Known Anomalies: BayRS 13.00, Site Manager 7.00, and BCC 4.05

BayRS Version 13.00
Site Manager Software Version 7.00
BCC Version 4.05

Part No. 303551-A Rev. 00
October 1998

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Known Anomalies: BayRS 13.00, Site Manager 7.00, and BCC 4.05

This Bay Networks® document supplements both the *Release Notes for BayRS Version 13.00* and the *Release Notes for Site Manager Software Version 7.00*, and contains information about:

- Router known anomalies in BayRS™ Version 13.00
- Site Manager known anomalies in Version 7.00
- Bay Command Console (BCC) known anomalies in BCC™ Version 4.05

This document does not list resolved anomalies, that is, known anomalies that were documented in previous releases that have since been fixed.

Known Router Anomalies in Version 13.00

The sections that follow describe the known router anomalies and, when applicable, suggested workarounds. Bay Networks will resolve most of these known anomalies in the near future.

ARN Anomaly

Title: LEDs turn off and on again after you remove the cable connection from a 100BASE-FX interface.

Platform: ARN

Number: 35472

Description: When you remove a valid cable connection from a 100BASE-FX interface on an ARN, the Link, 100, and Receive LED indicators turn off after approximately 5 seconds. The three LEDs then light again and remain on until you re-establish a valid cable connection.

Workaround: Set Total, Inbound, and Outbound Link Activation Limits to 256, 0, 256.

ASN Anomaly

Title: ASN2: Hardware.bat script shows incorrect information.

Platform: ASN

Number: 25912

Description: For ASN2 routers that shipped with pre-11.00 software, the output of the show hardware slot script will not correctly identify the ASN2 processor module.

ATM Anomalies

Title: ATM Signalling cannot obtain GAME buffer when resetting slot under heavy traffic.

Platform: BLN

Number: 21656

Description: Resetting an ATM slot while under heavy traffic load may cause an ERROR in the ss_ptsp.c file. The log states that ATM signalling cannot get a GAME buffer.

This error appears to occur when traffic is flowing uni-directionally from one slot to another. The receiving slot resets while the transmitting slot faults and requires manual intervention to restart.

Title: Cannot delete ATM from the Configuration Manager Circuit List window.

Platform: BLN

Number: 33228

Description: Deleting ATM from the Configuration Manager Circuit List window improperly sets the MIB.

Workaround: Do not attempt to delete an ATM circuit using the Configuration Manager Circuit List window.

When deleting ATM from an interface, you must use the Edit ATM Connector window. When deleting ATM from the router, you must use the delete ATM option from the Configuration Manager Protocols menu.

BGP Anomalies

Title: BGP policy filters support matches for a single AS path expression only.

Platform: All

Number: 20592

Description: A BGP policy only supports a single AS path regular expression to match to.

Title: Trouble deleting BGP with BCC.

Platform: BLN

Number: 28827

Description: When BGP is deleted with BCC, the configured peers may still remain in the routing table.

Title: BGP peer holdtimer does not negotiate to zero.

Platform: BCN

Number: 74687

Description: When a BGP peer-to-peer session is established with one end advertising a holdtimer of 0, the session should establish without the use of keepalives. However, the open exchange incorrectly results in use of the non-zero value.

Workaround: Configure the holdtimers at both ends of the peer session to be the same value.

Bisync over TCP Anomalies

Title: Bisync over TCP: During 2400 baud operation, BOT traffic may stop.

Platform: AN

Number: 18831

Description: BOT traffic stops when a certain character stream appears during 2400 baud operation.

Workaround: Use the default value of 1580 bytes for the MTU parameter on the Bisync interface for operation at 2400 baud.

Title: Poll sent by host echoed back to host if you disconnect an asynchronous cable.

Platform: BLN

Number: 32649

Description: If you disconnect an asynchronous cable to a device to which the router is forwarding alarms, the router echoes the polls from the host back to the host.

Workaround: Disconnect the cable from the router instead of disconnecting it from the alarm device.

CSMACD Anomaly

Title: Collision errors in 100-MB Ethernet interface driver statistics.

Platform: BCN

Number: 15966

Description: On BN or ASN routers, collisions that occur during normal operating conditions on a 100 MB Ethernet interface can cause the driver to record additional errors as part of its receive driver statistics. These errors, which normally do not appear as part of the driver statistics, display as Receive Symbol errors, CRC errors, runts (InternalMacRxErrors), and alignment errors.

Workaround: Ignore these errors.

DataPath Anomaly

Title: The router displays several Tag Violations when the ATM driver goes down.

Platform: BLN

Number: 13731

Description: The router displays several Tag Violations when the ATM driver goes down. The router displays the errors when you have configured more than 500 group mode virtual circuits (VCs) running IP with no RIP or OSPF and you unplug the FO cable on one of the interfaces or you reboot the router.

If the routers are connected back to back both will display the Tag Violations.

DCMMW Anomalies

Title: There is no way to disable creation of default RMON matrix and host tables.

Platform: AN

Number: 31379

Description: Setting wfDCMEntry.wfDCMRMONDfltHost and wfDCMEntry.wfDCMRMONDfltMtrix has no effect on a BayStack router DCM. However, most applications can handle the default rows.

Workaround: If the default matrix and host tables create a problem, delete the hostControlEntry and MatrixControlEntry after the router boots.

Title: Setting thresholds using the Threshold Manager requires Technician Interface setting.

Platform: BLN

Number: 35674

Description: Before setting thresholds using the Threshold Manager, make sure to set the RAESA sub agent. The DCM sets this automatically. However, setting MIB II variables on a BLN, for example, requires that you set this sub agent.

Workaround: Use the Technician Interface to set the wfdrivers.wfRAEsaLoad variable to the value used by the other drivers on that router.

DLSw Anomalies

Title: Dynamically adding DLSw default NetBIOS name failed to work.

Platform: BLN

Number: 18081

Description: When you dynamically add a default NetBIOS name entry, the entry does not become active until you save and reboot the configuration file.

Workaround: Add default NetBIOS in local or remote mode.

Title: Dynamically changing the SAP credit can cause DLS connectivity problems.

Platform: BLN

Number: 29482

Description: Routers running 8.12/16,10.01/4 and 11.00/4 have a problem with DLS connectivity after making dynamic changes to the DLS SAP credit. The problem only occurs if the SAP credit is changed from a lower number (such as 10), to a higher number (such as 25). After, no new sessions can be established through that peer.

Title: SDLC Fast and Slow Poll Timer default values are too high for DLSw.

Platform: All

Number: 34067

Description: If you have a router performing SDLC to LLC conversion, and you use the default values for the SDLC parameters Fast Poll Timer and Slow Poll Timer, SDLC controller performance is very poor.

Workaround: Change the Fast Poll Timer to 200 and the Slow Poll Timer to 400. These changes will improve performance for both single- and dual-switch DLSw configurations in which the router acts as an SDLC primary device. Depending on the number of SDLC controllers you are supporting, you may need to increase or decrease the numbers to improve controller response time and router performance.

DVMRP Anomalies

Title: DVMRP cannot correctly handle multinetted circuits.

Platform: BLN

Number: 11559

Description: DVMRP currently does not handle multinetted circuits.

Title: DVMRP does not appear as requestor using MRINFO.

Platform: AN

Number: 13776

Description: There is currently no workaround.

Title: You cannot change DVMRP Debug Level.

Platform: All

Number: 33386

Description: If you try to change the DVMRP Debug Level, you get an error message: “SNMP Set Error.”

FireWall Anomalies

Title: The Check Point FireWall-1 GUI does not display statistics for Bay Networks routers.

Platform: BLN

Number: 30544

Description: The System Status View window in the Check Point FireWall-1 GUI does not display statistics for Bay Networks routers.

Workaround: Use the **fw stat -long router_ip_address** command to generate statistics for Bay Networks routers.

Title: The Check Point Log Viewer displays the incorrect time.

Platform: BLN

Number: 30546

Description: The time that the Check Point Log Viewer displays is behind by one hour. For example, if the time should read 12:17, the Log Viewer displays the time as 11:17. Log events from the management station (or fw daemon) display the correct time.

Title: The Octal sync link module is not fully supported.

Platform: BLN

Number: 31070

Description: The Octal Sync card is not fully supported in Phase 1 of FireWall. Only ports 1-6 effectively apply policies. Ports 7 and 8 act as unsupported interfaces would and allow all traffic to flow as normal.

Title: Address translation should not be enabled on NT systems.

Platform: BLN

Number: 31121

Description: With the Windows NT and Windows 95 GUI clients, Address Translation policies can be downloaded to Bay Networks routers. However, Address Translation is not supported by Bay Networks routers and downloading Address Translation policies to a Bay Networks router may cause problems on the router.

Title: The Check Point FireWall-1 Log Viewer occasionally stops logging.

Platform: BLN

Number: 31122

Description: Occasionally, the FireWall-1 Log Viewer stops logging events.

Workaround: You can usually make the FireWall-1 Log Viewer resume logging events by stopping and restarting the FireWall daemons. To stop the daemons, use the command **fwstop**. To restart the daemons, use the command **fwstart**.

Title: Cannot use the Check Point FireWall-1 GUI to install policies to individual interfaces.

Platform: BLN

Number: 31175

Description: Using the Check Point FireWall-1 GUI, you cannot define router objects by interface so that you can install policies on a per -interface basis.

Workaround: Use the **fwload** command to install security policies on a per-interface basis. For example, the command **fw load stop_snmp.W cct1@lab_router** installs the policy stop_snmp.W only on cct1.

Title: FireWall-1 GUI client erroneously displays a message stating that management software is 2.x not 3.0.

Platform: BLN

Number: 31245

Description: When you install a policy, the FireWall-1 GUI client cannot load the security policy because it falsely detects FireWall-1 management software version 2.x even though FireWall-1 management software 3.0 is installed.

Workaround: Install the X/Motif GUI client.

Title: FireWall-1 Log Viewer can consume up to 98% CPU, causing an HP workstation to hang.

Platform: BLN

Number: 31301

Description: If the HP-UX version of the Log Viewer is left open for long periods of time where many log entries are required, it can consume up to 98% CPU. The Log Viewer must then be killed to prevent the system from hanging.

Title: The last security policy may not have been reinstalled after rebooting the router.

Platform: BLN

Number: 31544

Description: After FireWall-1 is installed on the management station and the first policy downloaded to the router, automatic policy downloads have occasionally failed after the router has been rebooted.

Workaround: Restart the daemons on the management station. To stop the daemons, use the **fwstop** command. To restart the daemons, use the **fwstart** command.

Title: On the HP-UX platform, you receive a “library not found” error and cannot run the Check Point GUI.

Platform: BLN

Number: 32436

Description: When trying to run the Check Point 3.0a GUI on an HP-UX system, you will receive a missing library error and you will not be able to run the Check Point GUI.

Workaround: Install and use the X/Motif GUI provided on the Check Point software CD.

Title: TCP sessions not terminated after new policy download.

Platform: BLN

Number: 32847

Description: Existing TCP sessions, such as FTP and Telnet, are not terminated after a new policy is downloaded. For example, if the current policy on router 1 allows FTP, and an FTP session is active from point A to point B, and if you download a new policy on router 1 that does not allow FTP, the FTP session does not terminate the active session that exists from point A to point B. The new policy does, however, prevent all new FTP sessions across router 1.

Title: Check Point's FireWall-1 GUI returns incorrect data for anti-spoofing Bay Networks routers.

Platform: All

Number: 35173

Description: When you select the SNMP Fetch button in the Router Properties window of the Check Point FireWall-1 GUI, router interface information is returned in the form of the circuit name, such as E21 or S311. Although the FireWall-1 GUI displays a warning message that tells you to change the interface information from interface name to cct notation, the information should be returned in the form of a line number such as line 101104.

Workaround: Change the information from circuit name format to line number format for anti-spoofing to work correctly.

Title: You must use the command line to install a license on an NT system.

Platform: All

Number: 35205

Description: When you try to install a new license for an NT system from the Check Point FireWall-1 GUI, you receive an error stating that the license is invalid.

Workaround: Use the command line to install the FireWall-1 management station license, as follows. Select Start, select Programs, then at the Command Prompt enter:

```
c:\uses\default> cd \fw1\bin
c:\fw1\bin>  fw putlic  <ip address> <license string>  pfm activemod control routers embedded motif
```

To restart the *FW1.exe* process, go to the Control Panel, select Services, select Stop, and then select Start.

Title: You must stop and restart the firewall daemons with a new log directory for Log Viewer 12.10.

Platform: All

Number: 35416

Description: When you update a firewalled router from version 11.02 or 12.00 to 12.10, you must stop and restart the firewall daemons with a new log directory so that the log viewer does not continue to create log entries using cct notation of phase 1. Once you stop and restart the firewall daemons, the log viewer uses line notation of phase 2 and the log information provides details about which interface caused a log to occur.

To stop and restart the firewall daemons, first exit the Log Viewer and Security Policy windows and then enter these commands:

```
lab#  fwstop
lab#  mv /etc/fw/log /etc/fw/log.bak
lab#  mkdir /etc/fw/log
lab# chmod 777 /etc/fw/log
lab#  fwstart
```

When you have restarted the firewall daemon, then restart the Security Policy and Log Viewer windows.

Title: The Check Point Log Viewer window occasionally freezes.

Platform: All

Number: 35495

Description: When running the Checkpoint Firewall-1 version 3.0a Log Viewer on an Ultra system running Solaris 5.5.1, occasionally errors are displayed in the window that the Checkpoint Log Viewer was started in. The Log Viewer may also hang.

Workaround: Stop and restart the Log Viewer.

Title: Cannot configure Firewall on ARN Fractional T1 unless all timeslots are used.

Platform: ARN

Number: 35590

Description: When you configure Firewall-1 on an ARN Fractional T1 interface, you must use all timeslots for Firewall-1 to function properly.

Title: Cannot successfully install a FireWall-1 security policy using TACACS+.

Platform: All

Number: 75974

Description: When using the FireWall-1 OpenLook GUI, you cannot install a security policy using TACACS+.

Title: FireWall-1 logging alert function does not work on NT systems.

Platform: All

Number: 75975

Description: The FireWall-1 logging alert function does not work properly on Windows NT systems.

Title: FireWall faults if you do not fill out all required fields.

Platform: All

Number: 78226

Description: When using the OpenLook GUI to configure and download a security policy, FireWall-1 faults if you do not fill out all required fields.

Workaround: Fill out all required fields.

Frame Relay Anomaly

Title: Compression over a traffic-shaped VC does not increase performance.

Platform: All

Number: 32691

Description: Running WCP on a traffic-shaped virtual circuit does not increase performance.

Workaround: Increase the Be setting to allow more traffic to pass through before compression occurs. For example, if the compression ratio is 1:2, increase the Be setting, but keep the Be + Bc setting below the line rate.

Frame Relay Dial-on-Demand Anomalies

Title: Frame Relay sometimes fails to activate in dynamic mode on the AN, ASN and ARN.

Platform: AN, ASN, ARN

Number: 30701

Description: When dynamically configuring a Frame Relay dial-on-demand circuit on the AN, ASN, or ARN, the circuit sometimes fails to activate. After you save the configuration and reboot the router, the Frame Relay circuit activates correctly.

Title: Removing ISDN cable from active FR/DOD line causes a fault on ASN and AN.

Platform: ASN

Number: 31448

Description: If you remove an ISDN cable from an active Frame Relay/Dial on Demand line, the system will return an error message.

Title: Dynamically configuring a Frame Relay demand circuit on an ASN and AN can cause a failure.

Platform: AN, ASN

Number: 31477

Description: Dynamically configuring a Frame Relay dial-on-demand circuit on an ASN or AN can cause a failure. After the failure, the router recovers and operates properly.

Frame Relay SVC Anomalies

Title: A bus error can occur while the router is monitoring frame relay statistics.

Platform: BCN

Number: 35246

Description: While monitoring frame relay statistics, the router generates a bus error approximately 2 to 4 minutes into the monitoring. This could be caused by lack of memory or the screen buffer filling.

Title: Router does not place an SVC call after deleting and re-adding an interface.

Platform: ARN

Number: 79605

Description: If you delete a circuit with SVCs configured on it and then re-add the circuit with the same SVC information as was previously configured, the router will not place an SVC call to the switch network.

FRE-2-060E Anomaly

Title: Adding Bandwidth on Demand to a circuit with WCP on ISDN disables data compression.

Platform: BN

Number: 75314

Description: Adding Bandwidth on Demand to a PRI circuit disables WCP data compression. The call does come up and traffic flows; but, WCP never creates a VC and does not compress traffic.

FTP Anomaly

Title: FTP brute force attack causes bus error and reboot on BCN.

Platform: BCN

Number: 83931

Description: When configuring FTP on a BCN router with a Quad Ethernet, attempting to make a brute force attack using FTP causes a buffer overflow problem that results in a bus error. As a result, the router restarts.

GAME Anomalies

Title: An 8MB ARN with 10 VLANs faulted with insufficient memory when disable port.

Platform: ARN

Number: 71082

Description: An 8MB ARN with 10 VLANs configured on the 100MB Ethernet port, each configured with IP/RIP and IPX/SAP/RIP, may fault with insufficient memory to continue error when the Ethernet port is disabled.

Workaround: Use 16MB ARN to support 10 VLANs on the 100MB Ethernet port.

Title: *REASA.exe* not loaded when router is initialized.

Platform: BLN

Number: 72366

Description: For the AN, ARN, ASN, and BN routers, *REASA.exe* is not loaded when router is initialized (wfDrivers.wfRAEsaLoad.0 = 0).

Workaround: To load the alarm and events agent, add Enable/Disable button in Site Manager, configuration option in install.bat, or load each time router comes up.

Title: 8MB FRE-040 with 20 VLANs each with IP/RIP out of memory fault upon boot.

Platform: BN

Number: 74669

Description: An out-of-memory fault occurs upon boot for a 8MB FRE2-040 with 20 VLANs on the 100MB Ethernet port of the D100M link module, each configured with IP/RIP. This fault occurs upon boot and continues endlessly.

Workaround: Use at least 16MB FRE2 processor card to support 20 VLANs configured with IP/RIP on the 100MB Ethernet port.

Hardware Diagnostic Anomalies

Title: Fail LED on Link module remains on after boot.

Platform: BLN

Number: 19383

Description: The ATM link module FAIL LED may remain on after the link module boots.

Workaround: Even though it remains on, the LED does not affect the operation of the router. However, if you want the LED off, cold-boot the router.

Title: Extended diag link header does not indicate HW compression daughterboard present.

Platform: BLN

Number: 20022

Description: The extended diagnostics link header does not indicate that hardware compression daughterboard is present.

Workaround: The extended diagnostic does not support testing for the hardware compression daughterboard. However, the daughterboard should boot without incident.

Hardware Processor Anomalies

Title: Booting off a Bluefish slot causes Technician Interface errors.

Platform: BLN

Number: 18730

Description: When booting off a Bluefish slot, all keyboard input is received by the SRML (with the console cable connected), but the Technician Interface output comes out through the 10BaseT port on the ARE processor. This is not the diagnostic port, but the port adjacent to it. To use the Technician Interface, you need to have 2 windows open.

Title: Booting from FRE1 triggers MCP on ARE slot.

Platform: BLN

Number: 18733

Description: Booting a Version 9.01/16 image from a FRE1 slot triggers an MCP on the ARE slot. This fault sometimes occurs very quickly (before LANE begins to initialize) and other times when LANE is in the middle of opening up SVCs.

Workaround: Movie the flash to a FRE2 slot (with the FRE1 still in the router).

Title: Cannot use disable/enable scripts on unnumbered IP interfaces.

Platform: BLN

Number: 18865

Description: You cannot use the disable and enable scripts on unnumbered IP interfaces. The scripts do not allow an interface IP address format specifying both the IP address 0.0.0.0 and the circuit number.

For example, create two unnumbered IP interfaces. Try to disable only one of the interfaces (for example, disable ip rip 0.0.0.0.3). The script allows 0.0.0.0 and disables the first unnumbered interface. It does not allow 0.0.0.0.3 or 0.0.0.3.

Workaround: Use Site Manager or the Technician Interface directly.

HSSI Anomaly

Title: Low HSSI performance numbers for packets >512 bytes.

Platform: BLN

Number: 75080

Description: With priority queuing enabled on a HSSI interface, performance numbers are low for packets less than 512 bytes.

Workaround: Disable priority queuing on the HSSI interface.

IP Anomalies

Title: If the best route protocol changes back from RIP to OSPF, not all nexthops return.

Platform: ASN

Number: 29716

Description: When the best route protocol changes back from RIP to OSPF, not all next hops return immediately. After 30 minutes, however, OSPF will flush its link state database and the routes will reappear.

Title: A router in ISP mode fails to hear RIP on local broadcast of 255.255.255.255.

Platform: BLN

Number: 30040

Description: In ISP Mode, the router will fail to hear RIP on the local broadcast of 255.255.255.255. RIP on the directed broadcast is okay.

Title: Multicast counters stay at zero for unnumbered IP interface.

Platform: All

Number: 31927

Description: On an unnumbered IP interface, both MCAST-IN and MCAST-OUT counters stay at 0.

Title: Circuitless IP In-Receives counter does not increment.

Platform: BLN

Number: 33227

Description: The In-Receives counter for circuitless IP is not incrementing. The Out-Requests counter, however, is incrementing properly.

Title: Drivers stop receiving data after toggling IP base while running a large frame relay configuration.

Platform: BCN

Number: 33973

Description: Some drivers may not receive data, even though all interfaces are up, after disabling and then reenabling the IP base when running large frame relay configurations (for example, IP over 200 to 300 group mode PVCs per slot, across 6 to 9 slots). This problem can also occur after booting the router.

Workaround: If the problem occurs after disabling and then reenabling the IP base, use the technician interface to set wfIpBase.wfIpBaseArpBufLimitPrcnt from 100 to 75 as follows:

set wfIpBase.wfIpBaseArpBufLimitPrcnt.0 75;commit

After IP becomes available, disable and then reenable the IP base again.

If the problem occurs after booting the router, save the configuration file under a new name and then boot the router with that new file.

Title: After you dynamically change line coding, IP fails to come up.

Platform: AN, ARN

Number: 72315

Description: IP does not come up after the line coding is changed dynamically.

Workaround: For the router on which IP became inactive, do one of the following:

- Disable and reenable IP.
- Save the configuration file and reboot.

Title: Problem with MOSPF peers configured as AS boundary routers over a point-to-point link.

Platform: BLN

Number: 75530

Description: In certain configurations, if both peers are configured as AS boundary routers, the remote router will receive the multicast CANUREACH_ex, decrement the TTL, and transmit it out the same interface it was received on. The origin router will do the same. This will continue until the TTL expires.

The problem occurs only on sync lines when the OSPF interface type is defined to be point-to-point. If it is defined as broadcast then the problem does not occur.

IPv6 Anomaly

Title: IPv6 does not work on X.25 PDNs.

Platform: BLN

Number: 32725

Description: X.25 decapsulation of IPv6 packets fails.

IPX Anomaly

Title: You cannot bring up an IPX network on both hosts deleting one host.

Platform: BLN

Number: 72410

Description: When an IPX network exists over a frame relay or PPP serial line between two routers and one of the router's interface configurations is deleted via BCC, you cannot reestablish the IPX network.

ISDN Driver Anomaly

Title: BofL is not automatically enabled for ISDN leased lines using Bay Networks Standard.

Platform: All

Number: 28775

Description: Site Manager does not automatically enable Breath of Life (BofL) messages on an ISDN leased line if you configure Bay Networks Standard as the WAN protocol. Without BofL messages, the router cannot determine the status of the line.

Workaround: Using Site Manager, enable BofL. Refer to *Configuring WAN Line Services* for instructions on enabling BofL.

L2TP (LNS) Support Anomalies

Title: L2TP session remains active when IP fails to converge.

Platform: BLN

Number: 33966

Description: When the router is acting as the remote dial-in client and its IP address does not match the RADIUS assigned IP address, the IP control protocol eventually fails to converge, but the session remains active.

Title: Disabling an L2TP circuit does not stop tunnel activation.

Platform: All

Number: 34495

Description: Disabling an L2TP circuit does not prevent the router (the LNS) from bringing up an L2TP tunnel. After the circuit is disabled, the LNS still responds to the LAC request and activates the tunnel.

Title: Changing the L2TP IP address causes the tunnel to fail.

Platform: BLN

Number: 75408

Description: Making a modification to an existing L2TP IP interface address causes the L2TP interface and the L2TP tunnel to fail. This does not occur when creating a new L2TP configuration in the same environment.

LB Anomaly

Title: The source route interface record is not deleted if source route spanning tree has been previously deleted.

Platform: BLN

Number: 12089

Description: If source routing is deleted either explicitly or by deleting a bridge or the circuit, the source route interface record is marked as deleted but the record is not removed from the router's MIB.

LLC Anomaly

Title: Deleting LLC from an Ethernet circuit creates a bus error.

Platform: BLN

Number: 30425

Description: Dynamically deleting LLC in an Ethernet circuit configured for APPN can create a bus vector error.

Workaround: Open the configuration file in local mode before deleting LLC from the Ethernet circuit.

MCT1E1 Anomaly

Title: Bus errors occur on an 8-MB ASN with more than four T1 connections.

Platform: BLN

Number: 29421

Description: On an 8 MB ASN configured with more than four T1 logical lines, the router faults when making a fifth logical line connection.

Workaround: Increase the ASN global memory configuration, or reduce the number of simultaneous T1 connections. These bus errors do not occur when the ASN is configured with 16 or 32 MB of memory.

MIB Anomalies

Title: The wfDot1dBaseNumPorts counter does not accurately track dynamic changes in the router configuration.

Platform: BLN

Number: 13901

Description: The wfDot1dBaseGroup.wfDot1dBaseNumPorts counter value is correct after a system boot, but the counter does not track all dynamic configuration changes. For example, the counter does not increment after adding a circuit configured with bridge services only. The counter does, however, decrement after deleting the same circuit.

Title: The router counts BofL packets as unknown protocols.

Platform: BLN

Number: 19041

Description: If a router receives a Breath of Life (BofL) packet, the router considers it an unknown protocol. The router increments the MIB entry that tracks unknown protocols each time an interface receives a BofL packet.

Workaround: Disable BofL packets for the interface.

Title: The MIB-II ifIndex incorrect after you delete a circuit, causing problems with Omniview.

Platform: BLN

Number: 25568

Description: The router creates MIB-II attributes when you create circuits on the router platform. The MIBII attributes include the ifNumber, which is the number of network interfaces (regardless of their current state) present on the system and the ifIndex.

The ifIndex is a unique value for each interface. Its value ranges between 1 and the value of ifNumber. The value for each interface must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.

If you dynamically delete a circuit on the router, the MIBII attribute ifNumber decreases by 1. If you check the IfIndex, the result will be noncontiguous.
The result is that when the router is polled for ifNumber it shows the correct value but when the ifIndex is polled between 1 and the ifNumber there is a chance that there are indexes/circuits outside this range.

The result is that SNMP management stations such as Omniview will display an error.

Title: The wfIfEntry/ifEntry wfIfLastChange incorrect when interface down.

Platform: BLN

Number: 28249

Description: The MIB-II wfIfEntry/ifEntry attribute wfIfLastChange is incorrectly set to 0 when an interface is disabled or drops because of a line failure. This produces an incorrect value for the length of time an interface has been out of service.

NAT Anomalies

Title: Network Address Translated not supported in IP ISP Mode.

Platform: BLN

Number: 32473

Description: NAT will not work with ISP mode.

Title: NAT static entries are not deleted when NAT is removed.

Platform: All

Number: 87042

Description: When you delete NAT from all interfaces on a router, static entries that you previously defined are still present in the MIB. If you add NAT back to the router, those static entries will appear in Site Manager.

Netboot Anomaly

Title: Cannot netboot with more than one QSYNC net module.

Platform: ASN, System 5000

Number: 29174

Description: Network booting may not work when two or more Quad Synchronous (QSYNC) net modules are installed in the same ASN router or System 5000 platform.

Workaround: Try using an interface on the other QSYNC net module for netbooting, or reversing the position of the two modules.

OSI Anomaly

Title: You cannot filter OSI over X25 with user-defined filters.

Platform: ASN

Number: 13727

Description: You cannot filter OSI over X25 with user-defined filter.

OSPF Anomalies

Title: OSPF border routers may fail to generate ASB Summary links.

Platform: LN

Number: 20561

Description: In some circumstances, an area Border router may not generate an ASB summary link advertisement, which in turn causes loss of connectivity to AS external routes.

Title: OSPF area border router incorrectly summarizes Type 2 Network.

Platform: BCN

Number: 85076

Description: In Version 11.03, revision 3 and revision 4, an OSPF Area Border Router (ABR) may incorrectly summarize a Type 2 Network-LSA, resulting in loss of inter-area connectivity. When the ABR generates the Type 3 Summary-LSA, it sends the wrong Link State ID because it fails to apply the network mask to the original Type 2 Network Link State ID.

Protocol Prioritization Anomalies

Title: Configuring a source route bridge (SRB) drop filter on SSAP range 0x00 to 0x00 brings the line down.

Platform: All

Number: 14612

Description: Configuring an outbound traffic filter to drop all SRB frames with a source SAP of 0x00 prevents the sync line from coming up, or causes it to go down when adding the filter dynamically. This occurs both with standard PPP and Bay Networks PPP.

Workaround: Create a different filter to accomplish equivalent filtering results. Do not specify outbound filter criteria with Add->Datalink->Source Routing->SSAP with the range 0x00-0x00.

Title: Outbound traffic filter address ranges in canonical format do not work on token ring interfaces.

Platform: BLN

Number: 29583

Description: In Router Software Version 10.01 and higher, specifying outbound traffic filter address ranges in canonical format can cause the filter to miss some addresses on a token ring interface. Outbound token ring filters require source or destination addresses entered in non-canonical format. Non-canonical format is also called most-significant-bit (MSB) or bit-swapped format.

For inbound traffic filters, you can use either canonical or non-canonical format for address ranges.

Workaround: Configure outbound token ring traffic filter ranges in non-canonical format. For example, to create an outbound traffic filter that drops the address 0x123456789ABC, specify the filter range as 0x482C6A1E593D, the bit-swapped format.

Qualified Logical Link Control Anomalies

Title: Destination SAP other than 04 not working with QLLC & outbound calls.

Platform: AN

Number: 32334

Description: A destination SAP other than 04 not working with QLLC and outbound calls.

Title: Full mac-cache-age cycle needed to recover after bouncing DLS global.

Platform: BLN

Number: 35062

Description: After you restart the DLS global MIB on an upstream QLLC router, sessions do not recover for at least the full configured DLSw mac-cache-age value. The problem does not happen on a downstream QLLC router. With a default mac-cache-age of 300 seconds, the delay is about 6 minutes.

RSVP Anomaly

Title: The **rsvp oi** command unexpectedly displays the message “No outgoing interfaces.”

Platform: BLN

Number: 34687

Description: The **rsvp oi** command displays “No outgoing interfaces.” This response is correct but can be confusing because in the past “No outgoing interfaces” triggered alarms.

Site Manager Configuration Anomaly

Title: IPv6 over frame relay SVCs not supported.

Platform: ASN

Number: 35060

Description: The Protocols window for frame relay SVCs includes an IPv6 option. However, BayRS does not support it.

Workaround: Do not select the IPv6 option.

Software Encryption Anomaly

Title: Data encryption does not work on PPP multilink circuits.

Platform: All

Number: 33912

Description: WEP causes a bus error when running on a PPP multilink circuit.

Software Services Anomalies

Title: The frame relay dial backup line does not deactivate when the primary line recovers.

Platform: ARN

Number: 27310

Description: The frame relay dial backup line does not deactivate after the primary line recovers.

Title: If you configure a hot standby circuit dynamically, it remains active permanently.

Platform: BLN

Number: 31638

Description: If you configure a hot standby circuit dynamically, it remains active permanently. The circuit does not deactivate even if you change the standby mode from No Action to Deactivate. The hot standby circuit should be inactive unless the primary circuit fails.

Sync Anomalies

Title: On an AN, DTR does not drop during warm boot.

Platform: AN

Number: 24650

Description: On an AN, DTR signal does not drop during warm boot.

Title: Hardware LAPB interface does not detect cable being removed.

Platform: BLN

Number: 25870

Description: If the cable is removed from any synchronous port except octal sync on a BN or an LN, the router gives no indication of the problem and the link remains active.

Workaround: Enable the Sync Polling parameter (Configuration Manager -> Edit Line -> Edit Sync Parameters). The configured WAN protocol will close all connections when the synchronous line driver detects connection signal lost.

Title: Loopback condition occurs when the synchronous cable is disconnected from the modem.

Platform: All

Number: 26082

Description: If you have a port on an octal sync or quad sync net module configured as an asynchronous interface, a loopback condition occurs when you disconnect the synchronous cable from the modem and do not disconnect it from the router. The log will fill with loopback detection messages.

Workaround: Disconnect the cable from the router instead of from the modem.

Title: On the BLN, a leased bandwidth circuit with WCP over a sync line causes an orphan buffer.

Platform: BLN

Number: 31499

Description: If you configure a BLN with the compression protocol (WCP) operating on a leased bandwidth-on-demand circuit over a synchronous line, this configuration causes orphaned buffers. This happens if WCP is added dynamically or if you reboot the router with this configuration.

Workaround: Do not configure WCP for leased bandwidth-on-demand circuits across synchronous lines on a BLN.

TFTP Anomaly

Title: You cannot TFTP to a rev. 7 or higher AN.

Platform: AN

Number: 75436

Description: You cannot TFTP to a rev. 7 or higher AN with Ethernet/token/sync interfaces.

Workaround: Issue this command at the Technician Interface prompt:

xtftp on

Technician Interface Anomaly

Title: The Technician Interface does not display all the characters in a prompt.

Platform: BLN

Number: 30056

Description: The Technician Interface prompt can be18 characters long. However, if you configure a prompt larger than 13 characters, the Technician Interface does not display the entire prompt.

VINES Anomaly

Title: When the router receives a VINES IP packet, it can cause VINES to reset on router.

Platform: All

Number: 85612

Description: If the router receives a VIP (VINES IP) packet destined for a client at the network layer, whose origin is a station on the same LAN, and if the client's routing server is not in the routing table, but the client is in the router's neighbor table, then VINES may reset on the router.

VLAN Anomaly

Title: Statistical counts not available for 802.1Q tagged circuits.

Platform: All

Number: 71816

Description: Statistics (for example, received octet, transmitted octet, and error counts) are not available for 802.1Q tagged circuits.

Workaround: Version 12.20 does not gather statistical counts for each 802.1Q tagged circuit. To view aggregate information for the 100BASE-T interface, use the BCC commands **show smacd receive errors, csmacd system errors**, **csmacd transmit errors**, and **csmacd stats**.

VRRP Anomaly

Title: Token Ring Address must be filled in under IP VRRP Config Params.

Platform: ASN

Number: 84778

Description: You need to enter a Token Ring Address in the IP VRRP Configuration Parameters window in Site Manager. If this is not done prior to configuring VRRP a fault occurs on router.

WEB Server Anomalies

Title: TCP connections not closed/released correctly.

Platform: BLN

Number: 34937

Description: If TCP connections to the HTTP server get interrupted (for example, if you press the "Submit" button on the log form while a transfer is in progress), the connections may still appear in the connection table in a "listening" state. Connections in this state use a small amount of system memory, but do not cause any problems.

Workaround: To completely delete these sessions, you must disable and then reenable the HTTP server with the following Technician Interface commands:

```
[3:TN]$ s wfHttpSrv.wfHttpSrvDisable.0 2; commit
[3:TN]$ s wfHttpSrv.wfHttpSrvDisable.1 1; commit
```

Title: The Navigational frame does not appear.

Platform: BCN

Number: 35055

Description: When connecting to a router with Netscape Navigator or Netscape Communicator running on UNIX, the Navigational frame (the left-most frame) may remain blank.

Workaround: To make the Navigational frame appear, reload the page by clicking on the browser Reload button while pressing the [Shift] key.

Title: Access to device prohibited when authentication set to digest.

Platform: All

Number: 83911

Description: Using Windows 95 with Netscape Communicator 4.5b1, with both the Manager (with or without a password) and User logins, when authentication is set to digest, the "Authorization failed. Retry?" window appears.

Workaround: This is expected behavior. If the browser doesn't support digest authentication, setting the server to digest will prevent access. This is not an HTTP server problem but a browser problem.

X.25 Anomalies

Title: Call accepted with misconfiguration of Mapping Types.

Platform: BLN

Number: 22555

Description: A call is erroneously accepted at the local end of a IPEX connection when the Local is mapping type E2E and the remote is Local, even though the call request is not sent out the remote port.

Title: IPEX facilities operation/configuration inconsistent with X25 services.

Platform: ASN

Number: 26284

Description: When configuring IPEX service for facilities, the configuration requirements are inconsistent and not the same as for other X.25 services.

Title: Calls are cleared but reconnect after the X25 Service is set to Disable.

Platform: BLN

Number: 34154

Description: Calls are cleared but reconnect even after the X25 Service is set to Disable. When you reenable the X25 Service, the calls are again cleared.

Title: X25 packets not reaching X25 hosts prior to timeouts.

Platform: All

Number: 83704

Description: If a target server application on an X25 host has a timeout system implemented and the X25 gateway's buffer does not fill up before a timeout occurs, the X25 packet is never formed nor sent to the X25 host. Subsequently, the X25 host closes the session because there is no data activity. The session does not work correctly; frequently, the foreign host closes the session.

Workaround: Allow a default packet size of 1 byte. This way, any data sent from the client side will be immediately used by the X24 GW #1 to form and send an X25 packet to the X25 host.

Known Site Manager Anomalies in Version 7.00

The sections that follow describe the known Site Manager anomalies and, when applicable, suggested workarounds:

- General Site Manager Anomalies
- Site Manager Anomalies on PCs
- Site Manager Anomalies on SunOS 4.*x*

Bay Networks will resolve most of these known anomalies in the near future.

General Site Manager Anomalies

Title: DLSw does not take advantage of NetBIOS name caching.

Platform: All supported by Site Manager

Number: 16067

Description: DLSw does not take advantage of NetBIOS name caching within source route bridging.

Title: Editing *ti.cfg* remotely creates an invalid configuration file.

Platform: All supported by Site Manager

Number: 23666

Description: If you modify the *ti.cfg* file using the Configuration Manager in remote mode, the router will update the *ti.cfg* file with the router's hardware information. If you make subsequent changes to the file (for example, adding an Ethernet interface), save the file, then try opening it in local mode, the router is not able to read the hardware information. However, the router boots correctly with the file.

Title: An SNMP set error occurs when you change the Sync Media type.

Platform: All supported by Site Manager

Number: 25967

Description: SNMP set error occurs when you change the Sync Media type either from Raise DTR to V.25bis or vice versa.

Workaround: Ignore the SNMP set error; Site Manager does set the parameter correctly.

Title: When an IP interface is deleted in an OSPF area, Site Manger indicates that no more interfaces exist in that area.

Platform: All supported by Site Manager

Number: 26729

Description: When an interface is deleted in an OSPF area, Site Manager displays an erroneous window indicating that no more interfaces exist in that area. This is because Site Manager fails to get SNMP responses while checking to see if more interfaces exist in the area that the deleted interface was in. Site Manager does not get SNMP responses because OSPF is converging after the IP interface has been deleted, thus causing this erroneous window to appear.

Title: AN/ANH/ARN reports the wrong Scheduled Boot status.

Platform: All supported by Site Manager

Number: 27660

Description: When initially configuring the Scheduled Boot parameter in the RUI Boot Parameters window, the router occasionally returns status as Error Code.

Workaround: Try exiting and then reentering the window. Be sure you entered the volume of the file system that contains the boot image and configuration file.

Title: Initial IGMP Global Config Debug field Receive/Send values switched.

Platform: All supported by Site Manager

Number: 27949

Description: In the Initial IGMP Global Configuration screen, the values for Debug are incorrect. According to the IGMP MIB:

Bit 1 : log igmp receive messages
Bit 2 : log igmp sending messages

When Sending is selected, bit 1 is set and when Receiving is selected, bit 2 is set.

Title: Static Groups (IGMP) are available for older router versions.

Platform: All supported by Site Manager

Number: 29053

Description: When you configure a router running router software earlier than Version 11.00 using Site Manager Version 5.0 or 5.01, Static Groups is a selection under IGMP. When you click on it, nothing happens because Static Groups is not a feature supported for routers running software earlier than Version 11.00.

Title: Error message does not go away when the machine is locked.

Platform: All supported by Site Manager

Number: 30367

Description: When the machine is locked and you try to perform other tasks using Site Manager, you may get the error message “SNMP general Set Error! Machine is currently locked by manager xxx.xxx.xxx.xx.” When you click on OK, the error message goes away and then comes right back.

Workaround: You must kill the wfsm process to remove the error message completely.

Title: Error occurs when enabling OSPF Cost for PTP Links.

Platform: All supported by Site Manager

Number: 30448

Description: The OSPF parameter Cost For PtP Links displays an incorrect default value of 0. The value should be Disable. In addition, when you try to set the parameter to Enable, an SNMP error occurs.

Title: Cannot delete a channel in the ISDN Lease Line B Channels window.

Platform: All supported by Site Manager

Number: 30752

Description: When you select Leased - 2x64K as the Port Application Mode for an ISDN BRI interface, the Configuration Manager creates two B Channels. Clicking on the Delete button in the ISDN Lease Line B Channels window has no effect.

Workaround: To operate this ISDN BRI leased line with one B Channel, return to the Port Application window; then, select Leased - 1x64K.

Title: BAP preferred/reserved slots not configurable.

Platform: All supported by Site Manager

Number: 30910

Description: When configuring a Bandwidth Allocation Protocol (BAP) non-monitor circuit, Site Manager does not let you configure the preferred and reserved slots. Without these slots, the non-monitor router cannot find an available line and then cannot send the phone number associated with the line in a call response to the monitor router.

Workaround: Set the Bandwidth Mode parameter to dynamic monitor. The router that places the call becomes the monitor. If you require that one side be the non-monitor router, initially set the Bandwidth Mode to monitor or dynamic monitor, set the Preferred and Reserved Slot parameters, then reset the Bandwidth Mode to non-monitor.

Title: Unable to configure traffic filters for demand circuit groups.

Platform: All supported by Site Manager

Number: 32551

Description: On the BCN router, when configuring demand circuit groups, you cannot configure traffic filters from the Demand Circuit Groups window.

Title: Adjacent Host warning appears after Adjacent Host created.

Platform: All supported by Site Manager

Number: 33333

Description: After adding an IP adjacent host, and then configuring IP over a Null Encapsulated ATM PVC, the following warning message appears:

```
If Data Encapsulation is set to NULL and Virtual Connection Type is
set to PVC, then an IP Adjacent Host should be added.
```

Workaround: Ignore this message if you have already created an IP adjacent host.

Title: Site Manager menu options are available for unsupported releases.

Platform: All supported by Site Manager

Number: 33702

Description: The FireWall menu options are available in Site Manager for router versions previous to 11.02 Rev. 2 even though the FireWall is not supported with these versions. For versions 11.02 and 11.02 Rev. 1, SNMP set errors result if you try to activate the FireWall. For 11.02, the MIB is present, so FireWall can be activated, but doing so could cause faults in the router.

Title: Creating an L2TP circuit dynamically takes too long.

Platform: All supported by Site Manager

Number: 34211

Description: During dynamic configuration of an L2TP circuit, Site Manager takes more than 2 minutes to create all required circuits and related MIB instances.

Title: Help is missing for the Remote TCP Port Number in the IPEX Mapping Parameters window.

Platform: All supported by Site Manager

Number: 34285

Description: When using Site Manager, help is missing for the Remote TCP Port Number in the IPEX Mapping Parameters window.

Workaround: Refer to *Configuring X.25 Services* in the Bay Networks documentation set.

Title: No support for MCT1 and ISDN Interface selection buttons; ENET and FENET buttons perform the same task.

Platform: All supported by Site Manager

Number: 34837

Description: When using the Site Manager Values window to select the interfaces you want the firewall to protect, selecting the ENET button shows both Ethernet and Fast Ethernet interfaces; the MCT1 and MCE1 interfaces are listed when you select the ALL button, but not when you select the SYNC button.

Title: Adding Trap Exceptions for the RFWALL entity (119) causes Site Manager to fault.

Platform: All supported by Site Manager

Number: 34912

Description: When you add trap exceptions for the FireWall entity (RFWALL), which has an entity code of 119, Site Manager faults. Note that after Site Manager faults the first time, the configuration becomes corrupted and you must reboot the router to be able to enter the Trap Exceptions table for RFWALL, as well as for other protocols/entities.

Title: RFWALL entity is not in the Trap Interfaces/Exceptions tables for Site Manager 6.10.

Platform: All supported by Site Manager

Number: 34915

Description: Because the RFWALL entity is not included the Trap Interfaces and Trap Exceptions tables for Site Manager Version 6.10, you cannot filter on the RFWALL entity when watching events through the Trap Monitor table.

Title: Configure L2TP for only supported protocol interfaces.

Platform: All supported by Site Manager

Number: 35084

Description: For L2TP configuration, the Bay Networks router only supports IP traffic through the L2TP tunnel. When selecting a layer 2 protocol for the L2TP configuration, select only frame relay, PPP (including PPP multilink), or ATM for the L2TP interfaces.

Title: Site Manager should not allow you to configure line resources over frame relay.

Platform: All supported by Site Manager

Number: 35164

Description: When you add IP and RSVP over frame relay, and enter the IP address, a message box requests “No line resources record exists for this line. Create line resources?” BayRS does not support line resources over frame relay. If you configure this service, the router faults constantly.

Workaround: Press Cancel.

Title: Site Manager 6.10 cannot create a firewall when wfRFwallDelete is set to 2.

Platform: All supported by Site Manager

Number: 35498

Description: In FireWall phase 1, when you set the parameter wfRFwallDelete to 2, save the configuration, and reboot the router, FireWall no longer exists on the router. However, because the MIB is not properly cleaned up, the FireWall menu erroneously shows that FireWall is already created.

Workaround: Enter the Technician Interface and execute the following command:

[2:1] **set wfRFwallGroup.wfRFwallDelete.0 1;commit**

Title: Site Manager enables Firewall on Fast Ethernet interfaces for 12.00 and 11.02.

Platform: All supported by Site Manager

Number: 35499

Description: When using Site Manager 6.10 to create Firewall on 12.00 or 11.02 routers, sets are done to enable Firewall on Fast Ethernet interfaces that are not officially supported in phase1. No problems have been found on these interfaces.

To determine on which slots Fast Ethernet interfaces are located, use the Technician Interface.

Title: Warning appears when enabling on Site Manager management port after FireWall is running.

Platform: All supported by Site Manager

Number: 35508

Description: After the router is rebooted with the FireWall configuration file, the Firewall is active on all interfaces on which it is enabled. Any newly added Firewall interfaces will be active immediately and enforce the default policy until you download the desired security policy.

If Firewall is added to the Site Manager management port, a warning will appear because Site Manager will lose contact with the router as result of the default policy:

```
WARNING: A Hardware SNMP Get Request failed with error code '2',
the SNMP timeout and retries values may need to be increased.
```

Workaround: Use the Configuration Manager in local or remote mode Site Manager when adding FireWall to the Site Manager management port.

Title: Site Manager does wrong set for a second MCT1 port on BN Dual MCT1 Link module.

Platform: All supported by Site Manager

Number: 35511

Description: Site Manager performs an incorrect set for the second MCT1 port of a dual MCT1 link module for BN platform. This causes the interface to have no FireWall support.

Workaround: Perform the correct set using the Technician Interface, as follows:

1. **Find appropriate line number:**

```
[2:1] get wfLineMappingEntry.3.*
wfLineMappingEntry.wfLineMappingCct.104201 = 1
wfLineMappingEntry.wfLineMappingCct.10904302 = 2
```

2. **Determine Firewall instance that is incorrect:**

```
[2:1]$ get wfIFwallIfEntry.6.*
wfIFwallIfEntry.wfIFwallIfLineNumber.4.32 = 4302
```

3. **Reset the Firewall instance:**

```
[2:1]$ set wfIFwallIfEntry.6.4.32 904302
```

Title: Windows Site Manager cannot add a second QLLC map.

Platform: All supported by Site Manager

Number: 35597

Description: Windows Site Manager cannot add a second QLLC map when you use a blank in the Adjacent MAC address of the first QLLC map.

Workaround: To configure two or more QLLC maps and use a blank in the Adjacent MAC parameter, configure a bogus unique MAC address in the Adjacent MAC address parameter of the first QLLC map, and save the configuration. Add the second map, using whatever value you want in the Adjacent MAC address parameter. Then set the Adjacent MAC address of the first QLLC map to blank.

Title: Setting IP Global Max Policy to high multiple of 32 hangs Site Manager.

Platform: All supported by Site Manager

Number: 75320

Description: The Max Policy parameter setting can hang Site Manager and bring down the router's interface if the parameter is set to a high multiple of 32.

Workaround: Use the default field value or a low multiple of 32.

Title: L2TP physical and internal IP addresses must be unique.

Platform: BLN

Number: 75403

Description: When configuring L2TP, you are not allowed to set the router's IP address and its L2TP IP interface address on the same network. The physical and internal addresses cannot be the same.

Workaround: Set unique addresses for these two parameters.

Title: L2TP IP Interface address change must be synchronized.

Platform: BLN

Number: 75576

Description: If the L2TP IP Interface address is changed in the IP Interface window, the appropriate change is not performed in the L2TP MIB. As a result, subsequent L2TP tunnels and sessions do not activate.

Workaround: Change the L2TP IP interface only in the appropriate L2TP window.

Title: VLAN Name parameter should not allow the use of spaces.

Platform: All supported by Site Manager

Number: 79067

Description: Site Manager allows you to configure VLAN names with spaces. This is inconsistent with the configuration of other circuit names. This does not cause any operational problems but the VLAN name may not appear fully in script output.

Workaround: When configuring VLAN names, we recommend that you do not use spaces.

Title: Site Manager crashes when you select Protocols > IP > OSPF/MOSPF > Interfaces.

Platform: All supported by Site Manager.

Number: 79073

Description: Site Manager crashes when you select Protocols > IP > OSPF/MOSPF > Interfaces.

Title: Site Manager does not change compliance mode for all lines in backup pool.

Platform: All supported by Site Manager

Number: 83363

Description: If you use Site Manager to change the Compliance Mode for a dialup line, Site Manager only changes the Compliance Mode for that line, not for all lines in the demand pool.

Title:	Long names for GRE TUNNEL NAME or REMOTE CONN cause statistics to display incorrectly.
Platform:	All supported by Site Manager
Number:	85381
Description:	If you configure GRE tunnels with GRE TUNNEL NAME or REMOTE CONN names that are longer than 20 characters, the statistics for greconn.dat and gretnl.dat will not display correctly. The tunnel name or remote connection name will push over the remote or local IP address field.
Workaround:	Use names for GRE TUNNEL NAME and REMOTE CONN name that contain less than 20 characters.

Site Manager Anomalies on PCs

Title: Cannot access Protocols menu when in LANE Parameters window.

Platform: PC

Number: 34641

Description: On a PC running Site Manager, when you access the LANE Parameters window, the window opens on top of the Service Record List window. You can still access the Protocols pull-down menu in the Service Record List window, even though this window is not active. However, attempting to use the Protocols pull-down menu in this inactive window causes a fault in the PC Site Manager application that requires a restart.

Workaround: Ensure that the Service Record List window is active before using the Protocols pull-down menu.

Title: Error while accessing OSPF interfaces from Site Manager 6.20.

Platform: Windows 95®

Number: 81742

Description: Accessing the OSPF interfaces from the configuration manager from Site Manager 6.20 causes an error.

Site Manager Anomalies on SunOS 4.*x*

Title: Unable to open/modify 9.02 images using Site Manager Unix 4.00 and 3.00 fix 1.

Platform: SunOS 4.*x*

Number: 24098

Description: When you try to open a Version 9.02 image using Site Manager for Unix 4.00 and 3.00 fix 1, the message `Invalid Image Specified:`*`path to executable`* is displayed and the image cannot be opened/modified.

Title: Cannot delete circuit if LLC2 was configured on the circuit and deleted first.

Platform: SunOS 4.*x*

Number: 32443

Description: If you add LLC2 and later delete it, Site Manager will not let you delete the associated LLC1 circuit.

Workaround: To delete an LLC2 circuit, delete the LLC1 circuit. Then re-add the LLC1 circuit and reconfigure the protocols on it.

Title: Configuring DLSw on second and successive token ring interfaces can cause duplicate IP address assignments on the router.

Platform: SunOS 4.*x*

Number: 32476

Description: After configuring DLSw on one slot, using the router's circuitless IP address as the value for the DLSw Slot IP Address parameter can result in duplicate IP Address assignments on the router. This condition occurs specifically when attempting to configure DLSw on more than one slot. For a new slot, Site Manager displays by default the router's circuitless IP address assigned to the first instance of DLSw. Accepting this value causes the duplicate IP address condition, which in turn brings down any TCP connections to DLSw peers previously established from the first slot. Site Manager may also display Source Route Bridge (SRB) global parameters, even if you previously enabled SRB anywhere else on the router.

Workaround: Determine from the DLSw Slot IP table (Protocols>DLSw>DLSw Slot IP Table) a new, unique address to enter as the DLSw Slot ID. Also, you should only need to enter the Source Route Bridge (SRB) Interface Ring ID for each additional instance of DLSw on the router.

Title: Fault occurs when changing LEC Configuration Mode to Manual.

Platform: SunOS 4.*x*

Number: 35394

Description: A fault occurs when using Site Manager Software Version 6.10 to change the configuration mode of a LEC on a router running a BayRS software version prior to Version 12.10.

Workaround: To change the Configuration Mode on a router running a BayRS configuration prior to Version 12.10, use the corresponding Site Manager software version. For example, if using BayRS Version 12.00, use Site Manager Software Version 6.00 to change the Configuration Mode parameter.

Title: Parameter name, Protocol Type (hex), is imprecise.

Platform: SunOS 4.*x*

Number: 72899

Description: Site Manager requires a value for the parameter, Protocol Type (hex), as part of the 802.1Q configuration process. Despite the misleading parameter name, the entered value must be a decimal number in the range of 1514 through 65535. The displayed default value, 33024, is expressed in decimal notation.

Workaround: If required to provide a new value, enter this value in decimal notation. This value should be the decimal equivalent of the TPID field in the 802.1Q encapsulated frame.
If the device on the remote side of the 100BASE-T interface is a Bay Networks product, for example a member of the Accelar line, it is not necessary to change the default value. Currently all Bay Networks products insert a value of 33024 (or 8100 in hexadecimal notation) into the TPID field of 802.1Q frames.

Title: Deleting the last NAT IP interface on a slot causes a fault condition.

Platform: SunOS 4.*x*

Number: 75574

Description: When you delete the last IP interface on a slot configured with NAT, Site Manager unloads NAT.EXE, causing a FAULT. NAT itself can be deleted successfully from all interfaces on the slot, but the deletion of the interface causes NAT to be unloaded.

Title: SRB over hybrid PVC configures incorrectly; deleting causes router to reset.

Platform: Sun-OS

Number: 85799

Description: When you create a Hybrid Mode PVC with source route bridging, all fields on source routing/interfaces screen incorrectly display zeros. When you delete the PVC, all slots on the router restart.

Known BCC Anomalies in Version 4.05

This section describes the known anomalies for the Bay Command Console (BCC) interface and, when applicable, suggested workarounds. Bay Networks will resolve most of these known anomalies in the near future.

Title: Cannot properly show, modify, or delete nonsupported objects.

Platform: BCN

Number: 29046

Description: You cannot use BCC commands to show, modify, or delete objects not supported by the BCC in the current release. The **show config** command does not display objects that BCC does not support. For example, **show config** does not display frame relay on a sync interface, although an instance of frame relay may exist on that interface. If an existing object supported by the BCC contains other objects not supported by the BCC, do not delete the BCC-configurable object. For example, do not delete a sync circuit configured with frame relay. This leaves an erroneous configuration on the router.

Workaround: Do not modify or delete any BCC configured object that contains another object not supported by (invisible to) the BCC interface.

Title: ISDN and COM1 ports are mutually exclusive on earliest AN routers.

Platform: AN

Number: 30708

Description: For the earliest ANs released by Bay Networks, the COM1 port becomes unusable after you configure the ISDN port. (Since the BCC does not support ISDN in Release 11.02, you must configure the ISDN port using Site Manager.) The BCC allows you to configure the COM1 port, even if you previously configured the ISDN port using Site Manager. These COM1 settings are invalid or meaningless, since the ISDN port takes precedence.

Workaround: If you use Site Manager to configure the ISDN port on an original-release AN, do not subsequently use the BCC to configure the COM1 port on the same AN.

Title: Does not detect new ports after a hot-swap.

Platform: BCN

Number: 70999

Description: After using the BCC to delete ports associated with a specific link module, and then replacing that module with one of a different type (hot-swapping), the new module does not initialize. Based on this condition, the system logs a Warning event message, indicating that the LOADER detected a misconfigured link module. (Deleting ports associated with an existing module is a standard task you complete before hot-swapping any link module with another.)

Workaround: Before hot-swapping any link module with one of a different type, first use Site Manager to delete ports associated with the link module currently installed.

Title: Values displayed for the type parameter of any board object require translation to a clearer module description.

Platform: All supported by the BCC

Number: 71867

Description: Values displayed by the BCC for the type parameter of any board object require translation to a clearer module description. For example, the board type qenf translates to a Quad Ethernet with Hardware Filters module.

Workaround: Refer to the BCC section of the router *Release Notes* for a detailed list of all module types supported by the BCC in this release.

Title: The **show dial backup lines** command displays an erroneous connector number for the BRI port on a hybrid Sync/BRI module.

Platform: AN, ANH, ASN

Number: 73727

Description: On AN, ANH, and ASN platforms, the BCC **show dial backup lines** command displays an erroneous connector number (2) for the BRI port configured on slot 1 connector 1 (AN/ANH) or slot *<x>* module *<y>* connector 1 (ASN).

Workaround: Note that the **show dial backup lines** command output on AN/ANH/ASN platforms refers to the only BRI connector on the specified board. Note also that in the output of the **lso**, **info**, **?**, and **show config** commands, the BCC displays this connector number correctly as bri/1/1 (AN/ANH) or bri/1/1/1 (ASN).

Title: After disabling the HTTP server object, BCC **show http** *<option>* commands display no entries.

Platform: All supported by the BCC

Number: 74807

Description: After disabling HTTP server, BCC **show http** *<option>* commands return “Object specified does not exist or is not accessible”.

Title: Commands imported from **show config** output incorrectly sequenced, preventing configuration of an IP interface with mask 255.255.255.224 (zero subnet).

Platform: All supported by the BCC

Number: 75008

Description: The BCC does not allow you to add an IP interface with a zero subnet mask (255.255.255.224) until you configure the IP global parameter "all-subnets" to "enabled." (Commands saved from the output of **show config** do not follow the correct sequence.)

Workaround: Before configuring an IP interface address with a zero subnet mask (255.255.255.224), first configure the global IP parameter "all-subnets" to "enabled." The same is true when importing configuration commands from a file created by saving the output of the BCC **show config** command. (Reorder the sequence of commands in the file as described above, then save the file.)

Title: Commands imported from **show config -file** output attempt to configure backup-pool and backup line objects in an incorrect sequence.

Platform: All supported by BCC

Number: 75041

Description: Commands imported from **show config -file** output attempt to configure backup-pool and backup line objects in an incorrect sequence.

Workaround: To successfully configure backup-pool and backup-line objects from **show config -file** output, manually reorder the sequence of commands in the file to configure all dial lines first, backup-pool next, and backup-circuit last.

Title: Response time for the BCC **show fr summary** command slows in proportion to the number of configured services.

Platform: BLN

Number: 75372

Description: BCC response time for the **show fr summary** command increases (becomes slower) in proportion to the number of configured services. For example, it takes the BCC 4 minutes to return a summary of 96 frame relay services, and approximately 20 minutes to return a summary of 192 services.

Title: Novell Server names are not aligned in **show ipx** services commands.

Platform: All supported by the BCC

Number: 75370

Description: When you enter the **show ipc services** or **show ipx service-addresses** command, IPX does not align the Novell server names correctly. They are offset by one from the other server names.

Title: Bus error when you enter **tic bcc**.

Platform: BLN

Number: 82919

Description: If you enter the command **tic bcc**, the router experiences a bus error.

Title: FE1 circuit information is included in **show serial stats** display.

Platform: BLN

Number: 84877

Description: When you enter the **show serial stats** command, the resulting display includes information about the FE1 circuit.