Interface	Access to debug output is now available in the Web browser interface, in the **Utilities** section. Note: enabling debugging can impact the routers performance.

Enhancement	Overview (Continued)
FTP and TFTP Enhancements	FTP Server default file-system—a user can specify the file-system (FLASH/CFLASH) FTP will use when performing file uploads or downloads. TFTP server—may be configured to overwrite existing files For more information, refer to the *SROS Command Line Interface Reference Guide*.
HTTP Filtering	Allows URL filtering to be applied to incoming or outgoing sessions on any IP interface. Integrates with Websense Enterprise content filtering server to permit or deny HTTP requests. Websense service can allow a Web session to continue, or it can block the URL giving the router a blocked page message to forward back to the Web browser via an HTTP redirect. Multiple content filter servers can be configured for redundancy purposes.The ProCurve Secure Router's Web content filtering capabilities require your network to have a Websense Security Suite solution (version 6.1.1 or later) that includes Websense Enterprise. For more information, refer to Chapter 7, "Content Filtering" in the *Secure Router 7000 dl Advanced Management Configuration Guide*.
ipNetToMedia Table Support	It is now possible to poll the **ipNetToMedia** table (a mapping of MAC-address to IP-address) with SNMP.
IPsec	Added the capability to configure antireplay window size and display out-of-sequence errors on inbound ESP SA's. For more information, refer to the *SROS Command Line Interface Reference Guide*.
Network Monitor	Provides Layer 3 network connectivity and performance testing through the use of ICMP ping probes, TCP connect probes, and HTTP probes. The results of these probes can be used to perform specific actions, such as the removal of routes from the route table to initiate a demand routing backup connection. For more information, refer to Chapter 9, "Network Monitoring" in the *Secure Router 7000 dl Advanced Management Configuration Guide*.
SNMPv3 Support	Secures SNMP management through addition of authentication and encryption. For more information, refer to "Using SNMP to Manage the ProCurve Secure Router" in Chapter 2 of the *Secure Router 7000 dl Basic Management Configuration Guide*.
SNTP Client and Server	The SNTP (Simple Network Time Protocol) Client uses SNTP to obtain time settings from an NTP (Network Time Protocol) server. The SNTP Server responds to SNTP Client requests for time settings. The SNTP Server only responds if time settings have already been received from a valid NTP server via the SNTP Client. In order to respond to Client requests, the SNTP Server must also have the SNTP Client configured. For more information, refer to "Enabling the SNTP Server on the ProCurve Secure Router" in Chapter 1 of the *Secure Router 7000 dl Basic Management Configuration Guide*.
TACACS+ Enhancements	New capabilities are summarized below: • Connection accounting - send accounting records for outbound Telnet connections. • Exec accounting - send accounting records for new connections or logins. • Exec authorization - allows users to enter directly into 'enabled' mode for new CLI sessions. For more information, refer to Chapter 2, "Controlling Management Access to the ProCurve Secure Router" in the *Secure Router 7000 dl Basic Management Configuration Guide*.

Release J.06.06 Enhancements

The overviews provided below include pointers to additional information where it is available. For the latest version of ProCurve Secure Router documentation, refer to "Downloading Documentation and Software from the Web" on page 1.

Table 7. Summary of J.06.06 Enhancements

Enhancement	Overview
VPN Wizard and Firewall Wizard support IE7	These wizards may be used when using Internet Explorer 7 to access the router's Web browser interface
Support for 2007 US Daylight Saving Time	When **auto-correct-DST** is enabled, the router changes to daylight saving time following the new rules for 2007.

Release J.08.03 Enhancements

The overviews provided below include pointers to additional information where it is available. For the latest version of ProCurve Secure Router documentation, refer to "Downloading Documentation and Software from the Web" on page 1.

Table 8. Summary of J.08.03 Enhancements

Enhancement	Overview
31–Bit Prefixes on IPv4 Point-to-Point Links (RFC 3021)	Added support for 31-bit prefixes on point-to-5point links, per RFC 3021. Note: Both sides of the point-to-point link must support RFC 3021 to work properly. See example on page 19.
Redistribution Between BGP and Static OSPF and Static RIP Routes	Static, connected, OSPF and RIP routes may be redistributed into and out of BGP. See example on page 19.
Concurrent Bridging and Routing	Bridge non-IP traffic and route IP traffic simultaneously on the same interface. Appletalk, IPX, and SNA traffic can be bridged across the IP link. See See "Integrated Routing and Bridging (IRB)" on page 16.
Configurable Administrative Distance in OSPF and RIP	From router configuration mode, the **distance** command may be used to change the OSPF and RIP administrative distances from their default values.
Crypto Map Idle-timeout for Receive Data	VPN tunnels may be torn down before the expiration of the tunnel's hard lifetime, using the VPN Idle-Time option. If no data is received from a VPN peer within the time specified by the idle-time, the tunnel is torn down. Any routes added to the IP route table by Reverse Route Injection also will be removed from the route table. From Crypto Map Config Mode, an Idle Time may be configured with the command **set security-association idle-time <*idle-time*>**. Note: the ***idle-time*** value is measured in seconds.
DHCP Client Support for 802.1Q Ethernet Sub-interfaces	802.1Q encapsulated Ethernet sub-interfaces can now obtain IP addresses via DHCP.

Enhancement	Overview (Continued)
Enable/Disable ACL Entries Using Tracks	Access Control List entries may now be controlled by tracks by appending the **track <*track-name*>** keywords to the end of **permit** or **deny** statements. This is available for both Standard and Extended ACLs. When coupled with Schedule updates, this supports time-based ACLs.
Enhanced VPN **Show** Commands	Added support for four additional **show** commands that display security associations (SAs) used with VPNs. • show crypto ike sa address • show crypto ike sa policy • show crypto ike sa remote-id • show crypto ipsec sa remote-id
Fast Forwarding Engine (FFE) supports Policy-based Routing (PBR)	Fast Forwarding Engine (FFE) can now be used on interfaces with policy routes.
Global Schedule Extensions	• Absolute schedules can be used to influence the behavior of Network Monitor Tracks during specific time periods. • Periodic schedules can be used to influence the behavior of Network Monitor Tracks during recurring time periods, for example, every Monday from 7:00 AM to 5:00 PM. • Relative Time Schedules may be used in conjunction with Network Monitor Tracks to define times for which a Track should be put into a PASS state, regardless of the state of probes associated with the Track. Relative Times are particularly useful when routers are rebooted, to bypass Track actions until routers complete the boot-up process and Network Interfaces are fully initialized See example on page 19.
Integrated Routing and Bridging (IRB)	IRB allows IP traffic to be bridged between interfaces and, optionally, routed to others. Previously, IP traffic could be bridged or routed between interfaces, but IP bridging and IP routing could not be enabled on a single device simultaneously. See example on page 20.
IP Directed Broadcast Support	Added support for directed broadcast of IP packets. Without this feature enabled, packets destined for the broadcast IP address of any interface connected to a router will be dropped. With directed broadcast enabled on an interface, such packets are forwarded to the broadcast Ethernet MAC address (FF:FF:FF:FF:FF:FF) for all devices on that network segment. Note: Enabling directed broadcasts on router interfaces may introduce security holes. Several well-known Denial of Service attacks are possible when directed broadcasts are enabled on Ethernet segments. ProCurve recommends that Access Lists be used in conjunction with directed broadcast when this feature is used. Directed broadcasts are disabled on all interfaces by default. See example on page 21.
IPsec Crypto Maps can now be enabled/ disabled by a track	Crypto maps can now be enabled or disabled with tracks. This is useful in scenarios where multiple VPN Gateways may be used to reach the same remote private network. See example on page 22.

Enhancement	Overview (Continued)
Network Address Translation	Added support for NAT Source Port Preservation. When Source Port Preservation is enabled, the router attempts to use the same source port after NAT as the originating device used prior to NAT. This feature can be enabled with the command **ip firewall nat-preserve-source-port**. NAT allocates source ports on public interfaces on a first-come, first-serve basis, so if two devices attempt to use the same source port at one time, one session's source port will be translated by NAT. By default, the same is true when one device attempts to establish two or more simultaneous sessions using the same source port. This behavior can be changed only for cases where one device attempts to establish multiple sessions using the same source port (and cannot be changed when two or more devices do so) with the command **ip firewall nat-preserve-source-port record-source-addres**s. Note: Basic preservation is enabled by default. Source address recording is not enabled by default, as it is commonly unnecessary and consumes more memory than basic preservation.
Network Monitor Track Control Timers	• Probe Pass/Fail Tolerance: Users may now specify different tolerance values to put probes into the PASS state or the FAIL state. This is useful for users who wish to only use a link if it is very reliable; for example, if the probe should pass only after 5 consecutive successes, but fail after only 2 failures, the Probe Config Mode command 'tolerance consecutive pass 5 fail 2' would be used. • Increased Number of Track Test Objects: The number of probes that can be tested by a single Track has been increased from 2 to 60,000. • Multiple Track Test Objects: Schedules may now be tested in addition to probes. • Inverse Track Test Logic: Tracks can now be put into a PASS state when a test fails, using the 'not' keyword. • Weighted Track Test Logic: Users may now assign weights to test objects, putting the Track into either a PASS or FAIL state based on the cumulative weight of all objects. See example on page 23.
Octal T1/E1 Supports Multiple HDLC's Per Interface (256 Total)	256 logical interfaces per Octal T1/E1 Module are now supported. This eases implementations of point to multipoint leased-line applications, where fractional T1s at remote locations may be DACSed to one or more full T1s at a host location. See example on page 24.
Quality of Service	• QoS Maps can now match DSCP aliases. Rather than inputting decimal values, such as "46," alias strings, such as "if," can be used. • Added a fifth queue for Class Based Weighted Fair Queuing (CBWFQ)
Route Map Control of Redistribution Between Routing Processes	Added support for route-map control of redistribution between routing processes. See redistribute command. See example on page 24.
Route Tagging for Internal Filtering (allows dynamic insertion of VPN RRI Routes)	Route tags give users accurate and easy control over redistribution between routing protocols. Users may assign tags to static routes and routes inserted into the routing table via VPN Reverse Route Injection (RRI). Additionally, routes learned via BGP have tags associated with them and are set to the AS number of the last Autonomous System in the path to the destination network. See example on page 25.
Sending Internet Key Exchange (IKE) Initial Contact	Added support for IKE Initial Contact message during establishment of IKE tunnels. In the event that a router loses power or is rebooted while an IKE tunnel is established, it is possible that the other router will not know that the tunnel is down. When the router comes back online and attempts to establish a tunnel to the other router, using the IKE Initial Contact message, the other router will delete any existing Security Associations. This saves memory and improves performance on the other router. Note: IKE Initial Contact is supported by default and does not require any user configuration.

Enhancement	Overview (Continued)
SMTP Authentication	SMTP authentication for outgoing system-generated e-mails (e-mail logging) is now supported. The command **logging email receiver-ip <*e-mail server address*> auth-username <*username*> auth-password <*password*>** is used to configure authentication.
SNMP Packet Debugging	Added the ability to debug SNMP packets with the command **debug snmp packets**.
SSLv3 / TLS 1.0 Support in Web Browser Interface	The Web browser interface now supports SSLv3 / TLS 1.0 for HTTPS connections.
Support for Diffie-Hellman Group 5	Added support for Diffie-Hellman Group 5, for use with IKE policies and IPSec Perfect Forward Secrecy (PFS).
Tab-Completion of Filenames	Added tab completion of filenames in **show** and **copy** commands.
User Interface	• boot config' commands that allows user to specify a particular file to use for config restore (instead of startup-config file) • UTF-8 support in CLI
User-configurable H.323 ALG Timeout for Call Control Association	Users may now configure the timeout value for H.323 signaling policy sessions. The default value is 8 hours.
'VLAN-aware' Bridging on Frame-Relay and HDLC	Virtual Local Area Network (VLAN) tagged packets can be transparently transmitted across bridged HDLC and Frame Relay links by adding the **bridge-group <value> vlan-transparent** command to applicable interfaces. See example on page 26.
VPN Reverse Route Injection (with static route tags)	Reverse Route Injection (RRI) allows a router to add remote VPN networks to its route table when the VPN tunnel is up. By adding the route to its local route table, the router can then redistribute the route into a routing protocol, so that other routers can dynamically learn how to reach the remote network. This is useful when setting up redundant VPN gateways at a host site, which is connected to by multiple remote sites. See example on page 26.

New Feature Examples

This section contains examples of selected features listed in Table 8 on page 15. See the latest version of the *ProCurve Secure Router dl Command Line Interface Reference Guide*, available on the ProCurve Web site, for more information.

31–Bit Prefixes on IPv4 Point-to-Point Links (RFC 3021)

To work properly, both sides of the point-to-point link must support RFC 3021.

Example:

```
!Router A Configuration
interface ppp 1
ip address 192.168.1.0 255.255.255.254

!Router B Configuration
interface ppp 1
ip address 192.168.1.1 255.255.255.254
```

Redistribution Between BGP and Static OSPF and Static RIP Routes

Example:

```
router bgp 65000
redistribute rip
! Output omitted
!
router rip
redistribute bgp
! Output omitted
```

Global Schedule Extensions

Example Absolute Schedule:

```
schedule S
 absolute start 17:00 30 april 2007 end 07:00 5 may 2007
 no shutdown
```

Example Periodic Schedule:

```
schedule T
 periodic weekday 08:00 to 17:00
 no shutdown
```

Example Relative Schedule:

```
schedule MY-SCHEDULE
relative start-after 120
! The schedule will be put into an INACTIVE state for 120 seconds
! after this command is entered. Accounting for the boot-up process,
! this also means that it will be INACTIVE for the first 120 seconds
! after boot-up.
!
probe MY-PROBE icmp-echo
destination 10.5.2.222
period 15
tolerance consecutive fail 2
no shutdown
!
track MY-TRACK
test probe MY-PROBE
time-schedule MY-SCHEDULE
! The Track will be put into a PASS state while the Schedule is INACTIVE.
! When the Schedule is ACTIVE, the Track's PASS/FAIL state is tied to
! the state of the associated Probe's PASS/FAIL state.
no shutdown
```

Integrated Routing and Bridging (IRB)

As an example, consider a network requirement to bridge IP traffic between two sites that are connected via a T1/PPP link, while simultaneously routing traffic destined to the Internet over a second Ethernet interface at the host site.

Main Site:

```
ip routing
!
bridge irb
bridge 1 protocol ieee
!
int bvi 1
 ! BVI Interface ID is the same as the Bridge Group
 ip address 192.172.1.1 255.255.255.0
 ! This IP address is the default gateway for hosts at both sites
 no shutdown
!
int eth 0/1
 bridge-group 1
 ! All traffic not intended for 192.172.1.1 will be bridged to PPP 1
!
```

```
int ppp 1
 bridge-group 1
 !  All traffic not intended for 192.172.1.1 will be bridged to Eth 0/1
!
int eth 0/1
 ip address 1.1.1.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 1.1.1.254
```

Remote Site:

```
no ip routing
!  The remote site does not need to bridge and route simultaneously,
!  so IP routing is disabled
!
bridge 1 protocol ieee
!
int eth 0/1
 bridge-group 1
!
int ppp 1
 bridge-group 1
```

IP Directed Broadcast Support

Example:

```
int eth 0/1
ip address 10.19.235.43 255.255.255.0
ip directed-broadcast
! All directed broadcasts – ie, 10.19.235.255 – will be forwarded
!
int eth 0/2
ip address 172.16.1.1 255.255.255.0
ip directed-broadcast SECURE
! Only directed broadcasts permitted by the ACL "SECURE" are forwarded
!
ip access-list extended SECURE
permit ip 192.168.1.0 0.0.0.255 172.16.1.255 0.0.0.0
! Directed broadcasts from the 192.168.1.0 /24 network are permitted.
! All other directed broadcasts will be discarded.
```

IPsec Crypto Maps can now be enabled/disabled by a track

This feature is useful where multiple VPN Gateways may be used to reach the same remote private network.

Example:

```
probe PRIMARY-VPN-PING icmp-echo
destination 1.1.1.1
! Primary VPN Gateway Public IP is 1.1.1.1
period 15
tolerance consecutive fail 2
no shutdown
!
track PRIMARY-VPN-TRACK
test probe PRIMARY-VPN-PING
no shutdown
!
ip crypto
!
crypto ike policy 100
! This is the Primary VPN Gateway to the host private network
initiate main
respond anymode
local-id address 100.100.100.100
peer 1.1.1.1
attribute 1
encryption 3des
hash md5
authentication pre-share
!
crypto ike policy 200
! This is the Secondary VPN Gateway to the host private network
initiate main
respond anymode
local-id address 100.100.100.100
peer 2.2.2.2
attribute 1
encryption 3des
hash md5
authentication pre-share
!
crypto ike remote-id address 1.1.1.1 preshared-key 123456789012 ike-policy 100
crypto map VPN 10 no-mode-config no-xauth
!
crypto ike remote-id address 2.2.2.2 preshared-key 123456789012 ike-policy 200
```

```
crypto map VPN 10 no-mode-config no-xauth
!
crypto ipsec transform-set esp-3des-esp-md5-hmac esp-3des esp-md5-hmac
mode tunnel
!
crypto map VPN 10 ipsec-ike
description PRIMARY-VPN-GATEWAY
match track PRIMARY-VPN-TRACK
! If the specified Track is in a FAIL state, this peer is not be used, and the router
! moves on to the next crypto map entry (crypto map VPN 20)
match address VPN-10-vpn-selectors
set peer 1.1.1.1
set transform-set esp-3des-esp-md5-hmac
ike-policy 100
crypto map VPN 20 ipsec-ike
description CORPORATE
match address VPN-10-vpn-selectors
set peer 2.2.2.2
set transform-set esp-3des-esp-md5-hmac
ike-policy 200
!
interface ppp 1
ip address 100.100.100.100 255.255.255.252
crypto map VPN
!
ip route 0.0.0.0 0.0.0.0 ppp 1
```

Network Monitor Track Control Timers

Example Using Weighted Track Test Logic:

```
track T
 test list weighted
   if probe A weight 100
   ! When the probe is in a PASS state, it will contribute a weight of 100
   ! to the total weight of the test.
   if probe B weight 100
   if probe C weight 100
   threshold 100
   ! When the  combined weight of the three probes under test is equal to
   ! or greater than 100, the track is in a PASS state.  When the combined
   ! weight is less than 100, the track is in a FAIL state.
```

Octal T1/E1 Supports Multiple HDLC's Per Interface (256 Total)

Point-to-multipoint leased-line applications, where fractional T1s at remote locations may be DACSed to one or more full T1s at a host location, are supported using this feature.

Example:

```
interface t1 1/1
tdm-group 1 timeslots 1-6
tdm-group 2 timeslots 7-12
tdm-group 3 timeslots 13-18
tdm-group 4 timeslots 19-24
!
interface ppp 1
bind 1 t1 1/1 1 ppp 1
!
interface ppp 2
bind 2 t1 1/1 2 ppp 2
!
interface ppp 3
bind 3 t1 1/1 3 ppp 3
!
interface ppp 4
bind 4 t1 1/1 4 ppp 4
```

Route Map Control of Redistribution Between Routing Processes

Example:

```
interface eth 0/1
ip address 10.19.235.43 255.255.255.0
no shutdown
!
!
interface eth 0/2
encapsulation 802.1q
no shutdown
!
interface eth 0/2.10
vlan-id 10
no shutdown
ip address 172.16.10.1 255.255.255.0
!
interface eth 0/2.11
vlan-id 11
no shutdown
```

```
ip address 172.16.11.1 255.255.255.0
!
interface eth 0/2.12
vlan-id 12
no shutdown
ip address 172.16.12.1 255.255.255.0
!
router ospf
network 10.19.235.0 0.0.0.255 area 0
redistribute static route-map STATIC-TO-OSPF
!
route-map STATIC-TO-OSPF permit 10
match ip address STATIC-ACL
! The ACL "STATIC-ACL" defines which networks will be redistributed
!
ip access-list standard STATIC-ACL
permit 192.168.1.0 0.0.0.255
! We will redistribute 192.168.1.0 /24 into OSPF
deny 192.168.0.0 0.0.255.255
! We will not redistribute any other 192.168.0.0 /16 network
permit any
! We will redistribute all other static routes into OSPF
!
ip route 192.168.1.0 255.255.255.0 172.16.10.254
ip route 192.168.0.0 255.255.0.0 172.16.11.254
ip route 10.0.0.0 255.255.255.0 172.16.12.254
```

Route Tagging for Internal Filtering (allows dynamic insertion of VPN RRI Routes)

Example:

```
ip route 192.168.254.0 255.255.255.0 ppp 1 tag 10
!  This associates tag 10 with the static route to 192.168.254.0 /24
!
route-map REDISTRIBUTE permit 10
 match tag 10
 !  This matches all routes in the route table associated with tag 10
!
router ospf
 redistribute static route-map REDISTRIBUTE
 !  Because of the route map configuration, static routes with tag 10 are
 !  redistributed into OSPF.  Other static routes are not.
```

'VLAN-aware' Bridging on Frame-Relay and HDLC

Example:

```
interface eth 0/1
bridge-group 1 vlan-transparent
! 802.1q is not required on Ethernet interfaces when VLANs are transparently
! bridged to WAN interfaces, even if the connected switch has 802.1q
! encapsulation enabled.
!
interface eth 0/2
bridge-group 2 vlan-transparent
!
interface hdlc 1
bridge-group 1 vlan-transparent
!
interface frame-relay 1.16
bridge-group 2 vlan-transparent
```

VPN Reverse Route Injection (with static route tags)

Example:

```
interface eth 0/1
bridge-group 1 vlan-transparent
! 802.1q is not required on Ethernet interfaces when VLANs are transparently
! bridged to WAN interfaces, even if the connected switch has 802.1q
! encapsulation enabled.
!
interface eth 0/2
bridge-group 2 vlan-transparent
!
interface hdlc 1
bridge-group 1 vlan-transparent
!
interface frame-relay 1.16
bridge-group 2 vlan-transparent
```

Software Fixes

Software fixes are listed in chronological order, oldest to newest. To review the list of fixes included since the last general release that was published, go to "Release J.06.06" on page 31.

Unless otherwise noted, each new release includes the software fixes added in all previous releases.

Series switches.Release J.01.02B was the first software release for the ProCurve Secure Router 7000dl Series.

Release J.02.01

Problems Resolved in Release J.02.01

- Fixed buffer overflow in https server that caused a reboot.
- Fixed OSPF not observing path-type when doing route selection.
- Fixed minor issues related to compact flash.
- Fixed a default configuration issue that occurred with ADSL / PPPoE overwriting the default route.
- Fixed E1+G.703 **ts16,** once configured, does not show in **show config** output.
- Fixed **terminal line length**, once set to zero, cannot be set to anything else again.
- WFQ in WEB changed to be enabled by default

Release J.02.02A

Problems Resolved in Release J.02.02A

- (none) — Added capability of configuring the Bundle ID for an MFR bundle.
- 28428 — Allow setting the path to the software image (operating system) to a file that does not exist.
- 28183 — Changed rate-limiting algorithm to prevent a huge burst of traffic after periods of inactivity.
- 28429 — Changed **wr mem** to write to either primary or secondary configuration file, depending on boot settings.
- 28567 — Changed **FIN** timeout in firewall.

- 26893 — Fixed issue where over 73K TCP firewall sessions were causing reboots.
- 27014 — Fixed issue where deleting a bridge could cause sluggish performance.
- 27088 — Fixed issue where the incorrect VPN Mode-Config address was displayed.
- 27124 — Fixed issue where the Media Type in SDP of the SIP Invite message was getting modified with random numbers.
- 27281 — Fixed issue where DHCP relay was not working across VLANs.
- 27315 — Fixed issue where the unit would reboot when the command show run was entered if the configuration contained DHCP server pool options.
- 27324 — Fixed issue where the bandwidth command for a GRE tunnel interface was not being displayed in the **show run** output and was not getting saved to the startup script.
- 27352 — Fixed problem with incorrect NTP server in running config.
- 27372 — Fixed issue where a TDM group could not be assigned to a Dual E1 module.
- 27407 — Fixed issue on the 7203/7102 where runt ARP packets were being sent by the unit.
- 28957 — Fixed connection / binding problem with HDLC and Serial interface.
- 27964 — IPCP will not negotiate to Juniper router. The symptom would be non-interoperability with Multilink PPP.
- 28373 — Protocol stack enhancements.
- 27573 — SNMP OID cleanup.

Release J.03.01

Problems Resolved in Release J.03.01

- 29068 — Added support for secondary IP address on 802.1Q sub-interfaces.
- 28464 — BOOTP relay agent doesn't forward DHCP NAK BOOTREPLY's.
- 28760 — **debug system** doesn't log any SSH login events (pass, fail or otherwise).
- 27391 — Deleting a PPPoE interface that is up will reboot the unit.
- 27624 — **no debug ip ospf hello** command not available.
- 25422 — **no router bgp** didn't exist.
- 28951 — Reboot occurs when deleting tunnel interface when the tunnel is up.
- 27274 — Router will let user bind a physical layer interface to two layer 2 protocols.

- 27827 — **show interface adsl 1/1 version** and **show interface adsl 1/1 information** commands are broken.
- 29733, 29751 — **show interface BRI *x/x*** shows interface as up although interface is down.
- 29370 — **show modules** does not currently report product numbers.
- 27511 — **test-pattern insert** and **show test-pattern** should not be allowed with 1's and 0's pattern.
- 29496 — VPN and firewall security association tracking problems with bad physical layer link. Added sequence numbers to SPI message exchange.
- 29645 — Web browser interface: Physical T1 interfaces do not show correct setting for DS0s.

Release J.04.01

Problems Resolved in Release J.04.01

- 29641 — Corrected message in regards to upgrading Boot-ROM
- 31273 — DHCP option 2 is now formatted correctly.
- 29525 — Ethernet LED behavior fixed.
- 28206 — OSPF redistribute metric-type will check for valid entry.

Release J.05.02

Problems Resolved in Release J.05.02

- 32154 — BRI Channel Staying Active When Interface Shuts Down.
- 34307 — Can't set **priority unlimited** under a QoS map until you set the priority to something else first.
- 33227 — Configuring serial-mode eia530 on a Serial NIM appears as x21 in **show run.**
- 31780 — DR: command **show demand resource pool** <cr> output format.
- 31950 — DR: Connect-sequence recovery is always enabled after a reboot.
- 32155 — DR: Demand Interface using legacy BRI module will not connect to Cisco AS5300.
- 31809 — DR: LLDP tx'd on demand interface even when configured for **no lldp send-and-receive**.
- 31694 — DR: Reboot by **show int** command

- 30953 — DR: **Show int demand X** displays `bandwidth= 0 Kbs` with calls connected with a dual ST card. Works with legacy cards.
- 29598 — **Erase CFLASH SROS.BIZ** causes an AutoSynch message `AutoSynch: startup-config not synched.`
- 31822 — Ethernet sub-interfaces always have an operational status of active/up.
- 31383 — GRE: Debug tunnel interface shows bogus IP address.
- 31094 — if you run out of space on a linux scp, the transfer looks like it worked.
- 31789 — MFR: Configuring a long BID reboots the uni.t
- 34138 — OSPF MD5 authentication does not work to a Cisco router.
- 31667 — OSPF MP: Cannot clear all multipath routes to a network by using the **clear ip route A.B.C.D** command.
- 31665 — OSPF MP: **show ip route summary** counts sometimes shows negative counts.
- 31658 — OSPF MP: With multipath enabled, type E2 routes (static redistributed) do not show up as multiple paths.
- 31479 — PBR: Does not Properly Route when Firewall is Enabled.
- 31392 — RIP Timeout Timer: Range or range checking is invalid.
- 31849 — Router reboots if command **no ip add** is entered in a ppp interface that is up.
- 32690 — Spanning-tree priority value does not store after reboot.
- 31763 — TACACS+: When trying to copy into multiple SSH and Telnet Sessions locks up the CLI.
- 32691 — Topology Notifications are sent continually when they shouldn't be.
- 34658 — Unable to send VPN data between a client PC and a VPN device on the internet when the outbound path has a VPN tunnel up.
- 34518 — Unit rebooted when using a large VPN pre-shared key.
- 31816 — VPN over a demand interface does not automatically switch back to primary link.
- 34293 — Web browser interface: HP 7102 Error with Uploading firmware from GUI.
- 33962 — Web browser interface: HP7102 Link Error on system Summary Page.
- 34350 — Web browser interface: HP7203 - 503 Server Error on VPN Certificates page.

Release J.06.03

Problems Resolved in Release J.06.03

- 34031 — ATM pvc queuing information is missing from the output of the command **show int atm 1.1.**
- 36717 — HDLC interface is down but still shows up in route table.
- 34087 — Help on **debug tftp server events** needs to say `TFTP server events` not `TFTP server packets`.
- 37044 — Help screen not encrypted in SSL session.
- 35403 — LLDP is not working on 802.1q interfaces.
- 32768 — MSN Messenger traffic reboots the unit.
- 33384 — OSPF configuration via the Web browser interface is misleading.
- 34257 — Policy classes with names **self** and **default** are not recommended.
- 28899 — QOS: CBWFQ doesn't work over analog modem.
- 35495 — Router incorrectly trusts RIP updates from an RRAS server (with metric 16) that is propagating valid routes from another local router.
- 35620 — SNMP reports a PPP interface (23) as a Multilink PPP Interface (108).
- 34331 — The **modem countrycode USA/Canada** command appears as **modem countrycode usa** in **show run** output.
- 34284 — Web browser interface status pages do not restart timers properly.

Release J.06.06

Problems Resolved in Release J.06.06

- 38622 — Network Monitor Web browser interface doesn't accurately show failed status
- 38804 — SNTP Server does not respond with the configured IP address

Release J.08.03

Problems Resolved in Release J.08.03

- 32541 - ARP - Proxy ARP replies to ARP requests on interfaces without IP addresses.
- ARP - Routing IP and bridging other protocols may cause routers to not reply to ARP requests.
- CLI - Deleting a track or probe from within that track or probe's configuration mode does not return users to the global configuration mode.

- CLI - The **show track** command does not reflect tracks applied to static routes.
- CLI - Users may configure a secondary IP address which is identical to the interface's primary IP address on that interface.
- CLI - When a console session times out, the CLI may get stuck in a loop, requesting that users **Press RETURN to get started** instead of providing the ***<hostname>*** prompt.
- Crash - The MSN Messenger ALG can cause the router to reboot.
- DHCP Server - The router does not reliably send DHCP Offers when acting as a DHCP server for a remote network.
- Ethernet - Collisions on an interface can cause Ethernet interfaces to stop padding small frames to the minimum allowable size of 64 bytes. This affects ARP (in addition to other traffic types), which effectively means the interface locks up after devices on the LAN segment clear their ARP caches.
- Firewall - Firewall route lookups contain two memory leaks (most likely to be seen with very high traffic levels).
- 25410 - Frame Relay - Asymmetrical throughput results are seen over Frame Relay when using the dual T1 module.
- 25316 - HTTP - The HTTP server is no longer enabled after Web-registration has been done.
- 25228 - HTTP/HTTPS - The parameters **ip http server** and **ip http secure-server** are now enabled by default.
- IP - Removing a secondary IP address on an interface may cause the router to stop responding to ICMP on any address assigned to that interface.
- IP - Secondary IP addresses do not properly create connected routes in the IP Route Table.
- Layer 2 - Changing T1 timeslot allocation for interfaces that are bound to a Layer 2 protocol (PPP, HDLC, Frame Relay) may cause the Layer 2 protocol to drop and not come back up until the router is rebooted.
- Modem - Input/Output rate statistics are incorrect on the modem interface.
- 38714 - Network Monitoring / ICMP Probe - If the ACL to define probe traffic for PBR specifies the echo type only, the track will not reinstate the primary link when the network problem is resolved.
- PPP - Changing the bandwidth statement on a PPP interface causes the interface to bounce.
- PPP - Packets in the PPP transmit queue are not deleted when a PPP interface goes down, which can lead to reboots.
- 25429 - PPP - Port 2 of the Dual T1 module will not bind properly in a MLPPP configuration.

- Security - Under **Certificates**, the Web browser interface fails to generate a valid Self Certificate Request when using Fully Qualified Domain Names as Subject Name identifiers.
- SSH/RADIUS - When a RADIUS server rejects a user's SSH login credentials, the router continues to send requests to the server until the maximum retry value is reached.
- TFTP - TFTP uploads to the router may fail, displaying the error, **Received Past Block ID**.
- VPN - Very high VPN traffic may cause devices to lock up.
- Web browser interface - Clicking the **WAN-T1** link in the **DSX-1 Map** field of the DSX configuration page returns a **404: Page Not Found** error page.
- Web browser interface- The **Debug** page allows users to **debug ppp packet** despite this being an invalid debug option.
- Web browser interface - The Web browser interface allows Ethernet subinterfaces to be selected for NAT while from the CLI this is not permitted. If no reboot is done, the Secure Router accepts the entry via the Web browser interface and it works fine until the router is rebooted. When a reboot is done, the router inspects the startup-config and deletes the “invalid” entry.

Known Software Issues and Limitations

This section identifies issues you may encounter when using a ProCurve Secure Router 7000dl. Issues are listed in chronological order, oldest to newest.

Release J.02.02A

- **29068** — Cannot create secondary address on 802.1Q interfaces.
- **28759** — Web browser interface - "**Telnet/SSH/Console -> Use password**." SSH does not use the specified password.
- **27370** — Files that are eight characters or less combined with file extensions of three characters or less cause the file to be displayed in all caps on the router. For example, `abcdefgh.biz` would be displayed in all caps on the router.
- **27511** — The **test-pattern insert** and **show test-pattern** should not be allowed with 1's and 0's pattern.
- **27626** — **no debug ip ospf hello** Command not available.
- **27827** — **Show int adsl 1/1 ver** and **show int adsl 1/1 info** commands do not display information correctly.
- **26606** — Debug commands for HDLC do not work.
- **26620** — DHCP Client does not work on an HDLC interface. This feature was not implemented for HDLC.

Release J.03.01

- 29525 — Activity LED on Ethernet ports is active although nothing is connected.
- 29641 — Upgrading Boot Code from system code gives confusing message that process failed, but in reality it succeeded.

Release J.04.01

- 31789 — A bid of length 26 or more will reboot the unit.
- 31758 — AutoSynch fails after copying image over from TFTP server.
- 31827 — Demand Routing: Correct demand interface doesn't dial when multiple demand interfaces have interesting traffic

- 31733 — Dial Backup doesn't work correctly if two Dial-Backup cards are installed.
- 31634 — Dual ISDN U interface card sometimes does not display the correct status message when call is connected.
- 31742 — Dual-port ISDN cards report wrong SNMP values.
- 31383 — GRE: Debug tunnel interface shows bogus IP address.
- 30201 — HDLC interface has wrong SNMP values.
- 31890 — **Logging forwarding source-interface <interface>** occasionally doesn't work
- 32071 — LLDP cannot be turn off on GRE Tunnel-interfaces.
- 31665 — OSPF MP: **show ip route summary** counts sometimes shows negative counts.
- 31697 — PIM: Mroute table shows interfaces are forwarding and pruned at same time.
- 31675 — Removing the cable of Dual ISDN card while operational will reboot the router. *Workaround: shutdown interface first.*
- 31849 — Router reboots if command **no ip add** is entered in a ppp interface that is up. *Workaround: Shut down interface first and then add null IP address.*
- 31780 — **show demand resource pool** output is not correct.
- 30953 — **show int demand X** displays `bandwidth=0 Kbps` with calls connected on Dual-ISDN S/T card.
- 29370 — **show modules** does not report part number for IPSEC module.
- 31272 — **show queue ethernet x/x** does not have value for queueing method.
- 31082 — **show run interface** does not work for loopback interfaces.
- 31757 — **show tech** command resets terminal length to default setting.
- 30847 — SIP ALG only works from “private to public”.
- 29215 — When large number of BGP routes are advertised MLFR link goes down.

Release J.05.02

- 33279 — Incorrect console status messages regarding ISDN modules when a module is not configured with a SPID and it is enabled or disabled.
- 30819 — Event message during boot shows ISDN interface `UP`.

- 31355 — FILESYSTEM: Locking mechanism may not work properly when copying files from cflash to flash.
- 33697 — MCAST: Simultaneous use of PIM and static multicast has incompatibilities.
- 28249 — Router reboots when the compact flash is removed while autosynch is updating.
- **show system** command is not implemented in this release, so it is not recognized by the CLI. It appears in error in the CLI reference guide.

Release J.06.03

- 37420 — 128MB Crucial compact flash does not work.
- 38659 — Changing Bandwidth statement bounces PPP interface.
- 38812 — Copying SROS.BIZ in bootstrap mode gives an incorrect message:

```
bootstrap#copy cflash SROS.BIZ flash

CFLASH SROS.BIZ
1 File(s) copied <--- incorrect message
Destination file already exists. Overwrite? [y or n]y
File copied
bootstrap#
```

  Workaround: Use the command **copy cflash SROS.BIZ flash SROS.BIZ**

- 38677 — **debug hdlc** is missing.
- 38714 — Network Monitoring / ICMP Probe - If the ACL to define probe traffic for PBR specifies the **echo** type only, the track will not reinstate the primary link when the network problem is resolved.
  *Workaround: Remove the **echo** parameter in the ACL.*
- 38804 — SNTP Server does not respond with the correct IP-address. The router responds with the nearest IP-address, which might not be the address queried. SNTP Clients drop the packet if the response is not from the IP-address queried. For example, when using a loopback interface, SNTP Client queries the loopback interface, but the SNTP Server responds with the nearest interface IP-address, which may be incorrect.

Release J.08.03

- VPN - Units that terminate a high number of VPN tunnels (64+) with heavy traffic on the tunnels may experience errors in encryption. When such an error occurs, an event is displayed: "Internal error in udm_pkt_sync." The unit will recover from this error and continue encrypting/decrypting packets properly.

— This page is intentionally unused. —

Part Number 5991-2124
August 2007B