

Release Notes for Router Software Version 11.00 Revision 4n

Router Software Version 11.00 Rev. 4n
Site Manager Software Version 5.00 Rev. 4n

Part No. 114968-A Rev. A
November 1996



Bay Networks

Copyright © 1988–1996 Bay Networks, Inc.

All rights reserved. Printed in the USA. November 1996.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, Optivity, PPX, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, BayStack, Bay•SIS, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, PathMan, PhonePlus, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

USA Requirements Only

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

This equipment generates, uses, and can radiate radio-frequency energy. If you do not install and use this equipment according to the instruction manual, this product may interfere with radio communications. This product has been tested and found to comply with the limits for a Class A computing device, pursuant to Subpart J of Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Operating this equipment in a residential area is likely to interfere with radio communications; in which case, the user, at his/her own expense, must correct the interference.

Shielded-compliant cables must be used with this unit to ensure compliance with the Class A limits.

EN 55 022 Declaration of Conformance

This is to certify that the Bay Networks products in this book are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022:1987 Class A (CISPR 22:1985/BS 6527:1988).

EN 55 022 Declaration of Conformance

This is to certify that the Bay Networks products in this book are shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022:1987 Class B (CISPR 22:1985/BS 6527:1988).

Japan/Nippon Requirements Only

Voluntary Control Council for Interference (VCCI) Statement

この装置は、第一種情報装置（商工業地域において使用されるべき情報装置）で、商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会（VCCI）基準に適合しております。

従って、住宅地域、その隣接地域等で使用した場合、ラジオ、テレビ受信機等に障害を与えることがあります。

上記基準に適合する遮蔽ケーブルをご自分でお求めになり、取扱説明書に従って、正しくご使用ください。

Voluntary Control Council for Interference (VCCI) Statement

This equipment is in the 1st category (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines that are aimed at preventing radio interference in commercial and/or industrial areas.

Consequently, when this equipment is used in a residential area or in an adjacent area thereto, radio interference may be caused to equipment such as radios and TV receivers.

Compliance with the applicable regulations is dependent upon the use of shielded cables. The user is responsible for procuring the appropriate cables. Read instructions for correct handling.

Canada Requirements Only

Canada CS-03 Rules and Regulations

Note: The Canadian Department of Communications label identifies certified equipment. The certification means that the equipment meets certain telecommunications network protective operations and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent the degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

Canada CS-03 — Règles et règlements

Note: L'étiquette du ministère des Communications du Canada indique que l'appareillage est certifié, c'est-à-dire qu'il respecte certaines exigences de sécurité et de fonctionnement visant les réseaux de télécommunications. Le ministère ne garantit pas que l'appareillage fonctionnera à la satisfaction de l'utilisateur.

Avant d'installer l'appareillage, s'assurer qu'il peut être branché aux installations du service de télécommunications local. L'appareillage doit aussi être raccordé selon des méthodes acceptées. Dans certains cas, le câblage interne du service de télécommunications utilisé pour une ligne individuelle peut être allongé au moyen d'un connecteur certifié (prolongateur téléphonique). Le client doit toutefois prendre note qu'une telle installation n'assure pas un service parfait en tout temps.

Les réparations de l'appareillage certifié devraient être confiées à un service d'entretien canadien désigné par le fournisseur. En cas de réparation ou de modification effectuées par l'utilisateur ou de mauvais fonctionnement de l'appareillage, le service de télécommunications peut demander le débranchement de l'appareillage.

Pour leur propre sécurité, les utilisateurs devraient s'assurer que les mises à la terre des lignes de distribution d'électricité, des lignes téléphoniques et de la tuyauterie métallique interne sont raccordées ensemble. Cette mesure de sécurité est particulièrement importante en milieu rural.

Attention: Les utilisateurs ne doivent pas procéder à ces raccordements eux-mêmes mais doivent plutôt faire appel aux pouvoirs de réglementation en cause ou à un électricien, selon le cas.

Canada Requirements Only *(continued)*

D. O. C. Explanatory Notes: Equipment Attachment Limitations

The Canadian Department of Communications label identifies certified equipment. This certification meets certain telecommunication network protective, operational and safety requirements. The department does not guarantee the equipment will operate to the users satisfaction.

Before installing the equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above condition may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Notes explicatives du ministère des Communications: limites visant les accessoires

L'étiquette du ministère des Communications du Canada indique que l'appareillage est certifié, c'est-à-dire qu'il respecte certaines exigences de sécurité et de fonctionnement visant les réseaux de télécommunications. Le ministère ne garantit pas que l'appareillage fonctionnera à la satisfaction de l'utilisateur.

Avant d'installer l'appareillage, s'assurer qu'il peut être branché aux installations du service de télécommunications local. L'appareillage doit aussi être raccordé selon des méthodes acceptées. Dans certains cas, le câblage interne du service de télécommunications utilisé pour une ligne individuelle peut être allongé au moyen d'un connecteur certifié (prolongateur téléphonique). Le client doit toutefois prendre note qu'une telle installation n'assure pas un service parfait en tout temps.

Les réparations de l'appareillage certifié devraient être confiées à un service d'entretien canadien désigné par le fournisseur. En cas de réparation ou de modification effectuées par l'utilisateur ou de mauvais fonctionnement de l'appareillage, le service de télécommunications peut demander le débranchement de l'appareillage.

Pour leur propre sécurité, les utilisateurs devraient s'assurer que les mises à la terre des lignes de distribution d'électricité, des lignes téléphoniques et de la tuyauterie métallique interne sont raccordées ensemble. Cette mesure de sécurité est particulièrement importante en milieu rural.

Attention: Les utilisateurs ne doivent pas procéder à ces raccordements eux-mêmes mais doivent plutôt faire appel aux pouvoirs de réglementation en cause ou à un électricien, selon le cas.

Canada Requirements Only *(continued)*

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Access Feeder Node, Access Link Node, Access Node, Access Stack Node, Backbone Concentrator Node, Backbone Concentrator Node Switch, Backbone Link Node, Backbone Link Node Switch, Concentrator Node, Feeder Node, Link Node) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (Access Feeder Node, Access Link Node, Access Node, Access Stack Node, Backbone Concentrator Node, Backbone Concentrator Node Switch, Backbone Link Node, Backbone Link Node Switch, Concentrator Node, Feeder Node, Link Node) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

T1 Service Compliance Statements

T1 Service

NOTE: This T1 Service notice applies to you only if you have received a single or dual port Multi-Channel T1 (MCT1) Link Module (which provides an internal CSU).

This equipment complies with Part 68 of FCC Rules. Please note the following:

1. You are required to request T1 service from the telephone company before you connect the CSU to a T1 network. When you request T1 service, you must provide the telephone company with the following data:
 - The Facility Interface Code
Provide the telephone company with both codes below:
 - 04DU9-B (1.544 MB D4 framing format)
 - 04DU9-C (1.544 MB ESF format)The telephone company will select the code it has available.
 - The Service Order Code: 6.0F
 - The required USOC jack: RJ48C
 - The make, model number, and FCC Registration number of the CSU.
2. Your telephone company may make changes to its facilities, equipment, operations, or procedures that could affect the proper functioning of your equipment. The telephone company will notify you in advance of such changes to give you an opportunity to maintain uninterrupted telephone service.
3. If your CSU causes harm to the telephone network, the telephone company may temporarily discontinue your service. If possible, they will notify you in advance, but if advance notice is not practical, you will be notified as soon as possible and will be informed of your right to file a complaint with the FCC.
4. If you experience trouble with the CSU, please contact Bay Networks Technical Response Center in your area for service or repairs. Repairs should be performed only by service personnel authorized by Bay Networks, Inc.

United States	1-800-2LAN-WAN
Valbonne, France	(33) 92-96-69-68
Sydney, Australia	(61) 2-9927-8880
Tokyo, Japan	(81) 3-5402-7041
5. You are required to notify the telephone company when you disconnect the CSU from the network and when you disconnect the BCNX or BLNX from the network.

Bay Networks Software License



Note: This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license — or the license included with the particular product — shall govern licensee’s use of Bay Networks software.

This Software License shall govern the licensing of all software provided to licensee by Bay Networks (“Software”). Bay Networks will provide licensee with Software in machine-readable form and related documentation (“Documentation”). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product (“Equipment”) that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee’s facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee’s permission to use the Software at licensee’s facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

Technical Support and Online Services

Bay Networks Customer Service	xvi
Bay Networks Information Services	xvii
World Wide Web	xvii
Customer Service FTP	xvii
Support Source CD	xviii
CompuServe	xviii
InfoFACTS	xix
How to Get Help	xix

Release Notes for Router Software Version 11.00 Revision 4n

Upgrading to Version 11.00/5.00 Rev. 4n	1-1
New Features	1-2
Dial Services	1-2
Dial Backup of Multilink Leased Lines	1-2
Dial Backup over Frame Relay	1-2
Dial Optimized Routing	1-2
Inactivity Mode	1-2
Traffic Filters	1-3
BRI Leased Line Operation for Japan	1-3
Frame Relay Service Records	1-3
Point-to-Point Protocol (PPP) Services	1-3
Additional Lines in a Multilink Bundle	1-3
Multilink Fragmentation	1-4
One-Way Authentication	1-4
Disabling Loopback Detection	1-4
X.25 Services	1-4
IPEX	1-4
X.25 Support for RFC 1356	1-5
Data Link Switching (DLSw) Services	1-5

IP Services	1-6
RIP Support for Dial-Optimized Routing	1-6
IP Accounting Support for Frame Relay Interfaces	1-6
ISP Mode	1-7
Dynamic BGP Policy Configuration	1-7
BGP Communities	1-7
Simplified Regular Expressions for BGP AS Pattern Matching	1-7
Static Host Entry Support for IGMP	1-8
Interface Redundancy	1-8
NTP Support	1-8
Technician Interface Diags Command	1-8
New and Enhanced Technician Interface Scripts	1-9
Enable/Disable DCM Scripts	1-10
Show DCM Scripts	1-10
Show Sync Scripts	1-13
New Log Event Messages	1-17
Modem Events	1-17
DSU/CSU Events	1-20
Guidelines for Using Version 11.00 Rev. 4n	1-22
ARN Memory Requirements	1-22
Using the Technician Interface ARN Installation Script	1-22
Cycling Power to the ARN	1-22
IP Equal-Cost Multipath Routing	1-23
DCM Software Image and Router Software Compatibility	1-23
Joining an Incompatible Emulated LAN	1-23
Support for Banyan 80C4 ISAP	1-23
Using IPX Dial Optimized Routing (DOR)	1-24
Inactivity Mode	1-24
RIP/SAP Pace and Packet Size Parameters	1-24
Diagnostic Packets and Time Synchronization	1-24
Using Frame Relay Service Records	1-24
Using Demand Circuits for Backup	1-27
Protocols Supported	1-29
Standards Supported	1-31
Supported Flash Memory Cards	1-36

Tables

Table 1. Standards Supported by Version 11.00 Rev. 4n 1-31

Table 2. Approved Flash Memory Cards 1-36

Technical Support and Online Services

To ensure comprehensive network support to our customers and partners worldwide, Bay Networks Customer Service has Technical Response Centers in key locations around the globe:

- Billerica, Massachusetts
- Santa Clara, California
- Sydney, Australia
- Tokyo, Japan
- Valbonne, France

The Technical Response Centers are connected via a redundant Frame Relay Network to a Common Problem Resolution system, enabling them to transmit and share information, and to provide live, around-the-clock support 365 days a year.

Bay Networks Information Services complement the Bay Networks Service program portfolio by giving customers and partners access to the most current technical and support information through a choice of access/retrieval means. These include the World Wide Web, CompuServe, Support Source CD, Customer Support FTP, and InfoFACTS document fax service.

Bay Networks Customer Service

If you purchased your Bay Networks product from a distributor or authorized reseller, contact that distributor's or reseller's technical support staff for assistance with installation, configuration, troubleshooting, or integration issues.

Customers can also purchase direct support from Bay Networks through a variety of service programs. As part of our PhonePlus™ program, Bay Networks Service sets the industry standard, with 24-hour, 7-days-a-week telephone support available worldwide at no extra cost. Our complete range of contract and noncontract services also includes equipment staging and integration, installation support, on-site services, and replacement parts delivery -- within approximately 4 hours.

To purchase any of the Bay Networks support programs, or if you have questions on program features, use the following numbers:

Region	Telephone Number	Fax Number
United States and Canada	1-800-2LANWAN; enter Express Routing Code (ERC) 290 when prompted (508) 436-8880 (direct)	(508) 670-8766
Europe	(33) 92-968-300	(33) 92-968-301
Asia/Pacific Region	(612) 9927-8800	(612) 9927-8811
Latin America	(407) 997-1713	(407) 997-1714

In addition, you can receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your authorized partner.

Bay Networks Information Services

Bay Networks Information Services provide up-to-date support information as a first-line resource for network administration, expansion, and maintenance. This information is available from a variety of sources.

World Wide Web

The Bay Networks Customer Support Web Server offers a diverse library of technical documents, software agents, and other important technical information to Bay Networks customers and partners.

A special benefit for contracted customers and resellers is the ability to access the Web Server to perform Case Management. This feature enables your support staff to interact directly with the network experts in our worldwide Technical Response Centers. A registered contact with a valid Site ID can

- View a listing of support cases and determine the current status of any open case. Case history data includes severity designation, and telephone, e-mail, or other logs associated with the case.
- Customize the listing of cases according to a variety of criteria, including date, severity, status, and case ID.
- Log notes to existing open cases.
- Create new cases for rapid, efficient handling of noncritical network situations.
- Communicate directly via e-mail with the specific technical resources assigned to your case.

The Bay Networks URL is *<http://www.baynetworks.com>*. Customer Service is a menu item on that home page.

Customer Service FTP

Accessible via URL *<ftp://support.baynetworks.com>* (134.177.3.26), this site combines and organizes support files and documentation from across the Bay Networks product suite, including switching products from our Centillion™ and Xylogics® business units. Central management and sponsorship of this FTP site lets you quickly locate information on any of your Bay Networks products.

Support Source CD

This CD-ROM -- sent quarterly to all contracted customers -- is a complete Bay Networks Service troubleshooting knowledge database with an intelligent text search engine.

The Support Source CD contains extracts from our problem-tracking database; information from the Bay Networks Forum on CompuServe; comprehensive technical documentation, such as Customer Support Bulletins, Release Notes, software patches and fixes; and complete information on all Bay Networks Service programs.

You can run a single version on Macintosh Windows 3.1, Windows 95, Windows NT, DOS, or UNIX computing platforms. A Web links feature enables you to go directly from the CD to various Bay Networks Web pages.

CompuServe

For assistance with noncritical network support issues, Bay Networks Information Services maintain an active forum on CompuServe, a global bulletin-board system. This forum provides file services, technology conferences, and a message section to get assistance from other users.

The message section is monitored by Bay Networks engineers, who provide assistance wherever possible. Customers and resellers holding Bay Networks service contracts also have access to special libraries for advanced levels of support documentation and software. To take advantage of CompuServe's recently enhanced menu options, the Bay Networks Forum has been re-engineered to allow links to our Web sites and FTP sites.

We recommend the use of CompuServe Information Manager software to access these Bay Networks Information Services resources. To open an account and receive a local dial-up number in the United States, call CompuServe at 1-800-524-3388. Outside the United States, call 1-614-529-1349, or your nearest CompuServe office. Ask for Representative No. 591. When you are on line with your CompuServe account, you can reach us with the command **GO BAYNET**.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system has libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system responds to a fax from the caller or to a third party within minutes of being accessed.

To use InfoFACTS in the United States or Canada, call toll-free 1-800-786-3228. Outside North America, toll calls can be made to 1-408-764-1002. In Europe, toll-free numbers are also available for contacting both InfoFACTS and CompuServe. Please check our Web page for the listing in your country.

How to Get Help

Use the following numbers to reach your Bay Networks Technical Response Center:

Technical Response Center	Telephone Number	Fax Number
Billerica, MA	1-800-2LANWAN	(508) 670-8765
Santa Clara, CA	1-800-2LANWAN	(408) 764-1188
Valbonne, France	(33) 92-968-968	(33) 92-966-998
Sydney, Australia	(612) 9927-8800	(612) 9927-8811
Tokyo, Japan	(81) 3-5402-0180	(81) 3-5402-0173

Release Notes for Router Software Version 11.00 Revision 4n

This document contains the latest information about Bay Networks[™] Router Software Version 11.00 Revision 4n.

Version 11.00 Rev. 4n contains support for BayStack[™] Advanced Remote Node[™] (ARN[™]) hardware, plus all new features and enhancements of Bay Networks Router Software Version 11.0.

These release notes include information about

- [Upgrading to Version 11.00/5.00 Rev. 4n](#)
- [New Features](#)
- [Guidelines for Using Version 11.00 Rev. 4n](#)
- [Protocols Supported](#)
- [Standards Supported](#)
- [Supported Flash Memory Cards](#)

Upgrading to Version 11.00/5.00 Rev. 4n

To upgrade your router software to Version 11.00 Rev. 4n, or to upgrade your Site Manager software to Version 5.00 Rev. 4n, refer to *Upgrading Routers from Version 7-9.xx to Version 11.0* for instructions. This document is included in your upgrade package.

New Features

Bay Networks has implemented many changes to the router software for Version 11.00 Rev. 4n. This section describes the major new features.

Dial Services

The following features are new for dial services. For important information about using demand circuits for backup, see “[Guidelines for Using Version 11.00 Rev. 4n](#),” later in these release notes.

Dial Backup of Multilink Leased Lines

Dial backup service is now available for leased multilink connections. In previous releases, it was available for only a single leased line or a leased multiline (Standard and PPP only). For more information, refer to *Configuring Dial Services*, Chapter 1.

Dial Backup over Frame Relay

Dial backup service is now available for an entire Frame Relay interface using Frame Relay across the backup circuit. You can now back up the entire Frame Relay interface, which means you can back up multiple PVCs instead of just one PVC. In previous releases, you could only back up a single Frame Relay PVC using PPP across the backup circuit. For more information, refer to *Configuring Dial Services*, Chapter 1.

Dial Optimized Routing

Dial optimized routing lets you exchange IP RIP and IPX RIP/SAP routing updates when a connection is active for data transmission. By limiting when the router can send updates, dial optimized routing reduces unnecessary connections and line costs. For more information, see *Configuring Dial Services*, Chapter 4.

Inactivity Mode

We have added inactivity mode and inactivity timer parameters to monitor inactivity based on the direction of traffic (transmit, receive, both, or either). You can configure inactivity mode for both inbound and outbound traffic. PPP's LQR, LCP, and periodic CHAP messages will not reset inactivity. For more information, refer to *Configuring Dial Services*, Chapter 8.

Traffic Filters

We have added new rules for traffic filters. To prevent routing updates and protocol-specific messages from keeping the circuit up, you can configure traffic filters that specify which packets are permitted across an established dial-up line and which packets are prevented from bringing up a dial-up line. You can also filter outbound packets to prevent the inactivity timer from resetting. For more information, refer to *Configuring Dial Services*, Chapter 4.

BRI Leased Line Operation for Japan

For BRI service in Japan, the router allows you to support a permanent point-to-point ISDN connection over a B channel without having to use the D channel to dial the call. This connection operates like a leased line. This option is useful when ISDN service providers do not use the D channel. For more information, refer to *Configuring Dial Services*, Chapter 3.

Frame Relay Service Records

Bay Networks now uses *service records* to define Frame Relay circuits. A service record is a data structure that allows flexible grouping and characterization of PVCs. A service record can contain a single PVC or multiple PVCs. For further information about Bay Networks implementation of service records, refer to *Configuring Frame Relay Services*. For information about how service records differ from access modes, see “[Guidelines for Using Version 11.00 Rev. 4n](#),” later in these release notes.

Point-to-Point Protocol (PPP) Services

The following features are new for PPP.

Additional Lines in a Multilink Bundle

The maximum number of lines allowed in a multilink bundle is now 30. The actual practical maximum depends on the nature of the network traffic and the network configuration.

Multilink Fragmentation

Enabling fragmentation means that PPP can split packets when necessary for better performance. With fragmentation enabled, PPP can split packets into fragments, then send the fragments over the lines in the multilink bundle, reassembling them on the receiving peer into the proper sequence. You can specify the minimum packet size to be considered for fragmentation. Multilink fragmentation is implemented as described in RFC 1717.

One-Way Authentication

One-way authentication uses an authentication protocol on only one side of a dial-up connection. The router placing the call disables the authentication protocol for a circuit, while the router on the receiving side enables authentication. Disabling the outbound authentication lets the router interoperate with other devices that may not allow two-way authentication or support CHAP. To use one-way authentication, you must also configure certain options for the switched circuit itself. See *Configuring Dial Services* for a description of how you must set up dial services to enable one-way authentication.

Disabling Loopback Detection

As part of its network integrity checking, PPP tests for a loopback condition in which, effectively, the router is talking with itself and not communicating with the network. For test purposes, you can now disable this loopback detection feature.

For more information on these features, refer to *Configuring PPP Services* and *Configuring Dial Services*.

X.25 Services

We have added the following new features to the X.25 services:

IPEX

Bay Networks X.25 services now include tunneling over TCP/IP Internet (IPEX). IPEX lets you send and receive messages between two X.25 systems via a TCP/IP network. The tunneling maps TCP sockets to X.25 virtual circuits.

IPEX works with X.25 switched virtual circuits (SVCs) as well as with TCP/IP protocols over all interface types that Bay Networks routers support. For further information about IPEX, refer to *Configuring X.25 Services*.

X.25 Support for RFC 1356

RFC 1356 defines a standard for multiprotocol encapsulation over X.25 networks. Bay Networks implements RFC 1356 for IP, OSI, IPX, DECnet, and XNS. This means you can use Bay Networks routers at one end of a connection, and equipment from another vendor (that also supports RFC 1356 for these protocols) at the other end of the connection. For further information about RFC 1356, refer to *Configuring X.25 Services*.

Data Link Switching (DLSw) Services

Version 11.00 Rev. 4n includes support for RFC 1795. For complete information, refer to *Configuring DLSw Services*.

RFC 1795, called DLSw Version 1, is an implementation of DLSw developed by a consortium of vendors. RFC 1795 supersedes the original DLSw specification, RFC 1434. ARN routers are fully compatible with Bay Networks routers that support the original RFC 1434 specification with Version 10.0 or earlier software.

Based on RFC 1434, RFC 1795 includes features that were not originally published, as well as modifications to the standard. RFC 1795 includes

- Modified frame format for session setup, including a field for the largest frame size.
- Directed broadcast CANUREACH and ICANREACH control frames. This feature reduces broadcasting over the network.
- Capabilities exchange, allowing routers to exchange resource information about each other. Capabilities exchange flows operate in three categories:
 - Fixed information, such as an organization's router software version
 - Customized information, where one router transfers the information to another router
 - Negotiation, where routers negotiate the use of proprietary functions (and only if both routers support the functions under negotiation)
- Rate-based pacing, a new standard for flow control between routers.

Flow control allows a DLSw router to inform another router to slow down or stop sending data when the receiving buffer(s) fill up. Rate-based flow control uses a windowing mechanism that allows the routers to send more or fewer packets, based on the state of the last receive window. If the router successfully receives the last transmission, it informs the sending router to continue to send more packets. Flow control is essential for successful delivery of SNA and NetBIOS data.

IP Services

The following features are new for IP services.

RIP Support for Dial-Optimized Routing

Dial-optimized routing (DOR) reduces costs on dialed lines. Under DOR, RIP exchanges routing information on the interface only when the router or a peer has activated the connection for a data transmission. RIP does not initiate a connection on a dialed line just to issue a routing update, unless it is the first time the dial line is initialized.

For information on configuring a RIP interface for DOR, see *Configuring IP Services*, Chapter 4.

IP Accounting Support for Frame Relay Interfaces

IP Accounting counts transit data packets -- that is, packets that IP receives on one interface and forwards to another interface. This mechanism allows a network service provider to bill a network user according to the amount of data routed between two locations.

Bay Networks currently provides IP accounting support for Frame Relay networks. For information on configuring a Frame Relay interface for IP accounting, see *Configuring IP Services*, Chapter 3.

IP accounting keeps track of transit data packets by making an entry for each packet in an IP accounting table. Each entry includes the source and destination addresses of the packet, the number of packets forwarded, and the number of bytes forwarded.

ISP Mode

ISP mode provides the following features for internet service providers (ISPs).

- Suppression of IP forwarding tables.

By default, IP maintains a forwarding table on each IP interface. IP uses this table as a cache for routes that are frequently used to forward data packets that arrive on the interface. In ISP mode, IP does not use forwarding tables.

- BGP soloist

By default, BGP runs on all slots configured with IP interfaces. In ISP mode, BGP runs as a soloist.

By default, ISP mode features are disabled on the router. For information, see *Configuring IP Services*, Chapter 3.

Dynamic BGP Policy Configuration

By default, BGP configures IP policies dynamically. This means that if you modify a policy, BGP dynamically re-evaluates all affected routes as a result.

For complete information on BGP dynamic policy configuration, see *Configuring IP Services*, Chapter 6.

BGP Communities

The BGP communities attribute identifies the communities to which the route belongs. (A community is a group of destinations that share some common property.)

You can configure a BGP accept or announce policy to match a BGP community. For complete information, see Appendix B of *Configuring IP Services*.

Simplified Regular Expressions for BGP AS Pattern Matching

In the Bay Networks implementation of AS path pattern matching for Version 10.0, the user must know regular expression syntax. For Version 11.00 Rev. 4n, we have provided a simpler syntax. For complete information, see *Configuring IP Services*, Chapter 6. You can also use the **ip bgp_routes** command in the Technician Interface in AS pattern matching. For complete information, see *Using Technician Interface Software*, Chapter 8.

Static Host Entry Support for IGMP

A network may include a member of a multicast group that is unable to register its network with the local IGMP router; for example, a host that is a member of a multicast group but that is not running IGMP.

In such a situation, you can register the group member's network statically on the router. For complete information, refer to *Configuring IP Multicast Services*, Chapter 3.

Interface Redundancy

Interface redundancy now works with AppleTalk and VINES. For information about redundancy, refer to *Configuring Interface and Router Redundancy*.

NTP Support

The Network Time Protocol (NTP) synchronizes the timing of internal clocks of various internet devices across large, diverse networks to universal standard time. NTP runs over UDP, which in turn runs over IP. The NTP protocol specification is documented in RFC 1305.

The current implementation of NTP supports only NTP Client mode. In this mode, the local NTP client, which runs on a router, accepts time information from other remote time servers and adjusts its clock accordingly. However, the NTP local client will not attempt to synchronize another device's clock.

Technician Interface Diags Command

The Technician Interface provides a new command for disabling and enabling diagnostics at powerup. Disabling the diagnostics results in a faster boot time.

By default, the router executes a complete set of diagnostic tests at every powerup. You can use the **diags** command to disable or reenble the powerup diagnostics.

diags [-on / off] [slot no.]

diags -on [slot]	The router executes all powerup diagnostics at subsequent restarts.
diags -off [slot]	The router skips powerup diagnostics at subsequent restarts.
diags	The router restarts immediately and executes complete diagnostics.

New and Enhanced Technician Interface Scripts

Version 11.00 Rev. 4n includes new and enhanced Technician Interface scripts:

- **enable/disable dcm** -- Renamed from enable/disable dcmmw. Adds **base module**, **expansion module**, and **middleware** options for enabling and disabling ARN DCM components individually.
- **show appn switch** <RTP_conn_name> -- Adds a new option that requests the APPN node to perform a path switch with a currently active RTP connection, then displays the results.
- **show ntp** -- Adds a new command group that shows statistics for the Network Time Protocol.
- **show sws** -- Adds options for **on-demand dialing_groups**, **optimized_routing**, and **pap_chap_information**.
- **show x25** -- Adds options for IP over X.25 (**ipex maps** and **ipex session**).
- **show isdn calls time** -- Adds a circuit number column to the display.
- **show dcm** -- Renamed from show dcmmw. Adds **base module**, **expansion module**, and **middleware** options for viewing information on individual ARN DCM components. Improves the display with additional output.
- **show ds1e1 timeslot** -- Improves the display with current, rather than originally configured DS1E1 timeslot assignments.
- **show csmacd**, **show ftp**, **show fr**, **show ip**, **show snmp**, **show sync**, **show tcp**, **show telnet**, **show tftp** -- Updates displays for these embedded scripts.
- **show process** -- Updates sampling interval from 5 to 30 seconds for the **buffers**, **cpu**, and **memory** options.
- **show smds** -- Adds some address verification information to the **stats** and **circuit** options.
- **show state all** and **show circuits** -- Adds IPX SAP (IPX Service Advertising Protocol) information to displays.
- **show sync** -- Adds options for **dsucsu_stats**, **dsucsu_config**, **modem_state**, and **modem_config**.

For complete information on all but the following scripts related to ARN hardware, see *Using Technician Interface Scripts*.

Enable/Disable DCM Scripts

Use the **enable dcm** *<base module | expansion module | middleware>* command to enable

- A DCM board (*probe*) installed on a BayStack AN®, ANH™, or ARN Ethernet base module.
- A DCM board installed on an ARN Ethernet expansion module.
- The DCM software subsystem (DCM middleware, *DCMMW*) on an AN, ANH, or ARN router. The DCMMW driver runs on the base module; it controls the DCM and provides access to collected RMON statistics.

Use the **disable dcm** *<base module | expansion module | middleware>* command to disable the same three components.

Examples

\$ disable dcm base

DCM base record disabled.

\$ enable dcm expansion

DCMMW base record enabled.

\$ enable dcm middleware

DCM Middleware and all probes have been Enabled.

Show DCM Scripts

Use the **show dcm** *<base module | expansion module | middleware>* command to display information about

- A DCM board installed on a BayStack AN, ANH, or ARN base module.
- A DCM board installed on an ARN Ethernet expansion module.
- The DCM software subsystem (DCM middleware, DCMMW) on an AN, ANH, or ARN router. The DCMMW driver runs on the base module; it controls the DCM and provides access to collected RMON statistics.

Example Display - show dcm middleware**\$ show dcm middle**

DCM Middleware Information

Application: DCMMWW

State: Enabled

Number of DCMs: 2

The command **show dcm middleware** displays the following information:

Application	Name of the middleware driver software (DCMMWW)
Operational Status	Current state of the application (enabled or disabled)
Number of DCMs	Number of installed DCM boards in the router

The commands **show dcm base module** and **show dcm expansion module** display the following information:

State	State of the DCM Entry table for each DCM in the DCMMW.mib.
Operational Status	Current state of the DCM (up or down).
Module Type	Type of DCM (Ethernet).
Memory Size	Size, in bytes, of the DCM board's memory.
Hardware Revision	Revision of the DCM hardware.
Firmware Revision	Revision of the DCM firmware.
Agent Image Version	Version of the Agent Image running on the DCM.
BootOption	Indicates whether DCM boots from the boot image in its Flash memory (LOCAL), or downloads an image in the DCM board's shared DRAM (DOWNLOAD).
Image Name	Name of the active DCM image.
Image Save Mode	Indicates whether DCM saves the boot image in shared memory to the DCM board Flash memory (SAVE), or leaves it in RAM to be lost at the next boot (NO_SAVE).
Config Source	Indicates whether DCM uses the configuration information in its Flash memory (LOCAL), or a configuration file in the DCM board's shared DRAM (SHARED).

(continued)

Config Save Mode	Indicates whether DCM saves configuration information currently in RAM to the DCM board Flash memory (WRITE), or leaves it in RAM to be lost at the next boot (NO_WRITE).
Maximum # Hosts per Entry	Maximum number of host address entries in the RMON Host Control table. This limit changes according to the amount of memory available to DCM. If the table reaches the maximum value, DCM deletes entries based on an LRU (least recently used) algorithm.
Configured # Hosts per Entry	Current number of host address entries configured in the RMON Host Control table.
Create Host Control Table	Indicates whether DCM sets up the RMON Default Host table at every boot (ENABLED), or lets an RMON application set up the table (DISABLED). Some RMON network management applications expect the DCM to set up a host configuration. Others enable and disable their own configurations during normal operations. Note that the DCM allows only one host table.
Create Matrix Control Table	Indicates whether DCM sets up the RMON Matrix Control table at every boot (ENABLED), or lets an RMON application set up the table (DISABLED). Some RMON network management applications expect the DCM to set up a matrix configuration. Others enable and disable their own configurations during normal operations. Note that the DCM allows only one matrix table.



Note: With current revisions of DCM software, the RMON Host and Matrix tables are created by default; you cannot delete or disable these tables.

Example Display - show dcm base module

\$ show dcm base

Base Module DCM Information

DCM State: Enabled

Operational Status: Up

Module Type: Ethernet

Memory Size: 2097152

Hardware Revision: BB

Firmware Revision: B

Agent Image Version: V1.4.0

Boot Option: Down Load
Image Name: 1:x10_140.exe
Image Save Mode: Save
Config Source: Local
Config Save Mode: Save

Maximum # Hosts per Entry: 500
Configured # Hosts per Entry: 500
Create Host Control Table: Disabled
Create Matrix Control Table: Disabled

Example Display - show dcm expansion module

\$ show dcm expansion

Expansion Module DCM Information

DCM State: Enabled
Operational Status: Up

Module Type: Ethernet
Memory Size: 16777216
Hardware Revision: C
Firmware Revision: B
Agent Image Version: V1.4.0

Boot Option: Down Load
Image Name: 1:x10_140.exe
Image Save Mode: Save
Config Source: Local
Config Save Mode: Save

Maximum # Hosts per Entry: 500
Configured # Hosts per Entry: 500
Create Host Control Table: Disabled
Create Matrix Control Table: Disabled

Show Sync Scripts

Use the **show sync** *<dsucsu_stats | dsucsu_config>* commands to display information about a DSU/CSU module installed in a BayStack ARN.

Use the **show sync** *<modem_state | modem_config>* commands to display information about a V.34 modem module installed in a BayStack ARN.

The command **show sync dsucsu_stats** displays the following information:

Slot	Base module slot that contains the DSU/CSU module. For the ARN, the value is always 1.
Conn	COM connector that contains the DSU/CSU module (1 or 2).
Op State	Current V.54 loopback operating state of the interface. States are: Normal (no loopback), Local (analog) Loopback, Digital Loopback, Remote Digital Loopback.
Service Status	Current status of the DSU/CSU module as reported by Out of Service or Maintenance Mode codes from the network carrier. Service states are: In Service, Out of Service (OOS), Out of Frame (OOF), Loss of Line (LOL), or Telco Loopback.
Out of Service Errors	Number of OOS control codes (bipolar violations) received from the central office.
Out of Frame Errors	On Clear Channel 64K lines only, indicates the number of times framing has been lost between the DSU/CSU and the central office.
Loss of Line Errors	Number of errors resulting from loss of line signal from the network service.
Total Errors	Combined number of Out of Service, Out of Frame, and Loss of Line errors.

Example Display - show sync dsucsu_stats

\$ show sync dsucsu_stats

Slot	Conn	Op State	Service Status	Out of Service Errors	Out of Frame Errors	Loss of Line Errors	Total Errors
-----	-----	-----	-----	-----	-----	-----	-----
1	2	normal	LOL	0	0	855	855

1 entry(s) found

The command **show sync dsucsu_config** displays the following information:

Hardware Revision	Hardware revision of the DSU/CSU module.
Software Revision	Firmware revision of the DSU/CSU module.
Opmode	Identifies the type of Telco service: 56K DDS1 or CC 64K.

Transmit Clock	Indicates whether this DSU/CSU receives timing from the Telco source (Slave) or provides transmit timing in a private-wire configuration (Master).
Transmit Monitor (64K only)	Indicates whether the 64K Transmit Monitor is enabled. The Transmit Monitor suppresses data to prevent unintended duplication of network control codes.

Example Display - show sync dsucsu_config

\$ show sync dsucsu_config

```
Configuration of DSU/CSU in Slot 1 Connector 2:  
HW Revision 3  
SW Revision 3  
Opmode: 56K DDS1  
Transmit Clock: slave (network)  
Transmit Monitor (64K only): disabled  
  
1 entry(s) found
```

The command **show sync modem_state** displays the following information:

Init Slot	Base module slot that contains the V.34 modem module. For the ARN, the value is always 1.
Conn	COM connector that contains the V.34 modem module (1 or 2).
Init State	Current state of modem initialization. States are <ul style="list-style-type: none">• Startup (1)• SCCInit (2)• GetInfo (3)• SetDefaults (4)• Initialization (5)• PhoneNumber (6)• Loopback (7)• InitComplete (8)
Line State	Current operational state of modem interface. States are <ul style="list-style-type: none">• Unknown (1)• On Hook (2)• Off Hook (3)• Connected (4)• Busied Out (5)• Reset (6)

Example Display - show sync modem_state**\$ show sync modem_state**

Slot	Conn	Init	State	Line	State
----	----	-----	-----	-----	-----
1	1	8			unknown

The command **show sync modem_config** displays the following information:

Configuration	Hardware revision of the V.34 modem module, listed by slot and COM connector number. For the ARN, all modules are Slot 1.
Software Revision	Firmware revision of the modem module.
Factory Defaults	Indicates whether exclusive use of the factory default initialization string is enabled or disabled. When enabled, only the default string is sent to the modem at restart. When disabled, the router sends a user-specified initialization string after the default string.
Initialization String	AT command string currently sent to the modem after the factory default string. Commands in this string take precedence over commands in the factory default string.
Factory Default String	AT command string sent to the modem at every restart: AT&M2&Q2&D0&S1&R0S0=0M1L2T
Country Code	Modem country code.

Example Display - show sync modem_config**\$ show sync modem_config**

```
Configuration of V34 modem in Slot 1 Connector 1:
HW Revision 3
Software Revision V1.440-V34_DS
Factory Defaults: disabled
Initialization String: AT&M1&Q1&D0&S1&R0S0=2
Factory Default String: AT&M2&Q2&D0&S1&R0S0=0M1L2T
Country Code: North America
```

New Log Event Messages

This section describes new Event messages for the Modem and DSU/CSU MIB entities that appear in log files.

For complete information, see *Event Messages for Routers and BNX Platforms*.

Modem Events

This section describes the event messages logged for the ARN V.34 modem. You can display these messages using the following Technician Interface command:

log -fwi -e modem

Entity Code/Event Code **110/1**

Decimal Identifier **16805377**

Severity: Fault

Message: System error, service attempting restart

Meaning: The V.34 modem driver experienced a fatal error and is restarting automatically.

Action: Review event messages logged before this event; the preceding messages should give more specific information about why an error occurred. Call the Bay Networks Technical Response Center if the modem driver fails to restart.

Entity Code/Event Code **110/2**

Decimal Identifier **16805378**

Severity: Warning

Message: Modem initialization failed on <slot no.> COM<connector_no.>

Meaning: The V.34 modem module in the ARN front panel connector indicated (Slot 1; COM1 or COM2) failed software initialization.

Action: Review event messages logged before this event; the preceding messages should give more specific information about why an error occurred. Call the Bay Networks Technical Response Center if the modem fails to initialize on restart.

Entity Code/Event Code **110/4**

Decimal Identifier **16805380**

Severity: Info

Message: Modem initialization completed on Slot<slot no.> COM<connector_no.>

Meaning: The modem completed initialization on the ARN V.34 modem module indicated (Slot 1; COM1 or COM2).

Entity Code/Event Code **110/5**

Decimal Identifier **16805381**

Severity: Info

Message: Modem initialization failed in the <state> state <operational_code> on Slot<slot no.> COM<connector_no.>

Meaning: The V.34 modem module indicated (Slot 1; COM1 or COM2) failed initialization and is currently in one of the following states:

- START_UP (1)
- SCC_INIT (2)
- GET_INFO (3)
- AT_DEFAULT (4)
- AT_INIT (5)
- PHONE_NUMBER (6)
- LOOPBACK (7)

Action: Try restarting the modem line driver. If the failure state is AT_Init (5), reset the modem configuration in the Site Manager V.34 Modem Interface window (refer to “Resetting the V.34 Modem Configuration” in the *Release Notes for Site Manager Software Version 5.00 Revision 4n*. Call the Bay Networks Technical Response Center if the modem fails to initialize on restart.

Entity Code/Event Code **110/6**

Decimal Identifier **16805382**

Severity: Info

Message: <loop_state> loopback initiated in modem on Slot<slot no.>
COM<connector_no.>

Meaning: The router initiated the specified loopback state on the V.34 modem module in the ARN front panel connector indicated (Slot 1; COM1 or COM2). The loopback states are:

- LOCAL ANALOG
- LOCAL DIGITAL
- REMOTE DIGITAL
- REMOTE DIGITAL W/ PATTERN
- LOCAL ANALOG W/ PATTERN

Entity Code/Event Code **110/7**

Decimal Identifier **16805383**

Severity: Info

Message: Could not initiate <loop_state> loopback in modem on Slot<slot no.>
COM<connector_no.>

Meaning: The router could not initiate the specified loopback mode on the ARN V.34 modem module indicated (Slot 1; COM1 or COM2). The loopback states are:

- LOCAL ANALOG
- LOCAL DIGITAL
- REMOTE DIGITAL
- REMOTE DIGITAL W/ PATTERN
- LOCAL ANALOG W/ PATTERN

Entity Code/Event Code **110/8**

Decimal Identifier **16805384**

Severity: Info

Message: Loopback terminated in modem on Slot<*slot no.*> COM<*connector_no.*>

Meaning: The router terminated loopback on the V.34 modem module in the ARN front panel connector indicated (Slot 1; COM1 or COM2).

DSU/CSU Events

This section describes the event messages logged for the ARN DSU/CSU adapter module. You can display these messages using the following Technician Interface command:

log -fwi -e dsucsu

Entity Code/Event Code **111/1**

Decimal Identifier **16805633**

Severity: Fault

Message: System error, service attempting restart

Meaning: The DSU/CSU driver experienced a fatal error and is restarting automatically.

Action: Review event messages logged before this event; the preceding messages should give more specific information about why an error occurred. Call the Bay Networks Technical Response Center if the DSU/CSU driver fails to restart.

Entity Code/Event Code **111/2**

Decimal Identifier **16805634**

Severity: Info

Message: DSU/CSU initialization started on Slot<*slot no.*> COM<*connector_no.*>

Meaning: The router began driver initialization on the DSU/CSU module in the ARN front panel connector indicated (Slot 1; COM1 or COM2).

Entity Code/Event Code **111/3**

Decimal Identifier **16805635**

Severity: Info

Message: DSU/CSU initialization completed on Slot<*slot no.*> COM<*connector_no.*>

Meaning: The router completed driver initialization on the DSU/CSU module in the ARN front panel connector indicated (Slot 1; COM1 or COM2).

Entity Code/Event Code **111/4**

Decimal Identifier **16805636**

Severity: Info

Message: <*loop_state*> initiated for DSU/CSU on Slot<*slot no.*> COM<*connector_no.*>

Meaning: The router initiated the specified loopback state on the DSU/CSU module in the ARN front panel connector indicated (Slot 1; COM1 or COM2). The DSU/CSU loopback states are

- Local Analog Loopback
- Local Digital Loopback
- Remote Digital Loopback
- Remote Digital Loopback W/ Pattern
- Local Analog Loopback W/ Pattern

Entity Code/Event Code **111/5**

Decimal Identifier **16805637**

Severity: Info

Message: Loopback terminated in DSU/CSU on Slot<*slot no.*> COM<*connector_no.*>

Meaning: The router terminated loopback operation on the DSU/CSU module in the ARN front panel connector indicated (Slot 1; COM1 or COM2).

Guidelines for Using Version 11.00 Rev. 4n

The following guidelines are new in Version 11.00 Rev. 4n.

ARN Memory Requirements

The following features require a minimum DRAM configuration of 8 Mbytes:

- DLSw
- ISDN BRI
- Token Ring base or expansion module configurations

Using the Technician Interface ARN Installation Script

You can use the *inst_arn.bat* script from a Technician Interface prompt on the router to configure all except the following ARN interfaces:

- V.34 modem adapter module
- ISDN U adapter module
- ISDN S/T adapter module

Refer to *Installing and Operating BayStack ARN Routers* for information on using the ARN installation script Quick-Start procedure.

Refer to *Release Notes for Site Manager Software Version 5.00 Revision 4n* for information about configuring V.34 modem and ISDN adapter module interfaces.

Cycling Power to the ARN

To ensure a complete power cycle, we recommend that you wait at least 4 seconds between powering off the ARN and powering it back on.



Caution: Cycling power to the ARN too quickly could cause an error.

IP Equal-Cost Multipath Routing

Version 11.00 Rev. 4n does not support IP equal-cost multipath routing for RIP and OSPF.

DCM Software Image and Router Software Compatibility

To run RMON on an ARN router, the DCM software image must be Version 1.4. The Version 1.4 DCM software image is backward-compatible with Router Software Versions 9.0x and 10.0x, and 11.0. However, if you attempt to run RMON on a Version 11.00 Rev. 4n router that has a DCM software image version earlier than Version 1.4, you will get an error message from the RMON Summary application telling you that the router does not support RMON.

Joining an Incompatible Emulated LAN

Bay Networks routers currently support only Ethernet IEEE 802.3 emulated LAN connectivity. When accepting the default, Unspecified, for the LEC LAN Type parameter, ensure that the LAN Emulation Configuration Server (LECS) supplies a configuration for an IEEE 802.3 emulated LAN. (Refer to *Configuring ATM Services* for more information about the LEC LAN Type parameter.)

If the LECS tries to assign a client to a Token Ring 802.5 emulated LAN, the attempt fails and the router software generates the following log message:

```
# 58: 01/11/96 17:05:59.714 WARNING SLOT 5 ATM_LE Code: 34
LEC: Config Resp incompatible LAN type (802.5) returned - FAILED
```

Support for Banyan 80C4 ISAP

Bay Networks routers now support the Banyan 80C4 ISAP on Ethernet.

Using IPX Dial Optimized Routing (DOR)

The following information will help you use DOR optimally.

Inactivity Mode

We recommend that you set the Inactivity Mode parameter to Transmit Only. Any other setting causes the inactivity mode to reset when the receive end can't filter Serialization, Watchdog, and Keep Alive packets for NORESET. These packets could keep the demand line active for long periods of time.

RIP/SAP Pace and Packet Size Parameters

As IPX routes and services grow in number, IPX RIP and SAP packets may be clipped when an IPX DOR circuit comes up or changes state. To stop the clipping, reduce the value of the Pace parameter for RIP and SAP packets or change the RIP/SAP packet size for the IPX DOR circuit. You should reduce the RIP/SAP Pace parameter for IPX DOR circuits to accommodate the number of IPX routes and services in the network.

Diagnostic Packets and Time Synchronization

No default priority queuing filters exist for IPX diagnostics packets or packets used in NDS time synchronization. You can configure a priority queueing filter to keep IPX diagnostic packets from bringing up a demand line. However, since the Bay Networks IPX ping packet is a diagnostic packet, the filter will affect it as well.

NDS time synchronization packets are treated as data packets. You can configure NetWare servers for larger polling intervals to reduce the frequency of bringing up the line for time synchronization packets.

Using Frame Relay Service Records

The following sections compare service records to the access modes that formerly defined Bay Networks Frame Relay services.

Group Access Mode

In group access mode, upper-layer protocols treat each Frame Relay network interface as a single access point to the switched network. The upper-layer protocols use a single network address to send all traffic destined for the switched network to the Frame Relay network interface. When you configure each router, you assign only one network address, for example an IP or IPX address, to the Frame Relay interface, not to each PVC. The DLCMI dynamically configures PVCs; you do not need to explicitly configure them.

Group access mode advantages are that it

- Supports all protocols.
- Simplifies network addressing because you define and associate only one protocol address with the Frame Relay interface.
- Is easy to configure.
- Conserves resources because it requires a small number of circuits.

Its disadvantages are that it

- Allows only one group of PVCs per Frame Relay connection.
- Uses large amount of buffer space during broadcasts.
- Increases customer costs because it has only a single broadcast domain.

Service Records and Group Mode

Service records retain all of the advantages of group mode. Service records also

- Allow multiple groups of PVCs per Frame Relay connection.
- Enable you to gather multiple PVCs for each network protocol into a separate group or service record, thereby reducing the number of buffers needed per circuit during broadcasts.
- Lower customer costs by creating multiple broadcast domains.

Using service records to define Frame Relay removes the need to think in terms of group mode.

Service Records and Direct Access Mode

In direct access mode, upper-layer protocols treat the Frame Relay network as a series of point-to-point connections. The upper-layer protocols view each PVC as an individual network interface.

Direct access mode advantages are that it

- Limits broadcasts to one PVC.
- Enables multiple layer-three networks per interface.

Direct access mode disadvantages are that it

- Creates a new Frame Relay circuit for each PVC, consuming router resources.
- Allows only one PVC per network.

Service Records and Direct Mode

A service record with a single PVC is the same as a direct access mode PVC. Using service records to define Frame Relay removes the need to think in terms of direct mode.

Service Records and Hybrid Access Mode

Hybrid access mode, as its name implies, combines characteristics of group and direct access modes. It works only for non-fully meshed network configurations that use both bridging and routing over a single Frame Relay interface. This mode is also best for spanning tree bridging.

You configure hybrid mode by enabling the hybrid mode service record parameter. See Chapter 3, “Customizing Frame Relay,” for instructions.

Default Service Record

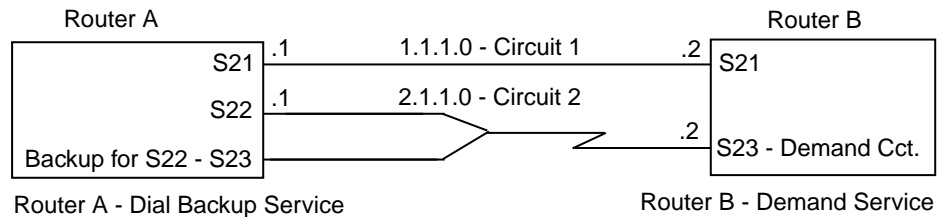
The router creates the first service record automatically. This first service record is called the *default service record*. Any PVCs that are not associated with a configured service record use the default service record.

Using Demand Circuits for Backup

You can now configure a demand circuit to act as a back up for a failed point-to-point circuit. If the point-to-point circuit fails, the router immediately establishes a demand circuit back to the original router and data transmission can continue. The demand circuit can operate independently of the point-to-point circuit, so the demand circuit can remain active after the point-to-point recovers.

This type of configuration is recommended only if you want to keep the demand circuit active after the point-to-point circuit recovers.

The following diagram shows how this configuration works.



In the diagram, Router A is connected to Router B via a point-to-point link. This link, connected at port S21, can support any WAN protocol that the router supports. Router B has a demand circuit configured at S23. It also has the backup circuit parameter set to the circuit number of the point-to-point link S21. If the point-to-point link fails, Router B activates the demand circuit.

Making the Configuration Work by Configuring an Unused Port

Typically dial backup service provides backup for a failed primary connection. In this case, you cannot use dial backup service because the circuit will not stay active once the point-to-point connection recovers. Instead, you configure another port on the same router as the point-to-point circuit for dial backup service. You make this port an unused primary interface set for slave mode, so it does not initiate calls.

The backup does not activate until the remote router makes a demand connection. When a call comes in to this disabled port, the backup circuit comes up on the backup interface.

You configure this unused port on the same subnet as the demand circuit of the remote router. The demand circuit then connects to the router independent of the initial point-to-point circuit.

In the diagram, Router A's disabled port is S22. Port S22 has address 2.1.1.1, which is the same subnet as the demand interface on Router B. For Router A, you configure S22 as the disabled primary circuit and S23 as its backup circuit. Also, Router A's is set to slave mode, so it waits for the incoming call from Router B.

When the point-to-point circuit fails at S21, Router B establishes a demand circuit to Router A. Router A receives the call and brings up the backup circuit on S23.

Once the demand connection is established, it remains active until you manually terminate the connection using the Technician Interface command **force takedown**. Even when the point-to-point circuit recovers, if its routing protocol rule precedence is lower than the demand circuit's precedence, data continues to flow over the demand connection until you terminate it. By manually terminating the connection, you control when the router returns to the point-to-point circuit for transmission.

To configure this application, do the following:

1. **Using Site Manager, create a point-to-point circuit on one router.**
2. **Using Site Manager, configure dial backup service for one router, for example, a central site router, then disable the primary interface.**
3. **Using Site Manager, create a demand pool and circuit on a remote router.**
This demand circuit will act as the backup circuit. Do not configure a backup circuit from Site Manager.
4. **Using the Technician Interface, set the wfSwserv0ptsBackupCct attribute of the router with the demand circuit configured to the point-to-point circuit number (for example, S21 in the diagram).**
5. **Set the Rule Precedence parameter of each circuit's routing protocol to designate which circuit the router will consider preferable.**

Protocols Supported

Version 11.00 Rev. 4n of Bay Networks Router Software supports the following bridging/routing protocols and router configuration features:

- AppleTalk and AppleTalk Update-based Routing Protocol (AURP)
- Advanced Peer-to-Peer Networking (APPN)
- Asynchronous Transfer Mode (ATM)
- ATM Data Exchange Interface (ATMDXI)
- ATM LAN Emulation
- Binary Synchronous Communication Type 3 (BSC3)
- Bootstrap Protocol (BOOTP)
- Border Gateway Protocol (BGP-3 and BGP-4)
- Classless Inter-Domain Routing (CIDR)
- Data Compression
- Data Link Switching (DLSw)
- DECnet Phase IV Routing Protocol
- Dial Backup, Dial-on-Demand, and Bandwidth-on-Demand
- Distance Vector Multicast Routing Protocol (DVMRP)
- Dynamic Host Configuration Protocol (DHCP)
- Exterior Gateway Protocol-2 (EGP-2)
- Frame Relay
- File Transfer Protocol (FTP)
- HP Probe Protocol
- Inbound and Outbound Traffic Filter Features
- Integrated Services Digital Network (ISDN)
- Interface Redundancy
- Internet Gateway Management Protocol (IGMP)
- Internet Protocol (IP)
- Internet Packet Exchange (IPX) Protocol

- Internet Service Provider Mode
- Internet Stream Protocol (ST2)
- Learning Bridge and Spanning Tree Protocols
- Logical Link Control 2 (LLC2) Protocol
- Native Mode LAN (NML) Protocol
- Network Time Protocol (NTP)
- Open Shortest Path First (OSPF) Protocol
- Open Systems Interconnection (OSI) Routing Protocol
- Point-to-Point Protocol (PPP)
- Protocol Prioritization
- Router Discovery
- Router Redundancy
- Synchronous Data Link Control (SDLC)
- Simple Network Management Protocol (SNMP)
- Source Routing Bridge Protocol
- Switched Multi-Megabit Data Service (SMDS)
- Telnet Protocol (Inbound and Outbound)
- Transmission Control Protocol (TCP)
- Transparent-to-Source Routing Translation Bridge
- Virtual Networking System (VINES)
- X.25 Protocol
- XMODEM and YMODEM Protocols
- Xerox Network Systems (XNS) Protocol

Standards Supported

[Table 1](#) lists the Request for Comments (RFCs) and other standards documents with which Version 11.00 Rev. 4n complies. Version 11.00 Rev. 4n may support additional standards that are not listed in this table.

Table 1. Standards Supported by Version 11.00 Rev. 4n

Standard	Description
ANSI X3t9.5	Fiber Distributed Data Interface (FDDI)
IEEE 802.1	Logical Link Control (LLC)
IEEE 802.3	Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
IEEE 802.5	Token Ring Access Method and Physical Layer Specifications
IEEE 802.10	Bridge with Spanning Tree
ITU Q.921	ISDN Layer 2 Specification
ITU Q.921	ISDN Layer 3 Specification
ITU X.25	Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuits
RFC 768	User Datagram Protocol (UDP)
RFC 791	Internet Protocol (IP)
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	Transmission Control Protocol (TCP)
RFC 813	Window and Acknowledgment Strategy in TCP
RFC 826	Ethernet Address Resolution Protocol
RFC 827	Exterior Gateway Protocol (EGP)
RFC 854	Telnet Protocol Specification
RFC 855	Telnet Option Specification
RFC 856	Telnet Binary Transmission

(continued)

Table 1. Standards Supported by Version 11.00 Rev. 4n *(continued)*

Standard	Description
RFC 857	Telnet Echo Option
RFC 858	Telnet Suppress Go Ahead Option
RFC 859	Telnet Status Option
RFC 860	Telnet Timing Mark Option
RFC 861	Telnet Extended Options: List Option
RFC 863	Discard Protocol
RFC 877	Transmission of IP Datagrams over Public Data Networks
RFC 879	TCP Maximum Segment Size and Related Topics
RFC 888	"STUB" Exterior Gateway Protocol
RFC 894	Transmission of IP Datagrams over Ethernet Networks
RFC 896	Congestion Control in IP/TCP Internetworks
RFC 903	Reverse Address Resolution Protocol
RFC 904	Exterior Gateway Protocol Formal Specification
RFC 919	Broadcasting Internet Datagrams
RFC 922	Broadcasting Internet Datagrams in Subnets
RFC 925	Multi-LAN Address Resolution
RFC 950	Internet Standard Subnetting Procedure
RFC 951	Bootstrap Protocol
RFC 959	File Transfer Protocol
RFC 994	Protocol for Providing the Connectionless-mode Network Service
RFC 1009	Requirements for Internet Gateways
RFC 1027	Using ARP to Implement Transparent Subnet Gateways
RFC 1042	Transmission of IP over IEEE/802 Networks
RFC 1058	Routing Information Protocol

(continued)

Table 1. Standards Supported by Version 11.00 Rev. 4n *(continued)*

Standard	Description
RFC 1075	Distance Vector Multicast Routing Protocol (DVMRP)
RFC 1076	Redefinition of Managed Objects for IEEE 802.3 Repeater Devices (AN Hubs only)
RFC 1079	Telnet Terminal Speed Option
RFC 1084	BOOTP Vendor Information Extensions
RFC 1091	Telnet Terminal-Type Option
RFC 1108	Security Options for the Internet Protocol
RFC 1112	Host Extensions for IP Multicasting Appendix I. Internet Group Management Protocol
RFC 1116	Telnet Line-mode Option
RFC 1139	Echo Function for ISO 8473
RFC 1155	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1157	Simple Network Management Protocol (SNMP)
RFC 1163	BGP-2 obsoleted by RFC 1267
RFC 1164	Application of BGP in the Internet
RFC 1166	Internet Numbers
RFC 1188	Proposed Standard for the Transmission of IP over FDDI
RFC 1191	Path MTU Discovery
RFC 1209	Transmission of IP Datagrams over SMDS
RFC 1212	Concise MIB Definitions
RFC 1213	MIB for Network Management of TCP/IP-based Internets
RFC 1267	Border Gateway Protocol 3 (BGP-3)
RFC 1293	Inverse ARP for Frame Relay
RFC 1294	Obsoleted by RFC 1490
RFC 1304	Definition of Managed Objects for the SIP Interface Type

(continued)

Table 1. Standards Supported by Version 11.00 Rev. 4n *(continued)*

Standard	Description
RFC 1305	Network Time Protocol
RFC 1315	Management Information Base for Frame Relay DTEs
RFC 1323	TCP Extensions for High Performance
RFC 1331	Obsoleted by RFC 1661
RFC 1332	PPP Internet Protocol Control Protocol (IPCP)
RFC 1333	PPP Link Quality Monitoring
RFC 1334	PPP Authentication Protocols
RFC 1340	Assigned Numbers (obsoleted by RFC 1700)
RFC 1350	The TFTP Protocol (Revision 2)
RFC 1356	Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode
RFC 1376	PPP DECnet Phase IV Control Protocol (DNCP)
RFC 1378	PPP AppleTalk Control Protocol (ATCP)
RFC 1390	Transmission of IP and ARP over FDDI Networks
RFC 1377	OSI over PPP
RFC 1403	BGP OSPF Interaction
RFC 1434	Data Link Switching: Switch-to-Switch Protocol
RFC 1483	Multiprotocol Encapsulation over ATM AAL5
RFC 1490	Multiprotocol Interconnect over Frame Relay
RFC 1552	The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
RFC 1577	Classical IP and ARP over ATM
RFC 1583	OSPF Version 2
RFC 1634	Novell IPX over Various WAN Media (IPXWAN)
RFC 1638	PPP Bridging Control Protocol (BCP)
RFC 1654	Border Gateway Protocol 4 (BGP-4)

(continued)

Table 1. Standards Supported by Version 11.00 Rev. 4n *(continued)*

Standard	Description
RFC 1661	Point-to-Point Protocol (PPP)
RFC 1662	PPP in HDLC-like Framing
RFC 1717	PPP Multilink Protocol (MP), obsoleted by RFC 1990
RFC 1755	Signaling Support for IP over ATM
RFC 1757	Remote Network Monitoring Management Information Base (RMON) (for AN, ANH, and ARN equipped with Data Collection Module only)
RFC 1762	PPP Banyan VINES Control Protocol (BVCP)
RFC 1763	PPP DECnet Phase IV Control Protocol (DNCP)
RFC 1764	PPP XNS IDP Control Protocol (XNSCP)
RFC 1795	Data Link Switching: Switch-to-Switch Protocol, Version 1
RFC 1819	Internet Stream Protocol, Version 2
RFC 1989	PPP Link Quality Monitoring, obsoletes RFC 1333
RFC 1990	PPP Multilink Protocol (MP), obsoletes RFC 1717
VINES 4.11	The Bay Networks router software works with the Banyan VINES 4.11 standard. Bay Networks Router Software Version 8.10 and later also support VINES 5.50 sequenced routing.

Supported Flash Memory Cards

[Table 2](#) lists the 2-MB, 4-MB, and 8-MB Personal Computer Memory Card International Association (PCMCIA) standard Flash memory cards that are qualified for use in Bay Networks routers.

Table 2. Approved Flash Memory Cards

Size	Vendor	Part Number
2 MB	AMD	AMC002AFLKA
	Amp	1-797078-3
	Fujitsu	MB98A811220
	Intel	1MC002FLKA
	Maxell	EF21B(AA) WEL.M-20
	Mitsubishi	MF82ML-G1FAT01
	Panasonic	BN-02MHFR
	Texas Instruments	CMS68F2MB-250
4 MB	AMD	AMC004CFLKA-150
	Centennial	FL04M-20-1119
	Centennial	FL04M-20-11138
	IBM	IBM1700400D1DA-25
	Intel	IMC004FLSAQ1381
8 MB	AMD	AMC008CFLKA
	Centennial	FLO8M-25-11119-01
	Intel	IMC008FLSP/Q1422
16 MB	Centennial	FL16M-20-1119-03
	Epson	HWB161BNX2