BayRS Version 12.01 and Site Manager Software Version 6.01 Release Notes

BayRS Version 12.01
Site Manager Software Version 6.01

Part No. 301894-A Rev. 00
March 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

Technical Support

Bay Networks Technical Publications

You can now print technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs*. Find the Bay Networks products for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

Documentation sets and CDs are available through your local Bay Networks sales office or account representative.

Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

Region	Telephone number	Fax number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 978-916-8880 (direct)	978-916-3514
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

Information about customer service is also available on the World Wide Web at *support.baynetworks.com*.

How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, call one of the following Bay Networks Technical Solutions Centers:

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	800-2LANWAN	978-916-3514
Santa Clara, CA	800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

Bay Networks Educational Services

Through Bay Networks Educational Services, you can attend classes and purchase CDs, videos, and computer-based training programs about Bay Networks products. Training programs can take place at your site or at a Bay Networks location. For more information about training programs, call one of the following numbers:

Region	Telephone number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 282 when prompted 978-916-3460 (direct)
Europe, Middle East, and Africa	33-4-92-96-15-83
Asia/Pacific	61-2-9927-8822
Tokyo and Japan	81-3-5402-7041

BayRS Version 12.01 and Site Manager Software Version 6.01 Release Notes

This document lists the anomalies (also referred to as bugs, change requests, or CRs) that have been fixed in Bay Networks® BayRS™ Version 12.01 and Site Manager Software Version 6.01. BayRS Version 12.01 includes all anomalies that were fixed in 12.00 Revisions 1, 2, and 3; Site Manager Software Version 6.01 includes all anomalies that were fixed in 6.00 Revisions 1, 2, and 3.

Use the BayRS Version 12.00 and Site Manager Software Version 6.00 documentation with BayRS Version 12.01 and Site Manager Software Version 6.01.

Maintenance Release Methodology

BayRS Version 12.01 and Site Manager Software Version 6.01 are Maintenance Releases.

Bay Networks is introducing a new methodology for releasing Bay Networks routing software.

Maintenance Releases are designated by a change in the second number to the right of the decimal point. They provide a collection of software bug fixes for the current Major Release. No new software or hardware features or functionality for either software or hardware is introduced beyond that already contained in the current Major Release.

A Maintenance Release will occur approximately each 3 to 4 months after a Major Release occurs. A Maintenance Release replaces the current Major Release (or the prior Maintenance Release) on the Price List and will become the current shipping version of BayRS. Each Maintenance Release will be a consolidation of the prior bug fixes made through Revision Releases, and will roll up all such software bug fixes provided by the recent Revision Releases.

Year 2000 Compliance

BayRS Version 12.01 and Site Manager Software Version 6.01 are Year 2000 Compliance Certified by Bay Networks. They have successfully passed Bay Networks Test Procedure which tests conformance to Bay Networks Year 2000 compliance definition, both of which can be found at Bay Networks Year 2000 Web Site at http://www.baynetworks.com/year2000/.

Image Builder Operational Note

If you are using Image Builder in Site Manager Software Version 6.10 to modify a BayRS Version 12.01 router image, you will receive an error. Please contact Bay Networks Customer Support to obtain the patch for this problem.

BayRS Version 12.01 Fixed Anomalies

Bay Networks has fixed the following anomalies in Version 12.01.

==========

SITE MANAGER COMPATIBILITY

==========

Router Version is managed by Site Manager version

v12.01 ----------> 6.01

v12.00 revision 1 ----------> 6.00 and 6.00 rev 1

v12.00 revision 2 ----------> 6.00 and 6.00 rev 2

v12.00 revision 3 ----------> 6.00 and 6.00 rev 3

==========

BayRS Version 12.01 corrects the following problems:

==========

CR 34749: DLSw.

If you delete DLSw from a circuit, then you disable DLSw globally, a bus error occurs.

CR 35587: IGMP.

If you have a static IGMP group, it does not age out. However, if the group receives an IGMP LEAVE message, the static group age time is erroneously set to the configured value and then aged out.

CR 30266: Frame Relay.

A bus error can occur in frame relay if a router receives frames destined for a frame relay source route interface while that interface is still initializing.

CR 34456: Frame Relay.

A fault may occur when you reboot a router with a configuration that was saved after certain dynamic configuration changes were made to frame relay.

CR 32296: ARN.

The ARN U interface Adapter Module will not respond to NT1 loop codes.

CR 32927: DECnet.

DECnet sends out an invalid packet, which causes other equipment to fail when the packet is received.

CR 34593: DECnet.

If you configure a 1 second hello timer on a DECnet interface, the router actually transmits a hello packet every 2.07 seconds.

CR 35156: DECnet.

The router advertises itself as unreachable when the global RouterLevel is set to level 1.

CR 33156: Scripts.

When you run the show bridge forward script to view the Learning Bridge forwarding table, and the table contains 4000 or more entries, the slot running the Technician Interface incurs a tag violation error.

CR 33356: FDDI.

In a Dual Homed configuration, PHY_A disconnects if a process runs too long in the CPU. The router reports a PHY_A disconnect and then, 50 seconds later, will put PHY_A back into standby mode. This could be a serious problem if PHY_B fails during those 50 seconds that PHY_A is disconnected.

CR 33880: DLSw.

DLSw does not use the Backup Peer Hold Down Timer after a TCP connection reset, only after the DLSw keepalives are exhausted.

CR 34771: DLSw.

Connections may fail to establish because the router does not send multiple CANUREACH messages when it receives multiple XID T2 Polls.

CR 30952: DLSw.

The DLS slot memory statistics show erroneous memory usage by this DLS slot. This condition reflects incorrect statistics and inhibits the establishment of new connections as the erroneous statistic is used to determine if DLS may acquire more memory from the system heap during connection establishment.

CR 34027: DVMRP.

DVMRP routes are not declared unreachable when the reporting neighbor times out. DVMRP waits for the route expiration timer to expire before updating those routes.

CR 34103: DVMRP.

Router does not always prune (s, g) caches for which there is neither a local member nor a downstream neighbor.

CR 34013: DVMRP.

If there is no DVMRP interface configured on the OSPF soloist slot, the router does not propagate MOSPF routes to other DVMRP slots.

CR 34336: DVMRP.

DVMRP fails to delete mask entries from routes_by_mask_utbl in the base environment. The mask entry should be deleted if it does not have a pointer to any routes in the main routing table.

CR 34890: DVMRP.

There is a race condition that may cause a bus error in MTM when DVMRP detects a routing change.

CR 34104: OSPF.

An ARP request can be generated out the wrong interface when the OSPF next hop for that network is in transition. A response from a device running proxy ARP at that time causes installation of the host route, which results in traffic being forwarded out of the wrong interface.

CR 33928: OSPF.

A router configured for OSPF may fail to properly advertise a Type2 LSA for a network on which it is the designated router. This results in a loss of connectivity to that network throughout the AS, and routers not using that network in their shortest path first calculations.

CR 34395: OSPF.

If you bounce an Autonomous System Border Router (ASBR) in an OSPF area, the Area Border Router (ABR) might permanently age out the Type 4 link for that ABR. This eliminates connectivity to that ASB's external routes for all routers outside of that area.

CR 30029: OSPF.

If the OSPF backup soloist is enabled and the router receives a database description (DD) packet with bad a checksum, the router generates a bus error.

CR 33035: OSPF.

The OSPF Multihop ECMP functionality fails to distribute networks across equal cost OSPF Point-to-Point paths in certain configurations.

CR 34155: OSPF.

An enhancement request to add gate statistic reporting capability to OSPF. This new feature enables you to determine how many buffers were processed after each run of the OSPF receive gate, and how many of each kind of OSPF messages were processed during that particular run.

CR 33984: OSPF.

An ABR will not originate a more specific summary net into a non-backbone area, when a less specific summary for that net is present in the non-backbone area. The ABR does not consider the validity of the less specific summary net, or whether the less specific summary net is even present in the backbone LSDB.

CR 33616: OSPF.

Both the designated router (DR) ineligible and DR eligible routers flap; they oscillate between down->init and init->down states.

CR 35249: OSPF.

On occasion, OSPF fails to boot because a bus error occurs in ospf_create_sum_lsdb+0x11a.

CR 34015: OSPF.

If you set the OSPF Range Status parameter to “not advertise” (in the OSPF range window of Site Manager or wfOspfAreaRangeEntry.wfOspfAreaRangeStatus), it does not hide the summary or prevent it from being advertised to the backbone area.

CR 34266: SDLC.

A DLC-SDLC DLSw connection does not recover after a virtual circuit is moved from an inactive to an active state.

CR 34754: IP.

A router, configured for Dial Optimized Routing and with the broadcast timer set to 24 hours, times out routing information protocol (RIP) routes before the broadcast timer expires.

CR 27260: IP.

If there are many hosts learned through the port, the IP host cache causes a slot reset when you enable it.

CR 32880: IP.

When telnetting from a BLN router configured for host-only mode, the router faults in ip_del.c at line 252. This occurs only on the first telnet attempt after you boot the router.

CR 33496: IP.

There is a problem in 11.02 and later, whereby a router does not cache any IP frames destined for hosts that are unresolved. Prior to 11.02, if a router received IP traffic destined for a local host for which it did not have an ARP entry, the router would cache up to the first 4 frames received for this host while attempting to resolve the address.

CR 33867: IP.

Enabling extended traffic filters in ISP mode causes a fault in ip_fwd_frag.

CR 33872: IP.

Packets are lost when you enable IP_ETF with ISP mode already enabled.

CR 34359: IP.

A router configured with ISP enabled and handling heavy traffic may encounter a BGP/OSPF soloist failure in ip_barp_operational_act+0x0 routing after the slot runs out of memory.

CR 34265: IP.

An error occurs in ISP mode resulting in a watchdog fault after BGP experiences multiple failed TCP connections.

CR 32277: IP.

RIP2 may advertise the same networks multiple times during a periodic update if a particular type of RIP policy filter is in place. The policy filter is configured to generate routes by placing a series of routes in the Advertise list while the Networks list is configured for the 0.0.0.0 / 0 range (all routes).

CR 34692: IP.

ISP mode experiences NFS timeouts.

CR 34809: X.25.

When X.25 sends messages to link access protocol balanced (LAPB) for IPEX in Gateway Mode, it occasionally sends them to the incorrect LAPB gate.

CR 34811: IPEX.

An error occurs when you bounce Link Access Protocol Balanced (LAPB), resulting in the following message: `System error, service attempting restart. Error in buf_float.c at line 113`.

CR 34816: IPEX.

Sometimes resets are not being sent because TCP cannot allocate a buffer.

CR 34817: IPEX.

In ipex_lapb_gw_send() in ipex_data.c, a message is sent to LAPB if there are no LAPB credits. But when the buffer used for this message is then freed, a buf float error occurs.

CR 34843: IPEX.

LAPB sometimes tries to send a LAPB_CONN_CONF message to IPEX Control Gate before IPEX is loaded, if the LAPB client type is not X25 (i.e., IPEX).

CR 34844: IPEX.

IPEX's TCP retry feature does not work in the IPEX Gateway Mode over direct LAPB.

CR 34845: IPEX.

When running IPEX Gateway Mode over direct LAPB, the session comes up, but no data is passed.

CR 26077: BGP.

If BGP is loaded onto more than one slot, or if there is a backup BGP soloist slot configured, it will not execute.

CR 28807: FTP.

When you boot a router with FTP disabled, you cannot initiate an FTP session to the router after enabling FTP.

CR 31649: PING-MIB

The reported IP ping round-trip times are incorrect. This affects both the TI ping command and the ping MIB.

CR 32394: Technician Interface.

A bus error may occur when using the embedded Technician Interface **enable/disable sync** command, and referencing the circuit by name, not by number.

CR 32457: IGMP.

Although it creates forwarding entries, IGMP does not always forward multicast packets.

CR 34068: IGMP.

An error occurs in igmp_xmit_act when you send rsvp path, igmp join, and rsvp resv messages to a router along with data.

CR 33672: SYNC.

If a port on an octal sync card receives an excessive amount of errors, it will cause lack of resource errors on the other ports that are on the same quic chip. Then, when the circuit experiencing the problem is disabled or fixed, the other ports continue to have lack of resource errors, even with minimal traffic load.

CR 33906: RSVP.

After you reset a circuit, downstream routers generate the following message: `No outgoing interfaces`.

CR 34085: QLLC.

A bus error occurs after you disable/enable the QLLC map entry twice.

CR 33674: QLLC.

When disabling X25QllcMapEntry, the state value does not change.

CR 34161: LLC.

A bus error occurs if you delete an interface with LLC2 when *llc.exe* is unloaded.

CR 34137: MOSPF.

The DLS slot fails if you globally disable MOSPF by selecting Protocols->IP->OSPF/MOSPF/QOSPF->Global and changing the Multicast Extensions option from “All Multicasting” to “None.”

CR 34450: MOSPF.

Multicast data flows do not fully recover after a hardware failure.

CR 34589: MOSPF.

When you repeatedly join/leave the same group, with a silence period of at least 30 seconds between each cycle, the traffic in the first 5 seconds may be dropped.

CR 33514: MOSPF.

After a reboot, the multicast bit is not turned on for some imported DVMRP routes.

CR 33571: MOSPF.

After rebooting a remote DVMRP router, traffic for source in the dvmrp cloud is not forwarded over pure MOSPF routes.

CR 34469: Frame Relay Traffic Shaping.

Traffic Shaping does not support values of 3/8, 5/8, etc. It is only able to deal with Tc values in the form of 1/n (1/3, 1/2, 1/4, etc.).

CR 34548: RIP.

A RIP announce policy filter does not work properly if configured to filter on OSPF TAG type.

CR 34596: SWSERV.

A fault occurs when you restart a BOD channel.

CR 29988: APPN.

The AN router experiences a fault in APPN, indicating that the system buffer is not large enough. This fault occurs only on the AN /E/S (Ethernet + Sync).

CR 32595: Telnet.

The ESC key (Escape) does not work if you telnet from a Bay Networks router to another Bay Networks router, and then telnet to a UNIX station.

CR 34024: BOT.

An enhancement request to enable the BayRS Bisync protocol to support more leading SYNC characters. Currently, the BISYNC code is hardcoded for 2 leading SYNC characters. The customer's Bisync controller requires 7 SYNC characters. The BayRS code requires configurable leading SYNC characters in order to interoperate.

CR 34484: PPP.

IP incorrectly considers the Maximum-Receive-Unit to include not only the Payload (information field), but the header as well. This can cause a discrepancy in the total packet size crossing the PPP line and the maximum protocol size.

CR 31530: RDISC.

A Zero Divide Bus Error occurs when you set the Min and Max Advertisement Interval to the same value when configuring Router Discovery.

CR 33780: Learning Bridge.

If you globally disable and then enable learning bridge (LB) on a slot, an error may occur where bridging fails to come back up on that slot.

CR 34112: DLSw.

When a router from another vendor sends frames with different circuit ID values to a receiving Bay Networks router, the Bay Networks router does not comply to RFC 1795 rules to reflect that the origin circuit ID values are unchanged, and not to vary the target circuit ID.

CR 34196: MOSPF.

This is a request to add new Technician Interface IP commands to display DVMRP routes, and for scheduling calculation.

CR 34783: Translation Bridge.

Packets larger than 1500 should be dropped if the translation bridge (XB) is configured for 802.3.

CR 33755: MOSPF.

This is a request to correct the imported DVMRP routes to AS external type 2, from the current type 1.

CR 32983: LOADER.

If there are two or more advanced routing engines (ARE) configured in one router, and you perform a named boot without specifying the *bn.exe* image or *config*, one of the AREs fails to load all of its executable files.

CR 34782: IGMP.

A bus error occurs when a frame relay interface configured with MOSPF fails.

CR 35039: MOSPF.

The router fails to reactivate the preferred route from a backbone area to a subnet, after restoration of a path that had previously failed.

CR 35115: X.25.

A bus error occurs when tearing down sessions during normal data transfer operations.

CR 34387: MIB II.

A multiline, multislot sync configuration returns zeroes or inaccurate values for wfIfEntry inoctets reported for that circuit.

CR 34704: MOSPF.

Multicast packets do not get forwarded after a topology change in a redundant network.

CR 34841: MOSPF.

Multicast packets do not get forwarded after bouncing a circuit with dual border routers.

CR 34938: MOSPF.

When a router is configured for bidirectional traffic and the topology is changed, traffic is restored in only one direction.

CR 35100: IPEX.

When a router is configured in IPEX Gateway Mode, it is unable to quickly bring up multiple sessions.

CR 35114: IPEX.

If you configure IPEX Gateway Mode over direct LAPB, it causes a bus error when the session restarts.

CR 30446: ATMZ.

Traffic is shaped differently when the “per-VC clipping” Atmizer feature is enabled than when it is disabled (default).

CR 34833: MOSPF.

A tag violation results when bouncing a circuit and sending multicast traffic.

CR 32052: TCP.

An enhancement request to enable TCP to record who closed a connection in the log, rather than merely that the connection was closed.

CR 35108: IPEX.

An enhancement request to identify IPEX log messages as error messages. Currently, only the function name and a value is logged, but it is not clear that the value is an error code.

CR 34893: ATMZ_ARE.

A problem exists in 11.02 (Revision 3 and later) that causes an Inter-Cell Gap that exceeds the configured Peak Cell Rate for a DS3 board.

CR 35065: TI.

When the date on a router is 2000 or greater (that is, 01/01/00), the **log** command using the **-d** function does not work correctly. Instead, the command displays the entire log.

CR 33958: Packet Capture

When using PCAP for a packet capture on a HSSI line, if the packet exceeds 140 bytes, PCAP will intermittently capture receive data before transmit. If the packet size is 160 bytes or more, PCAP always captures receive data before transmit.

CR 34387: TI.

A multiline, multislot sync configuration returns zeroes or inaccurate values for wfIfEntry entries reported for that circuit.

CR 34632: ATM.

An address exception error can occur in the ATMizer code when Per PVC cupping functionality is enabled.

CR 32167: AppleTalk.

A bus error occurs when you reset the AppleTalk base.

CR 34020: HSSI

Bursts of packets on a high-traffic HSSI line can cause an HSSI log message.

CR 35208: DLSw.

An llc/qllc topology degrades as traffic volume increases.

CR 35267: AT.

A bus error will occur in at_aptf.c @line 339 upon receipt of a MAC IP packet.

CR 35322: X.25.

If a configuration has multiple X.25 service records and you dynamically configure X.25 on a new slot (that is, for the first time), a g_map error occurs. This happens only using a dynamic configuration.

CR 34374: FireWall.

Multilayer 2 protocol encapsulation over different media fails if packets are received together in a list of buffers rather than one buffer at a time. Similarly, multilayer 3 protocols (e.g., IP and IPX) may not work either.

CR 32753: OSPF.

An area border router with area range summaries configured can get stuck in a load state while the other side of the adjacency is in a full state.

CR 33735: Switched Services.

When you attempt to configure DOR dynamically, a routing update (RIP/SAP for both IP and IPX) problem occurs, preventing the exchange of routes with the data packet call.

CR 33666: DLSw.

A reserved capx incorrectly returns an error code of DLS_CAPX_INVALID_CTRL_VEC_ID.

CR 33729: DLSw.

A VBM error may occur when DLS packets are fragmented in the network.

CR 33749: WCP.

A dial-on-demand circuit configured with WCP fails to come up when the other end of the circuit is a pre-12.00 router.

CR 30361: MIB.

The synchronous external clock speed fails to map over to the MIB II clock speed, causing improper aggregation between the internal and external lines.

CR 33155: SDLC.

An SDLC connection will be dropped when an ARN router sends a packet before it is polled.

CR 31684: DLSw.

Enhancement request to disable DLS multislot broadcasts from the DLC side.

CR 32854 and 33434: OSPF.

OSPF sends link state requests (LSR) when either the retransmit timer activated or a link state update (LSU) was received. Sending an LSR when an LSU was received results in multiple duplicate LSRs.

CR 31035: ATM.

When you disable the ATM driver, the ATM service record remains in an up state when it should be in a down state.

CR 32843: Telnet.

If you Telnet into the router via the ATM (LANE) port and disconnect abnormally (physically remove the Telnet client station off the network without disconnecting Telnet), the router fails to terminate the Telnet process.

CR 33330: Learning Bridge.

Resetting a learning bridge interface results in a bus error when you disable learning bridge globally. On an ARE, a Vector 2 MCP error can occur.

CR 19135: Source Route Bridge.

An enhancement request to produce a new script called **show srb traffic filters** that would function in the same manner as the **show ip traffic filters** script.

CR 32240: X.25.

Call requests are always cleared if full addressing is set to OFF.

CR 33151: IPEX.

A problem exists between 11.01 (and earlier) and 11.02 (and later) implementations of IPEX in which an 11.02 or later router cannot establish calls with an 11.00 router. A new MIB parameter, wfipexInscallingDte, has been added in the IPEX base. The default is disabled to prevent the calling DTE address from being added, but will allow router software version 11.02 or greater to interoperate with lower revisions of code.

CR 33379: DLSw.

ATM Data Direct fails to establish after the ATM link is disrupted.

CR 32580: Spanning Tree.

The Spanning tree algorithm fails to converge predictably under failure conditions.

CR 33181: RSVP.

The TSpec bucket rate, depth, and peak rate values get corrupted when the RSVP soloist is running on an ARE processor.

CR 33653: OSPF.

The TOS and metric fields in a summary link state update are corrupted.

CR 30499: IP.

Added the MIB variable wfBgpPeerEntry.wfBgpPeerASLoopDetect (Default value = disabled) to determine if a Peering session should be torn down if an AS-Loop is detected in the AS Path. In all cases the route(s) will be marked as unusable. Disabled = Peering will remain up.Enabled = Peering will be dropped.

CR 27239: Translation Bridge.

Enhancement request to allow packets larger than Ethernet to be translated. The current implementation allows only packet sizes of 1500. A new MIB parameter, wfBrXbFddiBridge, was added to the translation bridge base to allow FDDI and Token Ring size packets to be translated. You enable this parameter only if there are no Ethernet ports being used for translation bridge on the router. The mode must also be set to Ethernet II, not 802.3.

CR 25171: DECnet.

The router experiences a bus error when you delete DECnet in dynamic mode on a frame relay circuit.

CR 26560: SDLC.

You cannot establish an SNA session between a 3174 device configured as a pu2.1 device, an SDLC attached frad630 device connected to another frad630 device via frame relay (ban or bnn), and an Ethernet attached host (3172).

CR 32886: DLSw.

After a PU1 controller is disconnected and reconnected to the SDLC primary line on a router, DLSw fails to cycle properly between disconnected and established states. After entering an established state, the AS/400 sends an XID poll, which is transported across to the remote controller. The remote controller responds with an XID Final, which is transported back to the central site, received by DLSw and by the SDLC code, but never transmitted back to the AS/400.

CR 33853: DLSw.

The router faults when the MIB object wfDlsConnectionEntry is aged out.

CR 33921: SDLC.

An AN router can experience a bus error fault when you set the SDLC line to “VARY ON” on the AS400 for the remote SDLC controllers.

CR 33922: SDLC.

An AN router may experience a bus error fault when the SDLC is set to “VARIED OFF” on the AS400 for the remote SDLC controllers.

CR 33806: IPX.

The router stops passing IPX NetBIOS traffic in a frame relay group mode hub and spoke environment using NetBIOS static routes with Novell Conformance disabled.

CR 33778: OSPF.

When there are multiple ASBRs announcing default routes in their ASEs, the Technician Interface lists only one.

CR 33779: OSPF/MOSPF.

In a fail-over test involving Ethernet and FDDI, multicast failed to take the correct path through the Ethernet after the FDDI cable was removed. However, if the Ethernet cable was removed, multicast traffic successfully moved to the FDDI link.

CR 33056: IPX.

The router fails to apply two IPX filters of equal priority in the order in which they appear in the route filter table.

CR 33404: APPN.

A router configured for APPN may fault with tag violations.

CR 33785: DLSw.

When you globally disable DLS, wfDls.wfDlsTotalCircuits.0 shows active DLSw connections. wfDls.wfDlsTotalCircuits.0 should be set to zero when DLS is disabled.

CR 33764: APPN.

Large topology updates may not be completely exchanged when the sending CP is simultaneously receiving multiple updates from a third CP.

CR 33933: APPN.

When an EN (AS/400) has a large enough number of CP-CP sessions, the router that receives a Cross_Domain_Initiate GDS variable as a part of EN's LOCATE message incurs a tag violation. This problem stems from memory corruption during the allocation and release of buffers in Session Services.

CR 33700: RSVP.

A tag violation occurred on a router running Router Software Version 12.00 while starting the soloist.

CR 33120: Switched Services.

Routers running software version 11.01 and later send ISDN call setups requesting the same B channel on a PRI for successive calls. This condition occurs when attempting to establish multiple dial on demand or dial backup circuits in a short period of time.

CR 28383: Technician Interface.

A router experiences random faults and slot resets on an ARE slot while using the Technician Interface.

CR 34358: Technician Interface.

If you enter a year other than one between 1971 and 2070, the year will not be set correctly on the router. The router accepts only years between 1971 and 2070. If you use 2-digit notation, 71 through 99 becomes 1971 through 1999, and 00 through 70 becomes 2000 through 2070.

CR 33910: SYSLOG.

A bus error may occur when you telnet to a router on which SYSLOG and WCP are enabled.

CR 33307: IPX.

Packets are not always forwarded out the direct route. This problem can occur when an IPX route learned via RIP is also a directly connected route. If the route is learned through RIP first, and the cost of the RIP-learned route is less than the directly connected route, the directly connected route is dropped.

CR 34135: DLSw.

Heavy SDLC traffic volume occurring on the router may result in packet loss.

CR 34000: Firewall.

Communication between the FireWall router and the management station will not occur properly if the firewall control gate initializes on a slot that does not have the IP address used to communicate from the router to the management station.

CR 32814: Technician Interface.

When you disable a terminal attached to a router running the Technician Interface on an ARE card, the router enters the diagnostic state and fails to exit until you reset it.

CR 28911: GAME.

If you schedule a boot for the year 2000 or later, you receive a “Success” status message instead of a “Pending” status message.

CR 32980: GAME.

File Manager misinterprets file date stamps beyond the year 1999; it displays the date as the year 19xx.

CR 24909: Flash.

Routers will not boot using Hitachi Maxell type flash cards.

CR 33798: HW_PROCESSOR.

The router periodically checks to verify that the I/O module has not disconnected from the chassis by sending a signal to a certain pin on the I/O module. Noise occurring on that pin at the time of the check can cause the signal to be interpreted incorrectly, causing the router to generate the following message:

```
#   816: 07/08/97 08:31:03.769  WARNING  SLOT   MODULE   Code: 3

I/O module has been removed.
```

CR 33959: IPEX.

An enhancement request for the calling address insertion/overwrite feature. The alarm management system relies on the calling address field in the incoming call to identify the device reporting the alarm. The X.25 devices used in this network do not fill the calling address in their calling request packets. However, the alarm system still works because the public X.25 network inserts the correct calling address when it receives a call request with this field empty.

A new MIB variable, wfIpexMappingXlateCallingX121, has been created. When wfIpexInsCallingDte is enabled, the calling address is overwritten by the value specified in wfIpexMappingXlateCallingX121, if configured.

No CR: X.25 Operational Note.

If you create an X.25 Service entry in dynamic mode, you must reboot the router or reset the slot where the newly created entry is configured before the X.25 VC entry will be operational.

CR 34517: IPEX.

A problem in the Gateway Mode data flow routine causes calls not to be processed when there is no new data to process. This can cause data transfer to stop and never re-start for one-way traffic.

CR 34518: IPEX.

A problem in the Gateway Mode data flow routine causes the TCP window to be updated when data is stored in the data FIFO and by the value of an uninitialized variable. The TCP window should only be updated only when data is sent to PLP.

CR 34524: IPEX.

When IPEX detects that it received data from X.25 in out-of-sequence order, IPEX should drop the data instead of processing it.

CR 34525: X.25.

Error in PktDATind() in x25_lirif.c causes vc_env pointer to be tested for less than zero. Pointers are unsigned and are never less than zero.

CR 34519: IPEX.

The IPEX FSM does not process TCP_RETRY_CONT messages in the Established state.

CR 34520: IPEX.

The IPEX FSM does not process PLP_WIN_MSG in the Connected (CONN) state.

CR 34526: X.25.

When you boot a router with a disabled X.25 line, the log message always reports that line 1 is disabled for logical lines on an MCT1 circuit. The value 1 is not a valid line number. Line numbers are made up of channel, type, slot, module, and connector.

CR 34521: IPEX.

An error in the IPEX Gateway Mode routine can occur when data is sent to X.25 to test if there is PLP credit.

CR 34523: IPEX.

In IPEX FSM there is a case for IPEX_MSG_POLL_TCP message in 4 states, but there is no code that sends that message. Also there is no need to poll TCP. These cases should be removed.

CR 34522: IPEX.

In ipex_pri.h there is a define statement that uses an attribute that was deleted.

```
/* dynamically turn on logs through hidden mib parameter*/

#define IPEX_DEBUG_LOG_ON(ipex_env) \
(ipex_env->init_env->base_rec->wfIpexMaxSlotSessions == 1111)
```

The MIB attribute wfIpexMaxSlotSessions does not exist.

CR 33717: FDDI.

The DA30 was used to send SMT Port Management Request packets to the router. The response packet indicated that the long term link error rates on the ports were 10e-8 and 10e-15. The MIB indicated the link error rate to be 10e-15 on both ports.

CR 34582: X.25.

When the VC Gate environment is created for PVCs, the vc_state is init to X25_DATAXFR. This is incorrect because VC is not ready to transfer data; VC must wait for a client response message before entering the X25_DATAXFR state.

CR 34583: IPEX

When IPEX is in gateway mode and receives a reset when it is in the CONN state, it does not verify that the cause code is 09 (Operational) before switching to the EST state.

CR 34586: IPEX.

When IPEX receives a TCP Open request, it needs to send a connect request to X.25. However, no check is made to see if the needed circuit is operational. This leads to a bus error, no lapb buffers, and other errors.

CR 34584: IPEX.

The PLP bound FIFO needs to be flushed when you get a TCP_CLOSE_MSG in the IPEX Establish state before sending a Packet Level Reset request to X.25.

CR 34599: X.25.

You cannot configure LAPB Direct Interface-only circuits on SYNC and MCT1 interfaces.

CR 32864: IPEX.

If a failure occurs at the remote IPEX IP interface, IPEX can no longer establish TCP connections with the remote IPEX routers. An enhancement to the current IPEX implementation allows you to configure the secondary remote IP interface for backup using the new MIB attribute wfIpexMappingRemoteBackupIp.

CR 33576: X.25.

Attempting to scale X.25 to 10 PVCs over 24 T1 logical channels using the FRE2-040-32M causes a GAME system error. The same error occurs when attempting to scale X.25 to 32 PVCs over 24 T1 logical channels.

CR 33871: IPEX.

Clearing inbound X.25 calls causes bus errors to occur on a router configured with IPEX in end-to-end mode.

CR 32855: X.25.

PVC fails to come up after dynamically adding an X.25/PVC circuit.

CR 33410: IPEX.

If the X.25 client timer expires while IPEX is waiting for a clear confirmation from the remote X.25 connection (end-to-end mode only), X.25 will clear the call locally, causing the LCN to be freed. However, all structures related to the virtual connection (VC) do not get cleaned up properly. As a result, any calls placed to this LCN will fail.

CR 34290: X.25.

When you boot a router that has a configuration with a wfLapbPktEntry that is set to Disable, X.25 restarts with the following error message:

```
X25 System Error - DLRESind(), bad dlc_p pointer
```

CR 34292: X.25.

When you set multiple wfLapPktEntry variables to Disable using the Technician Interface and then enter the **commit** command, the router faults in mib_ent.c at line 726.

CR 34293: X.25.

When you disable an X.25 line, the log message reports that line 1 is disabled for logical lines on a MCT1 circuit. The value “1” is an invalid line number. Line numbers are made up of channel, type, slot, module, and connector.

CR 33714: IPEX.

The server process was disabled with 240 sessions running. When the listener process was restarted and the TCP connections had been reestablished, the server and router both showed over 280 established connections.

CR 34295: IPEX.

The IPEX FSM does not process DATA_IND messages in the Connected (CONN) state. IPEX can now go from the Established (EST) state to the CONN state and back to the EST state while maintaining active X.25 connections.

CR 33712: IPEX.

A PTOP virtual circuit may stop transmitting traffic on the network.

CR 33715/CR 34483: IPEX.

Traffic is started over 240 sessions at 45 percent capacity. Channel 1 is reset by toggling the wfLogicalLineDisable parameter on bln43 (client). Each time you reenable channel 1, traffic is restarted over it, eventually causing a bus error to occurs on the client-side router.

CR 34417: IPEX.

The IPEX audit gate checks for both a buflist and signal parameter each time the gate is scheduled. This violates GAME's operational model, which states that the signal parameter is valid only when buflist is set to NULL.

CR 34418: IPEX.

After receiving credits from X.25, IPEX should check whether it has data to send to X.25. If IPEX fails to perform this check, data could be retained in the FIFO.

CR 34419: IPEX.

Bad code segment occurring in IPEX FSM for the VC_DIED message while operating in an establish state.

CR 33716: IPEX.

Unable to restart IPEX client sessions on the router after terminating them.

Site Manager Software Version 6.01 Fixed Anomalies

==========

Site Manager Software Version 6.01 is a post 6.00 revision. This version is backward compatible and supports the following router software versions:

12.01

12.00

11.02

11.01

11.00

10.01

==========

Site Manager Software Version 6.01 corrects the following problems:

==========

CR 35251: OSPF.

Defaults are read from cdl-generated ASCII output files. Default values for MIBs of type GAUGE are represented as signed numbers. Site Manager is reading only type integer values as long unsigned integrations.

No CR: PPP.

When you select PPP Line Lists from the PPP Interface Lists window in dynamic mode, Site Manager terminates operation.

CR 33829: Logical Lines.

If you deselect the MCT card from the Add Circuit window, Site Manager does not allow you to re-select it.

CR 34761: X.25.

Site Manager grays out (deactivates or disables) the Flow Facility parameter on the X25 Service List window for all service types except IPEX.

CR 34906: Multilink/PPP.

Site Manager does not allow you to modify the Multilink Fragmentation parameter or the Multilink Trigger Size parameter on the PPP Interfaces window.

CR 34954: AppleTalk.

The Enable parameter should be the only parameter displayed in the Edit AppleTalk Global Parameters window, because MacIP is not supported.

CR 35261: LLC.

If you configure DLS/LLC on an ATM circuit, the LLC1 pull-down menu on the Service Record window is missing for that circuit.

CR 35142: OSPF.

When you reset the primary OSPF log mask, Site Manager resets the OSPF slot mask. The slot mask represents on which slots OSPF is eligible to run, and the log mask specifies which OSPF errors are written to the log.

CR 35182: IPEX.

Adding IPX to or deleting IPX from an 11.02 configuration terminates Site Manager operation.

CR 33513: Events Manager.

The events log displays the incorrect date for every year before the leap year.

CR 35226: IPEX.

The valid values in the Value field and in the Help window do not match for the Ipex Gateway Mapping PVC LCN entry. “Destination PVC LCN” should include a range between 1 and 4095.

CR 35239: X.25/QLLC.

When you configure X.25/QLLC Maps, Site Manager leaves the “Generate XID” field blank.

CR 35348: Router Redundancy.

Clicking on Edit Lines for Ethernet and 100Base-T router redundant interfaces brings up the 100Mb/s CSMA/CD parameters window, which is incorrect. Site Manager should bring up the Edit CSMA/CD parameters window. If you click on OK, Site Manager displays the following message: `ERROR: Invalid data entered for Interface Line Speed`. To exit the window, you must click on Cancel or enter an incorrect value for line speed.

CR 34152: IP Traffic Filters.

When you reorder the IP traffic filters, selecting “INSERT AFTER” inserts the filter before the precedence number that was selected, in either dynamic or local mode on a PC.

CR 34229: IP Traffic Filters.

Reordering filters on an interface with less than 32 filters disables the IP Extended Support parameter. When this happens, interfaces that require this parameter to be enabled will not apply any filter above the 32nd filter.

CR 34297: PPP.

BCP is not enabled for PPP when SRB or LB is configured on a switched services circuit (for example, dial on demand, dial backup, and hot standby). As a result, BCP is never negotiated when the dial circuit is established, and consequently, bridging does not work on that link.

CR 34527: BootP.

UNIX Site Manager appears to be querying Relay Agent Preferred Server information incorrectly.

CR 34039: NAT.

After you create an unnumbered point-to-point circuit, adding a NAT protocol to this circuit will not create a NAT interface entry instance.

CR 33887: Statistics Manager.

The Octets In and Octets Out fields for t_sync.dat within Statistics Manager do not get updated after you select Options -> Zero All Counters.

CR 34239: Router Redundancy.

An error occurs in Site manager (PC), whereby a general protection fault (GPF) results when you use the “edit lines” facility from the Edit Circuit window of a router redundant interface.

CR 34919/CR 35354: PPP.

When you enable the RFC I661 Compliance field in the PPP Line List window, wfSwservOptsRfc1661Compliance is enabled internally for a dial circuit.

CR 32366: ATM.

Site Manager sets the Per-VC Clipping parameter to an invalid value when you modify other parameters in the window.

CR 34819: LLC.

The LLC circuit pull-down option appears to the right of the Help option on the PC instead of to the right of the window pull-down option, as on the UNIX platform.

CR 32581: ARE.

When you click on a slot containing an ARE, DS3 or an ARE, E3 module, Site Manager displays the wrong part number. For an ARE, DS3, the correct part number is AG13110115; for an ARE, E3, the correct part number is AG13110114.

CR 34951: Static Routes.

Site Manager does not permit you to configure subnetted static routes.

CR 34717: ISDN.

Deleting a demand circuit dynamically fails to clear the local phone number entry.

CR 35118: BOD.

Site Manager allows Dynamic Monitor in the bandwidth mode for a leased line BOD, which should only be Monitor or Non-monitor. The Dynamic Monitor is only used for Demand circuit with BOD.

CR 33967: IP.

When selecting Protocols/IP/RIP Interfaces from the Site Manager menu in Configuration Manager, Site Manager faults. This condition occurs on both UNIX and PC platforms.

CR 34335: Frame Relay.

When you delete a frame relay PVC or service record, Site Manager does not display a confirmation prompt.

CR 34367: Source Route Bridge.

Site Manager does not allow you to add source route bridge (SRB) to a token ring interface. SRB is not on the Protocols menu.

CR 34370: DLSw.

If you add DLSw to a second token ring network, Site Manager sets the Bridge ID parameter to 0.

CR 34407: Site Manager.

If you delete LLC from a token ring interface, Site Manager also removes source route bridge from the interface. This happens with SunOS and Win95 Site Manager.

CR 34199: OSPF.

Site Manager does not allow you to configure OSPF and DVMRP on the same circuit.

CR 33557: X.25

The QLLC window contains two parameters, PU type and Generate XID, for which Site Manager requires you to enter valid values. However, when you enter values, exit the window and then reenter the window, Site Manager clears the values from the fields.

CR 34391: DLSw

When you configure a new DLSw/SDLC circuit in dynamic mode, the Source SAP and Destination SAP parameters are missing from the DLS Local Device Configuration window. Also, Site Manager corrupts the values you entered for the Source MAC and Destination MAC parameters.

CR 33935: ATM.

A program error occurs when you click the SAAL button from the Edit ATM Connector window in Site Manager.

CR 34119: Site Manager.

Site Manager does not allow you to change the name of an ISDN leased line configured on a BRI interface when using the Change Lines option from the Circuit Definition window.

CR 33521: MCT1-E1

The error message `Protocol ST2 or RSVP must be configured to edit line resources` appears when you attempt to edit logical line resources on a non-PRI circuit.

CR 32524: PPP.

A new PPP parameter, RFC 1661 Compliance, has been added in the PPP line list. Enabling this field will allow the router to run in compliance with RFC 1661.

CR 33299: ATM.

The SSCS TYPE field is not listed when you display an IP interface in Site Manager.

CR 28617: Site Manager.

When you configure a local phone number on a version 9.00 router using Site Manager 4.00 or greater, an SNMP set error occurs.

CR 29030: Switch Services.

Site Manager allows you to configure a standby primary circuit configured as a frame relay backup primary circuit.

CR 33151: IPEX.

A problem exists between 11.00 and 11.02 (and later) implementations of IPEX in which an 11.02 router cannot establish calls with an 11.00 router. Bay Networks has added a new IPEX parameter, Insert Calling DTE Address. The default is Disabled to prevent the calling DTE address from being added, but will allow router software version 11.02 or greater to interoperate with lower revisions of code.

CR 33626: Multiline.

Configuring multiline PPP over HSSI interfaces using Site Manager Dynamic Configuration does not work. wfCctOptsEntry instances are deleted during configuration.

CR 26320: PPP.

If you select a primary circuit from the Primary Circuit Definition Dialog box, and then click on OK to exit from the box, Site Manager changes the CHAP/PAP password to the default.

CR 28205: Interface Redundancy

Site Manager experiences a General Protection Fault (GPF) when you try to configure interface redundancy for router interfaces on a 5000 router. This problem was found in Site Manager Version 5.0.

CR 33533: HSSI.

Site Manager uses 16 as the default when setting the HSSI CRC size. According to the MIB, Site Manager should use 32 as the default.

CR 26479: Statistics Manager.

If you view IPX circuit information for an inoperable or inactive interface, the Statistics Manager displays the incorrect network and MAC address for that circuit.

CR 33004: Report Generator.

Report Generator cannot write to the root directory of a PC.

CR 33277: IP.

The TR End Station ARP type should not be an available option when editing the IP interface entry of a demand circuit group.

CR 29473: NTP.

IP Mask defaults to 0.0.0.0 in the NTP Access Configuration List window.

CR 28170: Router Redundancy.

Router Redundancy should allow you to select between 2 types of redundancy (new and old).

CR 33823: ARN:Sync.

The SYNC parameter screen for the V34 modem is missing the WAN Serial Interface Type field.

CR 33181: RSVP.

The TSpec bucket rate, depth, and peak rate values get corrupted when the RSVP soloist is running on an ARE processor.

CR 33665: DLSw.

Changing the source route Interface RD value on the DLSw Basic Interface window causes Site Manager to create a new source route interface.

CR 33931: Site Manager.

After you install Site Manager, a message should appear, indicating the environment variables that need to be defined to run Site Manager.

CR 33843: CRM.

When editing an existing CRM line entry on the PC, an error message appears.

CR 33299: ATM_RFE.

SSCS TYPE field for IBM's ATMARP SRV is not listed when displaying an IP interface in Site Manager.

CR 33602: IP.

Site Manager allows static routes with invalid subnets to be created.

CR 33482: ARN:ISDN.

If you open a local configuration file with an ISDN adapter module Port Application Mode configured for 2B+D, Site Manager displays the following message: WARNING: Empty Module 2 has circuits configured.

CR 33926: DLSw.

When you set the Source Route Internal LAN ID and the Source Route Bridge ID fields in the DLSw Basic Global window and click on OK, the values do not get saved.

CR 33787: ISDN.

There is a problem with Site Manager that may result in Site Manager erroneously enabling BOFLs on an MCT-1 module. If you select a primary circuit on an MCT-1 module from the Dial Backup Circuits window, click on Cct Type to display the Circuit Type and the Backup Pool ID, and then click on OK without making changes, BOFLs are enabled on all logical lines of the MCT-1. This action causes all dial-on-demand and dial backup circuits configured on that port to lose connectivity.

CR 33797: IP Traffic Filters.

A traffic filters tag violation may occur on a router after you dynamically create a Drop action IP filter.

CR 33796: IP Traffic Filters.

Site Manager lets you create IP traffic filters (Forward to IP Destination Address, Forward to Next Hop, and Forward to Next Hop Interface), but you cannot edit them with Site Manager locally or dynamically.

CR 33513: Site Manager - Admin.

To change the year on the router to the year 2000, on the Router Date and Time window from the Admin option, you move the year slider to 0. Then, use the Technician Interface date function to validate that 0 corresponds to 2000. The Router Date and Time window should be changed to accept four digits; you should not be expected to know that 0 equals 2000.

CR 34208: Scheduled Boot.

A Scheduled Boot should allow the date to be set between 1971-2070.

CR 33311: DLSw.

On Token Ring and Ethernet interfaces, Site Manager provides an LLC Interface pull-down selection that allows you to select LLC1 or LLC2. From there, you can access the DLSw interface definitions. This function is missing for ATM Interfaces. From the ATM Service Record, only the Protocol Add/Delete and Edit menus are displayed. You cannot access the DLSw interface from the default LLC1 view.

CR 33667: Source Route Bridging.

Site Manager should support Source Route Bridging over ATM DXI, using RFC 1483 and RFC 1490 encapsulation.

CR 34152: IP Traffic Filters.

When reordering the IP traffic filters, selecting INSERT AFTER inserts the filter before the precedence number you selected. This happens in both dynamic and local mode.

CR 34033: IP Traffic Filters

Site Manager faults when trying to edit an inbound IP traffic filter dynamically in Configuration Manager.

CR 33719: IPEX.

After you delete all entries on the IPEX Mapping Table Configuration list screen, the Add, Delete, and Apply buttons are no longer displayed, making it impossible to add a new mapping without having to back out of this screen and go back in.

CR 33720: IPEX.

Every time you delete an X.25 IPEX service record, a confirmation prompt appears, making the task of deleting several service records a laborious one.

CR 33721: LAPB.

The values range for the TCP Port parameter on the LAPB IPEX Mapping Add window is incorrect. The text for the parameter should also be changed to Remote TCP Port.

CR 33722: LAPB.

When you delete a LAPB Gateway circuit, the wfLapbEntry for that circuit is not deleted.

CR 33765: X.25.

The X25.mib has a new attribute (wfLapbPktPduSize) used to configure X.25 with the maximum message size from the X.25 client. A new parameter, Client PDU Size, needs to be added to Site Manager to configure this attribute in the X.25 Packet Configuration window.

CR 32864: IPEX.

If a failure occurs at the remote IPEX IP interface, IPEX can no longer establish TCP connections with the remote IPEX routers. An enhancement to the current IPEX implementation allows you to configure the secondary remote IP interface for backup using the new MIB attribute wfIpexMappingRemoteBackupIp. The new IPEX parameter in Site Manager is Remote Backup IP Address.

CR 34599: LAPB.

Site Manager does not allow you to configure LAPB Direct Interface circuits on SYNC and MCT-1 interfaces.