

Documentation Changes Notice for Router Version 11.01 and Site Manager Version 5.01

Router Software Version 11.01
Site Manager Software Version 5.01

BNX Software Version <x.x>

Part No. Test Part Number
January 1996



Copyright © 1988–1997 Bay Networks, Inc.

All rights reserved. Printed in the USA. January 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, Bay Networks, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and ANH, ASN, Bay•SIS, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, PathMan, PhonePlus, Quick2Config, RouterMan, SPEX, 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).

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	x
Bay Networks Information Services	xi
World Wide Web	xi
Customer Service FTP	xi
Support Source CD	xii
CompuServe	xii
InfoFACTS	xiii
How to Get Help	xiii

Documentation Changes Notice

Configuring ATM Services	4
Creating an ATM Token Ring Emulated LAN	4
Assigning an Emulated LAN Type	4
Protocol Support	5
Things to Remember	6
Configuring Bridging Services	7
Max Number Query Cache Entries Parameter	7
Priority Parameter	7
Bridge Table Size Parameter	8
Configuring Dial Services	8
Correct MIB OID Numbers	8
Demand Circuit Configuration	8
Range for BOD Recovery Threshold	10
Callback	10
Configuring Callback	11
Callback Configuration Parameters	12
Using the Incoming Phone List to Identify the Client	16
Standby Circuits	17

Comparing Standby Circuits with Dial Backup Circuits	18
How Standby Circuits Work	19
Configuring Each Side of the Standby Connection	20
Balancing Traffic Between a Primary and a Hot Standby Circuit	21
Using Time of Day Schedules to Manage Standby Circuits	22
Configuring Multiple Time of Day Schedules	22
Standby Configuration Parameters	25
Configuring DLSw Services	28
RFC 1434 and RFC 1795 Support	28
RFC Parameter	29
Initial Pacing Window	29
Multislot Broadcasts	30
Session Alive Filter	31
Qualified Link Level Control Support	31
Configuring IP Services	32
Opening the IP Accounting Window	32
Controlling Notification of a Full IP Accounting Table	32
Configuring an OSPF Neighbor on a Standard Point-to-Multipoint Interface	33
Configuring IP Utilities	33
Configuring IPX Services	33
Configuring IPX Interface Cost Parameter	34
Configuring Max Path and Max Path Splits for IPX	34
Configuring Line Services	34
Setting the Asynchronous Baud Rate	35
Setting the Synchronous IFTF Pattern	35
Setting the HSSI Carrier Loss Timeout	36
Setting the Synchronous Hold Down Time	36
Ethernet - CSMA/CD Line Service Enhancement	36
Ethernet BofL Messages	36
BayStack Router Interfaces	38
Configuring a DSU/CSU Interface	39
Using DSU/CSU Loopback Tests	42
Configuring a V.34 Modem Interface	47
Customizing the V.34 Modem Initialization String	53
Resetting the V.34 Modem Configuration	59

Configuring Routers	60
Configuring the BayStack ARN	60
Selecting the Base ARN Configuration	61
Configuring ARN Interfaces	67
Customizing the ARN Service Console	68
Configuring Traffic Filters and Protocol Prioritization	70
Number of Traffic Filter Rules	70
New Criteria	71
Event Messages for Routers and BNX Platforms	72
DLS Warning Events	73
DLS Trace Events	73
DSUCSU Fault Event	75
DSUCSU Info Events	75
FNTS_ATM Fault Event	77
FNTS_ATM Warning Events	77
FNTS_ATM Info Events	79
FR Event	81
KEYMGR Fault Event	81
KEYMGR Warning Events	82
KEYMGR Info Events	82
MODEM Fault Events	83
MODEM Warning Events	83
MODEM Info Events	84
PPP Info Events	85
PPP Trace Events	86
QLLC Fault Event	86
SWSERV Info Events	87
Technician Interface Info Event Messages	88
TTY Info Event Message	89
WEP Fault Event	89
WEP Warning Events	89
WEP Info Events	91
Quick-Starting Routers and BNX Platforms	93

Upgrading Routers from Version 7-10.xx to Version 11.0	93
Technician Interface dcmload Script	93
BOOT and Diagnostic PROM Upgrades for 11.01	95
Using the Bay Command Console	96
Errata	96
Using the BCC to Install a BN Router	101
Using Technician Interface Scripts	110
enable/disable dcm	111
show dcm	113
show ipx	118
show isdn	119
show sws	120
show sync	121
show wep	126
show x25	131
Using Technician Interface Software	134
ARN Diagnostics On/Off Option	134
AN and ANH Powerup Diagnostic Option	134
Secure Shell Commands	135

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 Service 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 -- with response times ranging to 4 hours, depending on local country conditions.

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) 916-8880 (direct)	(508) 670-8766
Europe	(33) 92-4-968-300	(33) 92-4-968-301
Asia/Pacific	(612) 9927-8800	(612) 9927-8811
Latin America	(561) 988-7661	(561) 988-7750

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 for the entire Bay Networks product suite. 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 redesigned 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 online 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 1-408-495-1002. 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) 92-4-968-968	(33) 92-4-966-998
Sydney, Australia	(612) 9927-8800	(612) 9927-8811
Tokyo, Japan	(81) 3-5402-0180	(81) 3-5402-0173

Documentation Changes Notice

[Table 1](#) lists the manuals included in the 11.01/5.01 release, and identifies new manuals, manuals updated since release 11.00/5.00, and those manuals affected by sections in this documentation change notice.

Table 1. 11.01 Documentation

Document Title	New Book for 11.01/5.01	Updated Book for 11.01/5.01	Affected by Section in DCN
<i>Cable Guide</i>			
<i>Configuring AppleTalk Services</i>			
<i>Configuring APPN Services</i>			
<i>Configuring ATM Services</i>			✓
<i>Configuring ATM DXI Services</i>			
<i>Configuring Bridging Services</i>			✓
<i>Configuring BSC Transport Services</i>			
<i>Configuring Data Compression Services</i>			
<i>Configuring Dial Services</i>			✓
<i>Configuring DECnet Services</i>			
<i>Configuring DLSw Services</i>			✓
<i>Configuring Frame Relay Services</i>			
<i>Configuring Interface and Router Redundancy</i>			
<i>Configuring IP Multicasting Services</i>			

(continued)

Table 1. 11.01 Documentation *(continued)*

Document Title	New Book for 11.01/5.01	Updated Book for 11.01/5.01	Affected by Section in DCN
<i>Configuring IP Services</i>			✓
<i>Configuring IP Utilities</i>			✓
<i>Configuring IPX Services</i>			✓
<i>Configuring LineServices</i>			✓
<i>Configuring LLC Services</i>			
<i>Configuring LNM Services</i>			
<i>Configuring OSI Services</i>			
<i>Configuring PPP Services</i>			
<i>Configuring Routers</i>			✓
<i>Configuring SDLC Services</i>			
<i>Configuring SMDS</i>			
<i>Configuring SNMP, RMON, BOOTP, DHCP, and RARP Services</i>		✓	
<i>Configuring Software Encryption</i>	✓		
<i>Configuring Traffic Filters and Protocol Prioritization</i>			✓
<i>Configuring VINES Services</i>			
<i>Configuring X.25 Services</i>		✓	
<i>Connecting ASN Routers and BNX Platforms to a Network</i>			
<i>Connecting BayStack AN and ANH Systems to a Network</i>			
<i>Event Messages for Routers and BNX Platforms</i>			✓
<i>Managing Routers and BNX Platforms</i>			
<i>Modifying Software Images for Routers</i>			
<i>Quick-Starting Routers and BNX Platforms</i>			✓
<i>Troubleshooting Routers</i>			

(continued)

Table 1. 11.01 Documentation *(continued)*

Document Title	New Book for 11.01/5.01	Updated Book for 11.01/5.01	Affected by Section in DCN
<i>Upgrading Routers from Version 7-10.xx to Version 11.0</i>			✓
<i>Using the Bay Command Console</i>	✓		✓
<i>Using Site Manager Software</i>			
<i>Using Technician Interface Scripts</i>			✓
<i>Using Technician Interface Software</i>			
<i>Writing Technician Interface Scripts</i>			

The following sections describe the amendments to the manuals:

- [Configuring ATM Services](#)
- [Configuring Bridging Services](#)
- [Configuring Dial Services](#)
- [Configuring DLSw Services](#)
- [Configuring IP Services](#)
- [Configuring IPX Services](#)
- [Configuring Line Services](#)
- [Configuring Routers](#)
- [Configuring Traffic Filters and Protocol Prioritization](#)
- [Event Messages for Routers and BNX Platforms](#)
- [Quick-Starting Routers and BNX Platforms](#)
- [Upgrading Routers from Version 7-10.xx to Version 11.0](#)
- [Using the Bay Command Console](#)
- [Using Technician Interface Scripts](#)
- [Using Technician Interface Software](#)

Configuring ATM Services

The following sections, which describe ATM token ring LAN emulation support, are new in *Configuring ATM Services*:

- [Creating an ATM Token Ring Emulated LAN](#)
- [Assigning an Emulated LAN Type](#)
- [Protocol Support](#)

Creating an ATM Token Ring Emulated LAN

Creating a token ring emulated LAN requires

- Adding a LANE service record (refer to *Configuring ATM Services* for details)
- Assigning an emulated LAN type as either Unspecified or IEEE8025 (refer to the next section)

Assigning an Emulated LAN Type

You can assign a LAN emulation client to join

- Any ELAN to which the LAN emulation configuration server (LECS) assigns it. That is, you assign an Unspecified LAN type (the default selection).
- Only Ethernet (IEEE 802.3) ELANs.
- Only token ring (IEEE 802.5) ELANs.

When you assign an unspecified LAN type, the client obtains the LAN type from the LECS when it joins an emulated LAN. When you assign IEEE8023 or IEEE8025, the client joins only Ethernet or token ring ELANs (respectively).



Note: If you specify that the LE client run in Manual configuration mode you must specify a LEC LAN type.

Parameter: Emulated LAN Type

Path: Configuration Manager > Protocols > ATM > Service Records > **LEC**

Default: Unspecified

Options: Unspecified | IEEE8023 | IEEE8025

Function: Indicates the data frame format this client uses when it joins an emulated LAN. Clients that use Automatic configuration mode use this parameter in their LE_CONFIGURE_REQUEST frames to specify the LAN type. Clients that use Manual configuration mode use this parameter in their LE_JOIN_REQUEST frames to specify the LAN type.

Selecting manual configuration mode (refer to the parameter description above) requires that you set the Emulated LAN Type to either IEEE8023 or IEEE8025.

Instructions: Accept the default, Unspecified, if you want the client to obtain the LAN type from the LAN emulation configuration server (LECS) when it joins an emulated LAN. Select IEEE8023 if you want the client to join only Ethernet emulated LANs. Select IEEE8025 if you want the client to join only token ring emulated LANs.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.5.20.1.1.6

Protocol Support

[Table 2](#) lists all supported protocols for standard PVCs and SVCs using LLC/SNAP, NLPID, NULL, LANE 802.3, or LANE 802.5 data encapsulation.



Caution: Ethernet and token ring emulated LANs can support different protocols. When adding a protocol to a LANE service record with an Unspecified emulated LAN type, ensure that the protocols you add are supported by the emulated LAN (Ethernet or token ring) that you want to join.

Table 2. Supported Protocols

PVC Using LLC/SNAP, NLPID, or NULL	SVC Using LLC/SNAP or NULL (RFC 1577)	SVC Using LANE 802.3	SVC Using LANE 802.5
Bridge	IP	Bridge	Bridge
Spanning Tree	- RIP	Spanning Tree	Spanning Tree
Native Mode LAN	- BGP	Native Mode LAN	IP
IP	- OSPF	IP	RIP
RIP		RIP	OSPF
EGP		BGP	BOOTP
BGP		OSPF	IPX
OSPF		BOOTP	RIP/SAP
BOOTP		Router Discovery	Source Routing
IGMP		IGMP	SR Spanning Tree
DVMRP		DVMRP	Translate/LB
NetBIOS		NetBIOS	LLC2
DECnet IV		DECnet IV	DLSw
VINES		VINES	APPN
IPX		IPX	
RIP/SAP		RIP/SAP	
XNS		XNS	
RIP (XNS)		RIP (XNS)	
AppleTalk		AppleTalk	
		LLC2	
		DLSw	

Things to Remember

When enabling protocols on a LANE service record, keep the following in mind:

- Each ATM service record globally controls
 - All protocols for any standard PVCs and SVCs that it contains
 - All nonbridging protocols for any hybrid PVCs that it contains

- Selecting LANE to run on an SVC service record defines that service record as belonging to an emulated LAN. This means that any protocols on that service record operate as if they were running over a traditional Ethernet or token ring LAN.
- By leaving the Emulated LAN Type as Unspecified (the default), you allow the LAN emulation configuration server (LECS) to determine what emulated LAN the LE client joins.
- By specifying IEEE8023 or IEEE8025 as the Emulated LAN Type, the LEC joins only an Ethernet or token ring emulated LAN (respectively).
- After you add protocols to a LANE switched virtual circuit, Site Manager adds a LEC (LAN emulation client) button to the ATM Service Records List window. Clicking on the LEC button opens the ARE LAN Emulation Parameters window. For additional information about customizing LAN emulation clients, refer to *Configuring ATM Services*.

Configuring Bridging Services

The following sections are amendments to *Configuring Bridging Services*:

- [Max Number Query Cache Entries Parameter](#)
- [Priority Parameter](#)
- [Bridge Table Size Parameter](#)

Max Number Query Cache Entries Parameter

The range for the Max Number Query Cache Entries parameter (which appears in the Edit Source Routing Global Parameters window) on page 3-19 lists the range as 1 to 100 query entries. The new range is 1 to 2147483647 query entries.

If you reset this value, proceed cautiously and be sure to specify a number that is in direct proportion to the number of Netbios stations. Note that increasing this cache will require more memory on the router.

Priority Parameter

The description of the Priority parameter (which appears in the Spanning Tree Interfaces window) on page 1-31 incorrectly lists the range of values as 0 to 255. The correct range is 1 to 255.

Bridge Table Size Parameter

The function description of the Bridge Table Size parameter (which appears in the Edit Bridge Global Parameters window) on page 1-21 incorrectly states that if you enter an invalid value, the system rounds up or down from the invalid value to the nearest valid value. You should click on the Values button and select one of the values listed. If you type a value other than one of those listed, the system returns an error message.

Configuring Dial Services

The following sections are amendments in *Configuring Dial Services*:

- [Correct MIB OID Numbers](#)
- [Demand Circuit Configuration](#)
- [Range for BOD Recovery Threshold](#)

The following sections about dial services are new in *Configuring Dial Services*:

- [Callback](#)
- [Standby Circuits](#)

Correct MIB OID Numbers

The MIB OIDs for the following dial services parameters are incorrect in the 11.00 version of *Configuring Dial Services*. [Table 3](#) lists the corrected OIDs.

Table 3. ISDN Numbering Type and Plan MIB OIDs

Parameter	MIB OID
ISDN Numbering Type	1.3.6.1.4.1.18.3.5.9.8.12.1.9
ISDN Numbering Plan	1.3.6.1.4.1.18.3.5.9.8.12.1.10

Demand Circuit Configuration

Configuring Dial Services omits a step for the demand circuit configuration.

When the demand pool is configured, configure the demand circuits. Select Dialup > Demand Circuits from the main menu bar. Site Manager displays the Demand Pools window. Click on Circuits; Site Manager displays the Demand Circuits window.

The Demand Circuits window has a Protocols button in the top left corner. Select Protocols > Add/Delete to configure protocols for the demand circuit. In this example, IP is the only protocol configured. Tables 4, 5, and 6 list the parameter values you need to enter for the sample configuration in Appendix A of *Configuring Dial Services*.

Path: Protocols > Select Protocols window

Table 4. IP Parameters

Parameter Name	Router 4 (S25)	Router 7 (S23)
IP Address	150.1.1.2	150.1.1.1
Subnet Mask	255.255.255.0	255.255.255.0

Path: IP > IP Adjacent Host window

Table 5. IP Adjacent Host Parameters

Parameter Name	Router 4 (S25)	Router 7 (S23)
IP Adjacent Host	150.1.1.1	150.1.1.2

Path: IP Adjacent Host window > Demand Circuit window

Table 6. Demand Circuit Parameters

Parameter Name	Router 4 (S25)	Router 7 (S23)
CHAP Local Name	BLN®-1 (case-sensitive)	BLN-2 (case-sensitive)
CHAP Secret	East (case-sensitive)	East (case-sensitive)
Connection Mode	Default (Collision Master)	Collision Slave

Range for BOD Recovery Threshold

The range for the bandwidth-on-demand parameter BOD Recovery Threshold is 10 to 400 percent. This parameter is located in the Bandwidth On Demand Monitor Options window.

The manual incorrectly states that the maximum for the range is 100 percent.

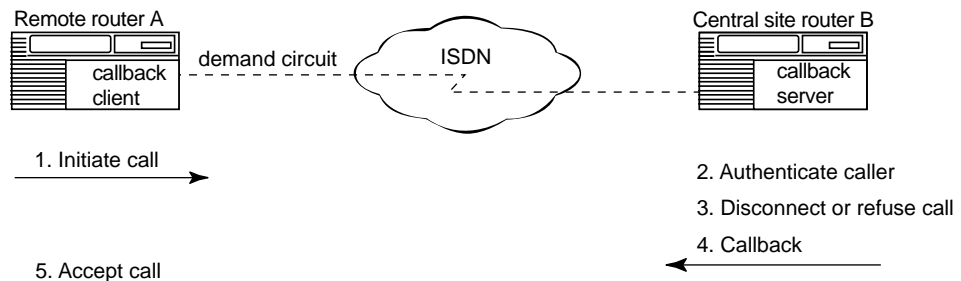
Callback

Callback is a dial-on-demand feature for use between two peer routers, such as a central site router and a remote router. With this feature, you can configure a router to call back an incoming caller. You can configure callback across any demand circuit, including those configured for bandwidth-on-demand service.

Callback offers the following advantages:

- Reduces tariffs because you can place calls using the lowest cost path
- Secures access for only authorized callers
- Consolidates accounting of phone charges

[Figure 1](#) shows how callback works.



DS0032A

Figure-1. Example of Callback Over a Demand Circuit

Remote Router A places a call to Central Router B. Central Router B determines whether the caller is authorized and, for authorized callers, terminates the initial call. Central Router B then places a return call to Remote Router A.



Note: You cannot use the callback feature with demand circuit groups.

Configuring Callback

Callback operates on a per demand circuit basis. You configure callback via the Callback Mode parameter. If you do not want to use the callback feature, you accept the default callback mode of Inactive.

Each end of a callback circuit is assigned the role of *server* or *client*. The server responds to any incoming call from the client and either authenticates the call using the protocols CHAP or PAP, or identifies the caller using the incoming filter feature. The server disconnects or refuses the call, and then dials the client back, using one of the following options:

- The outgoing phone list

The outgoing phone list is a user-defined list containing phone numbers of remote routers. Numbers in the outgoing phone list are associated with a specific circuit.

- Caller ID, also called Automatic Numbering Identification (ANI)

Caller ID is an ISDN service that you must purchase from your ISDN service provider. When you purchase this service, the phone number of the caller is placed in the call's setup message. Your network switch must also support caller ID.

After placing the initial call, the client waits for a return call from the server. A user-specified parameter determines how long the client waits for a response. During this time, the client will not place an outgoing call to any other destination.



Note: The server's callback configuration takes precedence over its Connection Mode parameter setting to ensure that the server can always call the client. The Connection Mode parameter determines whether or not a router can place a call. If the Connection Mode is set to No Dial, which instructs the router not to place calls, the server can still call the client.

Callback Configuration Parameters

The callback configuration parameters can be found in the Demand Circuits window. The Site Manager path to this window is Dialup > Demand Circuits. Remember that your demand pools must already be configured before you can configure demand circuits. For details, refer to *Configuring Dial Services*.

Parameter: **Callback Mode**

Default: Inactive

Options: Inactive | Server | Client | Server Call ID | Client One Charge |
Server One Charge | Server One Charge Call ID

Be aware of the following guidelines:

- If the router is set to Server, Client, or Server Call ID, the router performs CHAP or PAP authentication when it receives a call.
- The one-charge modes ensure that only the server-side of the callback connection incurs phone charges. When you choose any of these options, the server refuses the call from the client, eliminating charges for the client's initial call, but charging the server for its return calls to the client.
- To use any of the one-charge modes, each remote site must have a unique phone number. The server must be able to identify a single circuit for each phone number that it calls back.
- If you want to reduce your configuration work and you can purchase Caller ID service, select the modes that use Call ID. These modes do not require an outgoing phone list to place a call; they rely only on the phone number in the call setup message.
- If you cannot use Caller ID, or the phone number in the call setup message is not sufficient to place an outgoing call (for example, you have to dial "9" to get an outside line), do not select a Call ID mode.

Function: Determines the role of the router in relation to its peer, and how the router identifies the phone number to call back.

Instructions: Select one of the options listed in [Table 7](#).

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.5.1.53

Table 7. Callback Mode Options

Option	Meaning
Inactive	Disables the callback feature for this circuit.
Server	<p>Designates the router as the callback server.</p> <p>The server receives a call from the client. The server authenticates the caller, disconnects the call, and returns the call using a phone number in the outgoing phone list.</p>
Client	<p>Designates the router as the callback client. Use this mode when the other end of the connection uses Server or Server Call ID.</p> <p>The client initiates a call to the server, and then waits for the server to return the call. Once it receives the return call, the client authenticates the call before accepting it.</p>
Server Call ID (ISDN connections only)	<p>Designates the router as the callback server using caller ID.</p> <p>The server receives a call from the client, authenticates the call, and disconnects it. The server then returns the call using the phone number in the original call's setup message.</p>
Client One Charge (ISDN connections only)	<p>Designates the router as the callback client. Also indicates that there will be no charge for its initial call to the server. Use this mode when the other end of the connection uses Server One Charge or Server Once Charge Call ID.</p> <p>The client places a call to the server, expecting the call to fail. The server refuses the call, which eliminates any phone charge for the client. The client then waits for a return call from the server. This option saves the client the cost of the initial call.</p>
<i>(continued)</i>	

Table 7. Callback Mode Options *(continued)*

Option	Meaning
Server One Charge (ISDN connections only)	<p>Designates the router as the callback server. Also indicates that only the server will be charged for the return call to the client.</p> <p>The server receives a call from the client. The server, using incoming filtering, verifies that the client is an authorized caller by matching the client's phone number with a phone number and circuit number in the incoming phone list. If the server finds a matching entry, the server refuses the call. By refusing the call, the server eliminates any phone charges for the client.</p> <p>The server then returns the call using a phone number in its outgoing phone list for the matching circuit.</p>
Server One Charge Call ID (ISDN connections only)	<p>Designates the router as the callback server using caller ID. Also indicates that only the server will be charged for the return call to the client.</p> <p>The server receives a call from the client. The server, using incoming filtering, verifies that the client is an authorized caller by matching the client's phone number with a phone number and circuit number in the incoming phone list. If the server finds a matching entry, it refuses the call. By refusing the call, the server eliminates any phone charges for the client.</p> <p>The server then returns the call using the phone number in the original call's setup message.</p>

Additional Notes about the Callback Mode Parameter

If you modify the Callback Mode parameter, be aware of the following results:

- Server or Client Delay Time Resets

If you change the setting of the Callback Mode from a server mode to a client mode, or vice versa, the associated callback delay time resets to its default value.

For example, if you change the Callback Mode from Server to Client, and the Callback Server Delay Time was set to 5 seconds, this time resets to the default value of 0 seconds. Conversely, if you change the Callback Mode from Client One Charge to Server One Charge, the Callback Client Delay Time resets to its default of 5 seconds.

- Site Manager Prompts You to Enable Incoming Filtering

If you set the Callback Mode to either Server One Charge or Server One Charge Call ID, Site Manager prompts you to enable the Incoming Filter parameter. For these two callback modes, the router uses incoming filtering to verify that the client is an authorized caller. If you later change the Callback Mode from these modes to any other callback mode, Site Manager prompts you to disable incoming filtering.

- Site Manager Requests Caller Resolution Information

If you set the Callback Mode to Server, Server Call ID, Client, or Client One Charge, Site Manager prompts you to make a Caller Resolution Table entry by displaying the Caller Resolution Info window. These callback modes require a caller resolution entry to authenticate callers on each side of the connection and, for the server, to indicate which circuit to activate for a call.

- Site Manager Requests an Outgoing Phone Number

If you set the Callback Mode to Server or Server One Charge and there are no entries in the outgoing phone list, Site Manager prompts you to enter a phone number by displaying the Outgoing Phone Number window.

Parameter: Callback Server Delay Time (sec)

Default: 0

Options: 0 to 1800 seconds

Function: Specifies the amount of time the server waits before calling back the client. Delaying the call allows time for the client's modem to disconnect or for its ISDN connection to stop retrying the original call.

This parameter is available only if the Callback Mode is set to one of the server options.

Instructions: Enter the amount of time that you want the server to wait before calling the client back. If you are using a modem, enter a value greater than 6 seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.5.1.54

Parameter: Callback Client Delay Time (sec)

Default: 5 seconds

Options: 0 to 1800 seconds

Function: Specifies the amount of time the client waits for a return call from the server. During this time, the client will not place an outgoing call to any other destination. The delay gives the server a chance to return the initial call.

This parameter is available only if the Callback Mode is set to one of the client options.

Instructions: Enter the amount of time the client should wait for the server to call. Ensure that the value is greater than the Callback Server Delay Time.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.5.1.55

Using the Incoming Phone List to Identify the Client

If the Callback Mode of your router is Server One Charge or Server One Charge Call ID, the router uses incoming filtering to validate the user, not PPP authentication, which relies on the Caller Resolution Table. Using incoming filtering, the router can maintain security while refusing the initial call from the client. This saves the client phone charges.

When the server uses incoming filtering, it relies on the incoming phone number to identify the caller. When the server receives the call from the client, it matches the client's phone number with a phone number and circuit number in the incoming phone list. The circuit number, specified in the Callback Demand Circuit Name parameter, is the circuit that the server uses to place the outgoing call back to the client.

The Callback Demand Circuit Name parameter is located in the Incoming Phone List window. To access this window select Dialup > Incoming Phone List.

Parameter: Callback Demand Circuit Name

Default: None

Options: Available callback demand circuits

Function: When the Callback Mode is Server One Charge or Server One Charge Call ID, this parameter specifies the circuit that the server uses to call back the client.

Instructions: Click on the Values button. Site Manager displays a list of available callback circuits. Highlight the circuit you want and click on OK.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.7.1.9

Standby Circuits

The expansion of enterprise networks to remote branch sites requires reliable access to these sites. Therefore, it is important to have alternate connections to the remote sites in case a primary connection fails. To provide alternate connections, you can use *standby circuits*. A standby circuit is a special type of demand circuit that gives the router an alternate path to the destination. The destination can be a different interface at the primary circuit's original site or an entirely different site.

Standby circuits support asynchronous (RS449), synchronous (RS449, V.35, RS422, and X.21), and ISDN interfaces. Point-to-Point protocol (PPP) is the only data link protocol that you can configure across a standby circuit.

Comparing Standby Circuits with Dial Backup Circuits

Although standby circuits and dial backup circuits can both aid failed primary circuits, they differ in the following ways:

- Each standby circuit has a unique configuration; it does not adopt the primary circuit's configuration. In contrast, most dial backup circuits inherit the primary circuit's configuration.

This unique standby configuration offers a lot of flexibility when setting up alternate paths to remote sites. For example, you may want the standby circuit to have a different destination than the primary circuit, or you may enable compression on the standby circuit but not on its associated primary circuit.

- Standby circuits let you control when the router switches from the standby circuit back to the recovered primary circuit. You do not have this option with dial backup circuits. In dial backup configurations, the router terminates the backup circuit when the primary recovers. For example, to ensure the stability of a recovered primary before bringing down the standby, you can delay the return of data to the primary.
- Standby circuits support PPP multilink.

You can assign a bandwidth-on-demand pool to the hot standby circuit to relieve congestion. Bandwidth-on-demand connections use PPP multilink, the protocol that lets the router use multiple dialup lines simultaneously to transmit data. You do not have this option for dial backup circuits.

If you associate a bandwidth-on-demand pool to a hot standby circuit, the router monitors the hot standby circuit for congestion. If the circuit becomes congested, the router activates lines from the bandwidth-on-demand pool until congestion is relieved.

For maximum flexibility and control when setting up alternative connections, as well as quick response to failed primary circuits, standby circuits are the best choice. However, for more straightforward applications, where you do not need to configure an alternate site for the backup connection, dial backup circuits are more suitable. Either option ensures that critical data reaches its destination.

How Standby Circuits Work

There are two types of standby circuits:

- **Hot standby** -- A hot standby circuit backs up a failed primary circuit. When the primary circuit fails, the hot standby circuit activates to provide another route to the destination. A hot standby circuit can connect to another standby circuit, a demand circuit, or a demand circuit group.

Hot standby circuits can support the following types of primary circuits:

- Single leased PPP circuit
- PPP multilink circuit
- PPP multiline circuit
- Frame Relay primary circuit that has a service record containing only one PVC
- Bandwidth-on-demand circuit

If the hot standby circuit itself becomes congested, you can use bandwidth-on-demand service to provide additional lines. To do this, associate a bandwidth-on-demand pool with the hot standby circuit.

Hot standby circuits can back up primary circuits on any slot, not just the slot on which the hot standby circuit resides. For example, if a primary line on slot 4 fails, the router can activate a standby connection from slot 3.

- **Standby** -- A standby circuit has no relationship with the primary circuit. It does not back up a primary circuit if the primary fails. Instead, a standby circuit answers incoming calls destined for it. A standby circuit can also carry data when you manually activate it.

Standby circuits support standard demand circuit features such as multilink, unnumbered interfaces, dial optimized routing, and outbound filtering. Refer to *Configuring Dial Services* for more information about these features.

A standby circuit activates for one of the following reasons:

- A primary circuit fails.

A hot standby circuit activates when the primary circuit fails and then takes over data transmission. This activates an outgoing standby circuit. To determine if a primary failed, the router relies on Breath of Life (BofL) messages for PPP primary circuits and A-bit notification for Frame Relay primary circuits.



Note: When you associate a PPP primary circuit with a hot standby circuit, the router automatically enables BofL on the primary, so be sure to manually turn on BofL on the other side of the PPP primary connection. This does not apply to Frame Relay primary circuits.

- A call comes in designated for the standby circuit.

A standby circuit activates only when the remote router calls the host router across a standby circuit or you activate the circuit manually. This activates an *incoming standby circuit*.

- You activate a standby circuit manually.

Typically, circuits at the remote site will be hot standby circuits, while at the central site they will be normal standby circuits. This configuration allows the remote router to monitor the status of its primary connections, which number significantly fewer than the connections at the central site.

Configuring Each Side of the Standby Connection

A standby circuit must be configured at the central site and at the remote site. To configure a standby circuit, you select a demand circuit and then set the Standby Mode parameter to either Hot Standby or Standby.

When setting up a standby connection, note the following guidelines:

- Configure one side of the connection to initiate calls (the hot standby circuit). This is the outgoing side of the connection.

- Configure one side of the connection to receive calls (the standby circuit). This is the incoming side of the connection.



Note: If the standby circuit is part of a bandwidth-on-demand configuration, the outgoing side should be the *monitor* router, while the incoming side is the *nonmonitor* router.

- If you configure routing protocols on the standby circuit, the Inactivity Timeout parameter does not work. Once the router brings up the standby circuit, the routing protocols keep the connection active.
- Configure Time of Day schedules and failback timers only on the hot standby side of the connection.
- Use CHAP or PAP as the authentication protocol for the circuit.
- If you want to use unnumbered interfaces, configure them on the outgoing hot standby circuit and configure unnumbered demand circuit groups on the incoming standby circuit.

Balancing Traffic Between a Primary and a Hot Standby Circuit

Once a hot standby circuit is active, the routing protocol activates and finds an alternative route to the destination. When the primary recovers and resumes data transmission, the routing protocol deactivates. This is referred to as a *failback* to the primary circuit.

You can control the failback to the recovered primary circuit manually or automatically. One advantage of controlling failback is that you can delay the return of traffic to the primary circuit. This lets the primary circuit stabilize before it resumes transmission of critical data.

The following configuration choices enable you to manage traffic between the primary circuit and the hot standby circuit:

- RIP or OSPF precedence and cost parameters

The router sends traffic across the circuit with the better cost route. If the better route is the hot standby circuit, traffic continues across this circuit even if the primary recovers. Conversely, traffic will resume across the primary if that is the better route. Refer to *Configuring IP Services* for information about RIP and OSPF.

- Standby Failback Mode parameter

This parameter specifies the method that the router uses to deactivate the standby circuit and return to the primary circuit. Using this parameter, you can control the failback to the primary circuit automatically or manually.

- Failback Time parameter

This parameter specifies the delay before returning to the recovered primary circuit. The routing level configuration supersedes the value of this parameter. If the primary has a better cost route, traffic returns to the primary, regardless of the delay specified by this parameter. If the hot standby circuit has a better cost route, the router uses this circuit for the duration of the failback timer.

Using Time of Day Schedules to Manage Standby Circuits

Part of the standby circuit configuration is the Time of Day schedule. The Time of Day schedule defines the interval that the standby circuit is available. It also determines how the router uses the primary and standby circuits when they are both active.

You may configure several Time of Day schedules for a circuit in a 24-hour period. If you do not set up a schedule for the circuit, the circuit's availability defaults to 24 hours a day.

The Failback Time parameter is part of the Time of Day schedule. Depending on how you set the Failback Time, there may be a delay between the time the standby circuit is disconnected and the time traffic returns to the primary circuit.

Therefore, it is important to balance the use of the primary and standby circuits to ensure that data reaches the remote destination.

Be aware that the router monitors the primary circuit during the failback time. If the primary fails, the router continues to use the standby circuit.

Configuring Multiple Time of Day Schedules

Configuring multiple Time of Day schedules for one circuit can cause schedules to conflict. The next paragraphs describe two examples where this happens.

If the Failback Time for the active Time of Day schedule overlaps with the Failback Time of the next schedule, the router uses the Failback Time of the latter schedule. The router deducts the amount of failback time already elapsed from the latter schedule (refer to “Example 1: Failback Times That Overlap”).

[Table 8](#) shows the Time of Day configuration for standby circuit 1.

Table 8. Time of Day Schedules for Standby Circuit 1

Time of Day Schedule 1	Time of Day Schedule 2	Time of Day Schedule 3
Start Time: 8 a.m. End Time: 11a.m.	Start Time: 11 a.m. End Time: 5 p.m.	Start Time: 7 p.m. End Time: 11 p.m.
Failback Time: 60 minutes	Failback Time: 10 minutes	Failback Time: 10 minutes

Example 1: Failback Times That Overlap

- 7:00 a.m.** The primary circuit fails.
- 8:00 a.m.** The standby circuit becomes available.
- 10:30 a.m.** The primary circuit recovers and the failback timer starts counting down for 60 minutes. Data is still traveling across the standby circuit.
- 11:00 a.m.** Since 10:30 a.m., 30 minutes of failback time have elapsed for Time of Day Schedule 1, but Time of Day Schedule 2 is now active. This new schedule has a failback of 10 minutes, which supersedes the previous failback time of 60 minutes.
- Since 10:30 a.m., 10 minutes have already passed, so data traffic returns to the primary circuit.

If the failback time expires after the standby circuit expires, the router still deactivates the standby. The router will not wait for the primary circuit to recover. There is no circuit available until the primary circuit reactivates or the next interval arrives when the standby circuit is available (refer to “Example 2: Failback Time Results in No Available Circuit”).

Example 2: Failback Time Results in No Available Circuit

3:00 p.m.	The primary circuit fails and a standby circuit is activated, as specified in Time of Day Schedule 2.
4:55 p.m.	The primary circuit recovers. The failback timer starts counting down from 10 minutes.
5:00 p.m.	After 5 minutes, Time of Day schedule 3 is active. The standby circuit is brought down and will not be available until 7:00 p.m.
	For 5 minutes, there is no circuit available to transmit data.
5:05 p.m	Data traffic transfers back to the primary circuit.

Standby Configuration Parameters

Standby configuration parameters include the parameters described in the following sections:

- [Demand Circuit Parameters](#)
- [Time of Day Schedule Parameters](#)

Demand Circuit Parameters

To access the standby circuit parameters, select Dialup > Demand Circuits.

Parameter:	Standby Mode
Default:	Demand Normal
Options:	Demand Normal Standby Hot Standby
Function:	Indicates if this circuit operates as a demand circuit or as a standby circuit.
Instructions:	Select Standby to act as a standby circuit for incoming calls. Select Hot Standby if you want this circuit to aid a failed primary circuit. Accept the default if you want this circuit to operate as a demand circuit.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.4.5.1.50

Parameter: Standby Failback Mode

Default: None

Options: None | Automatic | Manual

Function: Controls the failback from the hot standby circuit to the primary. This option is available only if the Standby Mode is Hot Standby.

Instructions: Select one of the following options:

Automatic -- automatically deactivates the hot standby circuit and sends data traffic back across the primary circuit when it recovers. This option takes precedence over any Time of Day schedule.

Manual -- controls the primary and hot standby circuits by operator intervention. To return traffic to the primary you manually bring down the standby circuit. This option overrides the Time of Day schedule.

None -- instructs the router to rely exclusively on the Time of Day schedule for primary and standby circuit operation and to ignore this parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.5.1.51

Parameter: Manual Standby Action

Default: No Action

Options: No Action | Activate | Deactivate

Function: Allows you to manually control the standby circuit.

Instructions: Select Activate to activate a standby or hot standby circuit. Select Deactivate to bring down a standby circuit. Accept the default, No Action, if you do not want to manually activate a standby circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.5.1.52

Parameter: Standby Primary Circuit

Default: None

Options: Circuit number of the leased primary or bandwidth-on-demand primary circuits.

Function: Specifies the primary circuit that the hot standby circuit backs up. This option is available only if the Standby Mode is Hot Standby.

Instructions: Click on the Values button. Site Manager displays a list of primary and bandwidth-on-demand circuits. Highlight the circuit for which standby service should be provided and click on OK.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.5.1.4

Time of Day Schedule Parameters

To access the Circuit Time of Day Schedule window, click on Schedule from the Demand Circuits window.

Parameter: Failback Time (min.)

Default: 0

Options: 0 to 1439 minutes

Function: Indicates the amount of time the router waits before deactivating the standby circuit and returning to a recovered primary circuit. This option is available only if the Standby Mode is Hot Standby, the Standby Failback Mode is set to None, and you have selected a primary circuit for the Standby Primary Circuit parameter.

Instructions: Enter the amount of time, in minutes, that you want to delay the return to the primary circuit. Be sure to consider how much time it takes to ensure that the primary is stable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.11.1.10

Parameter: TimeOfDay Failback Mode

Default: Automatic

Options: Automatic | Manual

Function: This parameter controls the failback to the primary circuit if the Standby Failback Mode parameter is set to None.

Instructions: Select Automatic to automatically deactivate the hot standby circuit and return to the primary. The Failback Time parameter for this circuit determines the failback delay. Select Manual to deactivate the hot standby circuit by operator intervention.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.11.1.9

Configuring DLSw Services

Data Link Switching (DLSw) now supports:

- Bisync over TCP (BOT) on the Advanced Remote Node (ARN) using the Serial adapter module.
- Token Ring LAN emulation on DLSw and APPN networks. Refer to *Configuring ATM Services* for information on LAN emulation.

The following sections are new in *Configuring DLSw Services*:

- [RFC 1434 and RFC 1795 Support](#)
- [Multislot Broadcasts](#)
- [Session Alive Filter](#)
- [Qualified Link Level Control Support](#)

RFC 1434 and RFC 1795 Support

RFC 1795 is an implementation of DLSw that supersedes RFC 1434. RFC 1795 incorporates new features such as capabilities exchange, new flow control mechanisms (called adaptive pacing), and improved DLSw data flows.

RFC Parameter

With Release 11.01, you can select the specific RFC implementation on the router with the RFC parameter.

Parameter: RFC

Default: RFC1434

Options: RFC1434 | RFC1795

Function: Selects the RFC implementation to run on the router, either RFC 1434 or RFC 1795.

Instructions: Click on Values and select RFC 1434 or RFC 1795. Refer to *Configuring DLSw Services* for detailed information about the differences between these RFCs.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.28

Initial Pacing Window

The *initial pacing window* is an RFC 1795 Capabilities Exchange function that allows a DLSw router to advertise the initial number of data frames that it will accept from a sending DLSw router. After a connection is established between two DLSw routers, the two DLSw routers exchange their initial pacing window sizes within Capabilities Exchange messages.

Depending on the amount of network traffic during the session, the router may increase or decrease the pacing window size. An increase in the window size means that the router is granting permission to receive more data frames from the sending DLSw router. A decrease in the window size means that the router is reducing the number of data frames that it will accept from the sending DLSw router.

The Initial Pacing Window parameter is available from the DLSw Global Parameters window.

Parameter: Initial Pacing Window

Default: 5

Options: 5 to 100 frames

Function: Specifies the initial number of received data frames that the local DLSw router permits during an established connection with another DLSw router. The two DLSw routers advertise their initial pacing value to each other over capabilities exchange messages.

Instructions: Enter a value in the range 5 to 100. Depending on the amount of network traffic during the session, the router may increase or decrease the pacing window size. An increase in the window size means that the router is granting permission to receive more data frames from the sending DLSw router. A decrease in the window size means that the router is reducing the number of data frames that it will accept from the sending DLSw router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.27

Multislot Broadcasts

The software now allows you to isolate CANUREACH frames to the DLSw slots on which the frames are received. By default, when the router receives CANUREACH frames, the software converts these frames to SNA frames and broadcasts them across all DLSw slots. The Multislot Broadcasts parameter allows you to enable or disable CANUREACH broadcasts over all DLSw slots.



Note: Because a DLSw slot can have multiple ports (or interfaces), the Multislot Broadcasts parameter setting affects all DLSw ports on the slot on which CANUREACH frames are received.

Parameter: Multislot Broadcasts

Default: Enable

Options: Enable | Disable

Function: Broadcasts received CANUREACH frames over all DLSw slots, or to the specific DLSw slots on which the frames are received.

By default, when the router receives CANUREACH frames over a DLSw port, the software first converts the frames to SNA frames before broadcasting the frames across all configured DLSw slots. If you disable this feature, the router will broadcast the frames only over the DLSw slots on which the frames are received.

Instructions: Click on Values and select Enable or Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.5.1.26

Session Alive Filter

The DLSw software now allows you to enable or disable NetBIOS session alive frame transmissions. Previously, a NetBIOS session would always transmit session alive frames over DLSw every 30 seconds. These session alive frames could cause lines to remain active unnecessarily, possibly increasing the usage cost of the line.

Use the Technician Interface to enable or disable NetBIOS session alive frame transmissions.

To enable the NetBIOS session alive filter, stopping session alive frame transmissions, issue the following Technician Interface command:

set wfDls.wfDLsNetbiosSessionAliveFilter.0 1;commit

To disable the NetBIOS session alive filter, allowing session alive frame transmissions, issue the following Technician Interface command:

set wfDls.wfDLs.NetbiosSessionAliveFilter.0 2;commit

Qualified Link Level Control Support

DLSw is now supported over X.25 links using Qualified Link Level Control (QLLC). Refer to *Configuring X.25 Services* for information about QLLC.

Configuring IP Services

The following sections are amendments to *Configuring IP Services*:

- [Opening the IP Accounting Window](#)
- [Controlling Notification of a Full IP Accounting Table](#)

The following section is new in *Configuring IP Services*:

- [Configuring an OSPF Neighbor on a Standard Point-to-Multipoint Interface](#)

Opening the IP Accounting Window

Site Manager provides an IP Accounting window that allows you to modify IP Accounting parameters. (The IP Globals window does not include these parameters.)

Beginning at the Configuration Manager, use the following path to open the IP Accounting window:

Protocols > IP > Accounting

Controlling Notification of a Full IP Accounting Table

By default, IP Accounting sends a log message when the active IP Accounting table is 80 percent full. You must configure a trap to be sent. Use Site Manager to configure a trap exception for Entity 6 and event 99.

You can use Site Manager to specify a value from 1 to 100 (indicating the percentage of the maximum size) that causes IP Accounting to send a trap message.

Once IP Accounting has generated an event message indicating that the IP Accounting table has been filled to the specified percentage, IP Accounting continues to send a message for every percent above the configured value until you copy the active table to the checkpoint table, or until the active table is 100 percent full.

For example, if you use the default (80 percent), IP Accounting sends a log message when the active table is 80 percent full, 81 percent full, 82 percent full, and so on, until you copy the table or until the active table is 100 percent full.

Configuring an OSPF Neighbor on a Standard Point-to-Multipoint Interface

OSPF neighbors are any two routers that have an interface to the same network. In each OSPF network, routers use the Hello protocol to discover their neighbors and maintain neighbor relationships.

Beginning with Version 11.01, you can manually configure an OSPF neighbor on an OSPF interface that has been configured for a standard point-to-multipoint network. In previous versions, you could configure an OSPF neighbor manually on a nonbroadcast multi-access (NBMA) interface only. On a broadcast or point-to-point network, the Hello protocol dynamically discovers neighbors.

When you manually configure a neighbor on a standard point-to-multipoint interface, OSPF uses the OSPF multicast address 244.0.0.5, instead of the configured unicast address, to send Hello packets.

Configuring IP Utilities

The following NTP configuration option buttons have been renamed:

- In the NTP Access Configuration List window, the Add Access button has changed to the Add button, and the Delete Access button has changed to the Delete button.
- In the NTP Peer Configuration List window, the Add Peer button has changed to the Add button, and Delete Peer button has changed to the Delete button.

Configuring IPX Services

The following sections are amendments to Configuring IPX Services:

- [Configuring IPX Interface Cost Parameter](#)
- [Configuring Max Path and Max Path Splits for IPX](#)

Configuring IPX Interface Cost Parameter

The IPX interface Cost parameter now defaults to zero for all interfaces. For all non-WAN and HSSI interfaces, this translates into a tick cost of 1 in the routing table. For all WAN interfaces, this translates into a tick cost of 6 in the routing table.

Configuring Max Path and Max Path Splits for IPX

Prior to Version 11.0, configuring the Max Path parameter in the IPX global record enabled IPX to store and load balance over multiple equal cost paths. This function is now two separate parameters in the IPX global record, *Max Path* and *Max Path Splits*. The Max Path parameter now sets the number of paths that IPX can store to each individual destination network. For IPX to function correctly, set the Max Path parameter to the highest number of paths that exist from the router to any destination network, regardless of cost. The Max Path Splits parameter determines whether IPX should load balance. If you enable Max Path Splits, IPX uses up to Max Path equal cost paths that are equal to the lowest cost path. If you disable Max Path Splits, IPX uses only the lowest cost path to send data to a destination network.

Configuring Line Services

The following sections are amendments in *Configuring Line Services*:

- [Setting the Asynchronous Baud Rate](#)
- [Setting the Synchronous IFTF Pattern](#)
- [Setting the HSSI Carrier Loss Timeout](#)
- [Setting the Synchronous Hold Down Time](#)

The following sections are new in *Configuring Lines Services*:

- [Ethernet - CSMA/CD Line Service Enhancement](#)
- [BayStack Router Interfaces](#)

Setting the Asynchronous Baud Rate

You control the baud rate for Asynchronous PPP using the Async Baud Rate parameter on the Edit Sync Parameters window. The baud rate is the transmission speed (in bits per second) between the router and the modem. To set the baud rate for the asynchronous interface, you must first set the WAN Serial Interface Type parameter to Async.

By default, the asynchronous baud rate is 9600. Set this parameter to a value that is greater than or equal to the speed at which the modem connects, but that is independent of that speed. For example, you set a V.34 modem to its maximum modular connection speed of 28800 Kb/s or higher. However, you could set the baud rate for a V.42 bis or MNP 5 data compression modem with a high (4 to 1) compression ratio to 115200 baud.

You can select one of the following baud rates:

1200	38400
2400	57600
4800	64000
9600	76800
14400	96000
19200	115200
28800	

Setting the Synchronous IFTF Pattern

The router transmits an interframe time fill (ITTF) pattern when there is no data to transmit on a synchronous line. There are two ITTF patterns:

- HDLC Flags, an 0x7E pattern (0 1 1 1 1 1 1 0)
- Idles, an 0xFF pattern (1 1 1 1 1 1 1 1)

HDLC Flags is the default ITTF pattern for all synchronous media types except ISDN BRI. For ISDN BRI, the default pattern is Idles. To use these defaults, leave the Force ITTF parameter set to Default. Or, you can override the defaults by setting the Force ITTF parameter to Force Flags or Force Idles.

For a dial-on-demand interface, set the Force ITTF parameter to Force Idles.

Setting the HSSI Carrier Loss Timeout

You can determine how many seconds the HSSI line driver waits after losing the Carrier Signal before changing to the Carrier Lost state. If the Carrier Signal returns prior to reaching this threshold, the driver never enters Carrier Lost.

For most HSSI lines, keep the default value of zero (0) seconds; the driver immediately transitions to Carrier Lost state upon detecting carrier loss. For a problem line, enter the number of seconds (0 to 2147483647) that you want the router to detect Carrier Loss before entering a Loss state.

Setting the Synchronous Hold Down Time

The description in *Configuring Line Services* for the Synchronous Hold Down Time parameter is incorrect. The correct description follows.

On a synchronous interface that is configured for dial services, you can specify a time period (0 to 9999 seconds) for the router to wait before bringing down a backup line. This delay allows time for the primary line to fully recover before deactivating the backup line.

For a dial-on-demand interface, the Sync Hold Down Time parameter is set to 3 seconds by default.

Ethernet - CSMA/CD Line Service Enhancement

The following section about the operation of Breath of Life (BofL) messages on Ethernet circuits is new in the *Configuring Lines Services* guide for Router Software Version 11.01.

Ethernet BofL Messages

The router sends BofL messages for carrier detection on Ethernet circuits when the CSMA/CD interface transmitter is idle. Even with BofL enabled on the interface, the router does not send BofL messages if it is already transmitting regular data traffic.

With default values configured, the router declares an Ethernet interface down after 25 seconds (5 retries of 5 seconds each without a successful frame transmission). When you configure router redundancy on an Ethernet interface, Site Manager automatically adjusts CSMA/CD BofL parameters to reduce the time it takes the router to declare an interface down when there is a loss of service. With default router redundancy values configured, the router declares the interface down after 2 seconds (4 retries of .05 seconds each).

The following describes the two new BofL parameters:

Parameter: BofL Retries

Default: 5; 4 when the interface is configured for router redundancy

Options: 1 to 5 retries

Function: Specifies the number of BofL messages this interface can retransmit before the router declares the circuit down.

Instructions: Either accept the default of 5 BofL Retries, or specify a lower value. Use this parameter in conjunction with BofL Timeout Divisor and BofL Timeout to decrease the time it takes the router to declare an interface down.

MIB Object ID: 1.3.6.1.4.1.18.3.4.1.1.59

Parameter: BofL Timeout Divisor

Default: 1; 10 when the interface is configured for router redundancy

Options: An integer 1 to 59, less than or equal to the value of the BofL Timeout parameter

Function: The BofL Timeout parameter specifies a time period between transmissions of BofL messages from this Ethernet interface. Beginning with Router Software Version 11.01, the actual time between BofL transmissions is the value of the BofL Timeout parameter divided by the value of the BofL Timeout Divisor parameter. When set to a value greater than 1, this parameter reduces the value of BofL Timeout.

When you configure router redundancy on an interface, Site Manager automatically sets this parameter to reduce the time between BofL transmissions. If the circuit goes down, the interface reaches the BofL Retries value sooner, thus reducing the time it takes the router to declare a circuit down.

Instructions: Increase the value of this parameter if you want line status be detected in less than 1 second intervals. Leave this parameter set to 1 and use the BofL Timeout parameter for 1- to 5-second timeout values.

For example, with the BofL Timeout parameter set to 5 seconds and the BofL Timeout Divisor set to 10, the router sends a BofL message every 0.5 second (5 divided by 10). With BofL Timeout set to 5 seconds and the BofL Timeout Divisor set to 1, transmissions are every 5 seconds.

MIB Object ID: 1.3.6.1.4.1.18.3.4.1.1.60

BayStack Router Interfaces

The following sections about BayStack router interfaces are new in the *Configuring Line Services* guide for Router Software Version 11.01:

- [Configuring a DSU/CSU Interface](#)
- [Using DSU/CSU Loopback Tests](#)
- [Configuring a V.34 Modem Interface](#)
- [Customizing the V.34 Modem Initialization String](#)
- [Resetting the V.34 Modem Configuration](#)

Configuring a DSU/CSU Interface

BayStack™ AN®, ANH™, and ARN™ routers support an optional DSU/CSU adapter module that provides direct connection to 56-Kb/s Dataphone Digital Services (DDS) or 64-Kb/s Clear Channel (CC) service.

The DSU/CSU module converts serial DTE interface signals to baseband bipolar line signals, and vice versa. The DSU/CSU module consists of a DDS channel terminator (the CSU) and an encoder-decoder (the DSU). The DSU terminates the data circuit to the DTE and contains the transmitter, receiver, clock recovery circuitry, and the interface to the router. Both DDS 56K and 64K Clear Channel circuits provide a maintenance loopback path.



Note: AN and ANH DSU/CSU interfaces do not support network booting in Router Software Version 11.01. The ARN DSU/CSU network supports booting over interfaces configured for 64-Kb/s CC service.

The following sections describe BayStack router support for DSU/CSU interfaces:

- [Configuring a DSU/CSU Interface](#)
- [Using DSU/CSU Loopback Tests](#)

For information on viewing DSU/CSU configuration and status information, refer to [show sync](#) on [page -121](#). For information about the event messages that the DSU/CSU driver logs, refer to the DSUCSU information in [Event Messages for Routers and BNX Platforms](#) on [page -75](#).

To configure a DSU/CSU interface using the Configuration Manager:

1. **From the Configuration Manager window, click on the COM connector for the DSU/CSU Adapter Module.**

The Add Circuit window appears.

2. **Click on OK to accept the default circuit name.**

The WAN Protocols window appears.

3. **Select the WAN protocol for the interface and click on OK.**

(Choices are Standard, PassThru, PPP, SMDS, Frame Relay, X25, ATM DXI, or SDLC).

The Protocols window appears.

4. Select bridging and routing protocols for the interface and click on OK.
5. Configure protocol parameters, using the applicable protocol manual for information.

The Configuration Manager window reappears.

6. If necessary, edit the serial line parameters for the interface:



Note: The default line configuration is appropriate in most cases.

- a. Once the Configuration Manager window reappears, click on the COM connector.

The Edit Connector window appears ([Figure 2](#)).



Figure 2. DSU/CSU Edit Connector Window

- b. Click on Edit Line.

The Edit Sync window appears. Refer to *Configuring Line Services* for information on the line parameters you can configure.

- c. After editing line parameters, click on OK.

The Edit Connector window reappears.

7. Click on Edit DSU/CSU.

The Edit Adapter Module DSU CSU Parameters window appears ([Figure 3](#)).



Figure 3. Edit Adapter Module DSU/CSU Parameters Window

8. Click on OK to accept the default configuration, or edit the Option Mode, Transmit Clock Select, and 64K Transmit Monitor DSU/CSU parameters using the descriptions that follow.

DSU/CSU Configuration Parameters

Parameter: Option Mode

Default: DDS1-56KBPS

Options: DDS1-56KBPSs | CC-64KBPS

Function: Identifies the type of Telco service to which the DSU/CSU is connected.

Instructions: The data rate of DSU/CSU must match the network service. Select DDS1-56KBPSs when connected to a DDS1 56-Kb/s line. Select CC-64KBPS when connected to a Clear Channel 64-Kb/s line.

MIB Object ID: 1.3.6.1.4.1.18.3.4.30.1.1#6

Parameter: Transmit Clock Select

Default: Slave

Options: Slave | Master

Function: Determines the default transmit timing (clock) source for transmitting data to the network. When set to Master, an internal oscillator in the DSU creates the clock for a private-wire configuration. In Slave mode, a PLL internal to the DSU will recover and synchronize the DSU clock.

Instructions: Set both ends to Slave for a Telco network. For a private-wire configuration, set one end to Master and the other end to Slave. Note that there can be only one clock source on a DDS line.

MIB Object ID: 1.3.6.1.4.1.18.3.4.30.1.1#7

Parameter: 64K Transmit Monitor

Default: Disabled

Options: Enabled | Disabled

Function: Valid only in 64K Clear Channel mode (Option Mode set to CC-64KBPS). When enabled, 64K Transmit Monitor suppresses data to prevent unintended duplication of a network control code. For example, user data that happens to include the text of a loopback control code could place the remote end of the connection into a loop.

Instructions: Enable to monitor and suppress user data. Keep Disabled to allow all data.

MIB Object ID: 1.3.6.1.4.1.18.3.4.30.1.1#9

Using DSU/CSU Loopback Tests

The DSU/CSU module provides a set of loopback modes for testing both the router's DSU/CSU interface and the network/Telco circuit to the router. This section provides the following information:

- About the Loopback Tests
- Configuring V.54 Loopback Tests

About the Loopback Tests

You can activate DSU/CSU tests from the Configuration Manager, as described in the next section, “Configuring V.54 Loopback Tests.” The DSU/CSU module also responds to CCITT V.54 loop-up and loop-down codes.

The following subsections describe the supported tests:

- Digital Loopback
- Remote Digital Loopback
- Local Analog Loopback
- Pattern-2047
- Telco Loopback

Digital Loopback (DL)

Digital Loopback mode tests the local DSU/CSU and the Telco circuit. The DSU/CSU enters Digital Loopback when it receives a CCITT V.54 loop-up code, or when configured in Configuration Manager.

In Digital Loopback mode, the DSU/CSU loops Transmit data to Receive data by retiming and reshaping data it receives from the network, and transmitting that data back to the network. The remote facility transmits back to the router (DTE) all data it receives from the BayStack router. [Figure 4](#) illustrates the operation of a Digital Loopback test.

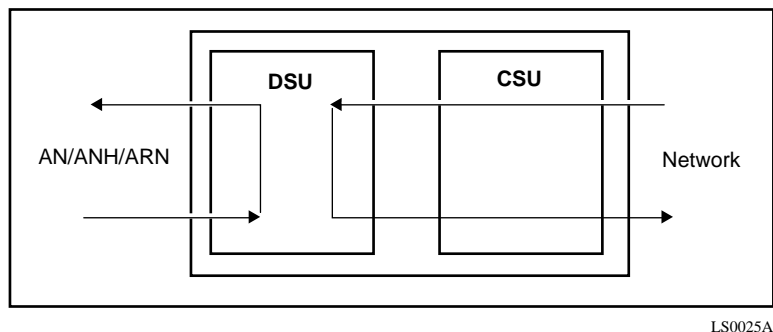
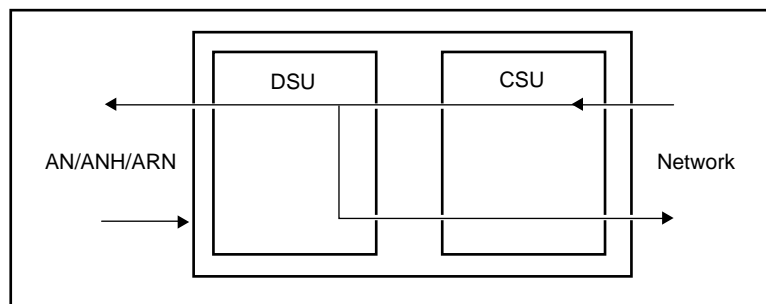


Figure 4. Digital Loopback

Remote Digital Loopback (RL)

Remote Digital Loopback (CCITT V.54 Loopback) tests the local DSU/CSU, the Telco circuit, and the remote DSU/CSU. The local DSU/CSU sends a V.54 loop-up code to the remote DSU/CSU to initiate a Digital Loop, and then sends a test pattern through the remote loop to check the returned data for errors. When the remote DSU/CSU receives the V.54 loop-up code, it provides the loopback path seen in [Figure 5](#).

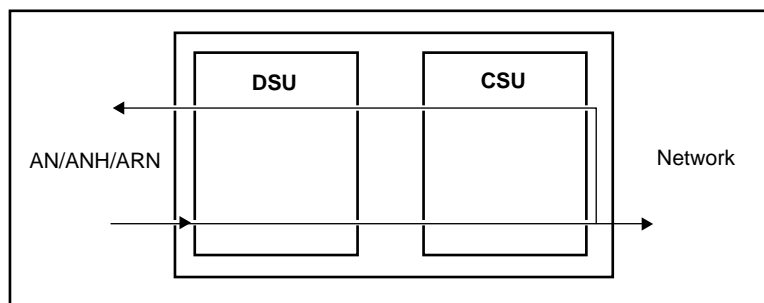


LS0024A

Figure 5. Remote Digital Loopback (CCITT V.54 Loopback)

Local Analog Loopback (AL)

Local Analog Loopback is a self-diagnostic local test, seen in [Figure 6](#).



LS0023A

Figure 6. Analog Loopback

While operating the local loop test, the CSU transmits data to the network to avoid causing a carrier alarm.

Pattern Only Test

In the Pattern-2047 test, the DSU sends a 2047 BERT pattern to the carrier network without initiating loopback ([Figure 7](#)).

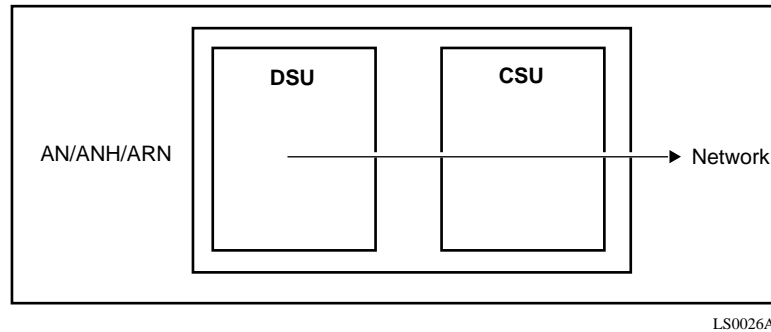


Figure 7. Pattern 2047 Test

The test allows you to connect a BERT tester at the remote end of a DDS line to verify data passing across the line.

Telco-Activated Loops

In addition to the tests you can initiate in the Configuration Manager, the DSU/CSU supports two standard DDS loopback conditions to test local loops and DDS termination equipment. The Telco facility initiates these tests upon customer request:

- CSU Loopback -- This test tries to isolate trouble in the network.
- DSU Loopback -- This test is similar to the Digital Loopback.


Configuring V.54 Loopback Tests

To configure a DSU/CSU loopback test from the Configuration Manager:

- 1. Click on the DSU/CSU COM connector.
- 2. In the popup window (refer to [Figure 2](#)), click on Edit DSU/CSU.
The Edit Adapter Module DSU CSU Parameters window appears (refer to [Figure 3](#)).
- 3. Accept or edit the V.54 Loopback and V.54 Time parameters, using the descriptions that follow.

DSU/CSU Loopback Parameters

Parameter:	V.54 Loopback
Default:	NO LOOP
Options:	NO LOOP ANALOG DIGITAL REM DIGITAL REM DIG/ PATTERN ANALOG/ PATTERN PATTERN-2047
Function:	Configures a V.54 loopback state within the DSU/CSU.
Instructions:	Select a test state or keep the default, No Loopback. Selecting a loopback state disrupts user data transmission through the DSU/CSU for a period specified in the V.54 Timer parameter.



Caution: When setting a remote loopback state, be sure to set the V.54 Timer parameter to a nonzero value. If the router’s only remote circuit is through the DSU/CSU, selecting a remote loopback state will leave this router unable to communicate with the remote router for the duration of the test.

MIB Object ID: 1.3.6.1.4.1.18.3.4.30.1#12

Parameter: V.54 Timer

Default: 0

Options: 0 to 255 seconds

Function: Sets the duration, in seconds, for the loopback testing specified in the V.54 Loopback parameter. Zero (0) indicates that loopback runs indefinitely.



Caution: Be sure to set a nonzero value when V.54 Loopback is set to a remote loopback state (REM DIGITAL or REM DIG/PATTERN), since a zero value will leave the router unable to communicate with the remote router if the only circuit is through the DSU/CSU interface.

Instructions: Enter the number of seconds for loopback testing to run.

MIB Object ID: 1.3.6.1.4.1.18.3.4.30.1#13

Configuring a V.34 Modem Interface

BayStack ARN routers support an optional V.34 modem adapter module.

For information on viewing configuration and status information about a V.34 modem interface, refer to [show sync](#) on [page -121](#). For information about the event messages that the V.34 modem driver logs, refer to the MODEM event information in “Event Messages for Routers and BNX Platforms.”

To configure a V.34 modem interface from the Configuration Manager:

- 1. Set up the dial services for this interface from the Dialup pulldown menu.**
Refer to *Configuring Dial Services* for information.
- 2. Click on the COM connector for the V.34 Modem Adapter module.**

The Edit Connector window appears ([Figure 8](#)).



Figure 8. V.34 Modem Edit Connector Window

3. **Edit the default physical layer (line) parameter values, or proceed with Step 4 to accept the default line configuration.**



Note: The default line configuration is appropriate in most cases.

To edit line parameters:

- a. **Click on Edit Line in the popup window.**

The Edit V.34 Sync Parameters window appears ([Figure 9](#)).

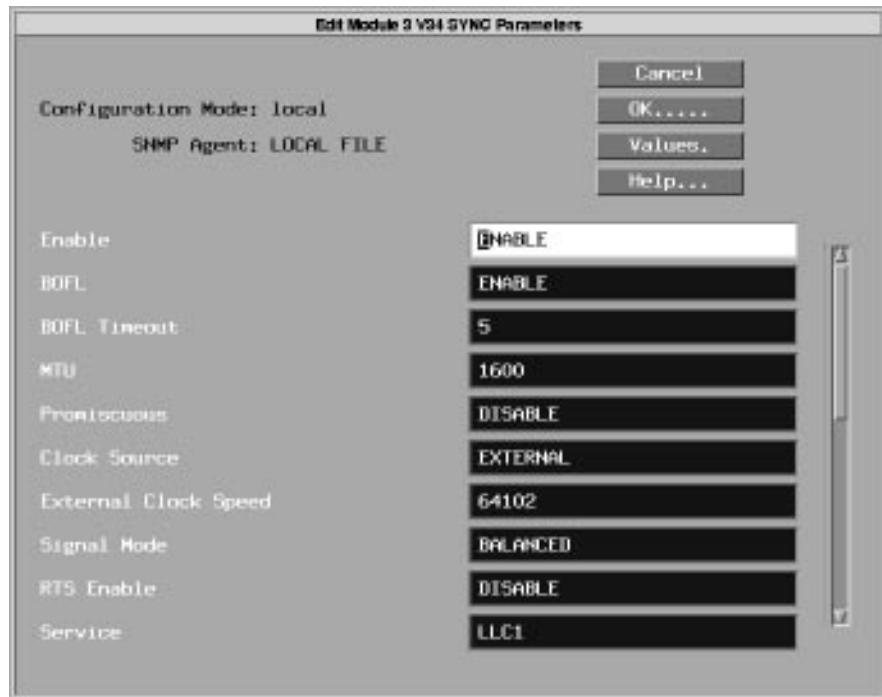


Figure 9. Edit V.34 Sync Parameters Window

Refer to *Configuring Line Services* or to the online help for information on the line parameters you can configure for a synchronous interface.



Note: The ARN V.34 Modem Adapter module does not support asynchronous services at this time.

b. After editing line parameters, click on OK.

The Edit Connector window reappears.

4. Click on Edit Modem.

The Configuration Manager displays the following warning message about changes to the modem initialization string.



5. Read the message and click on OK.

The Edit Adapter Module V.34 Modem Interface window appears [\(Figure 10\)](#).

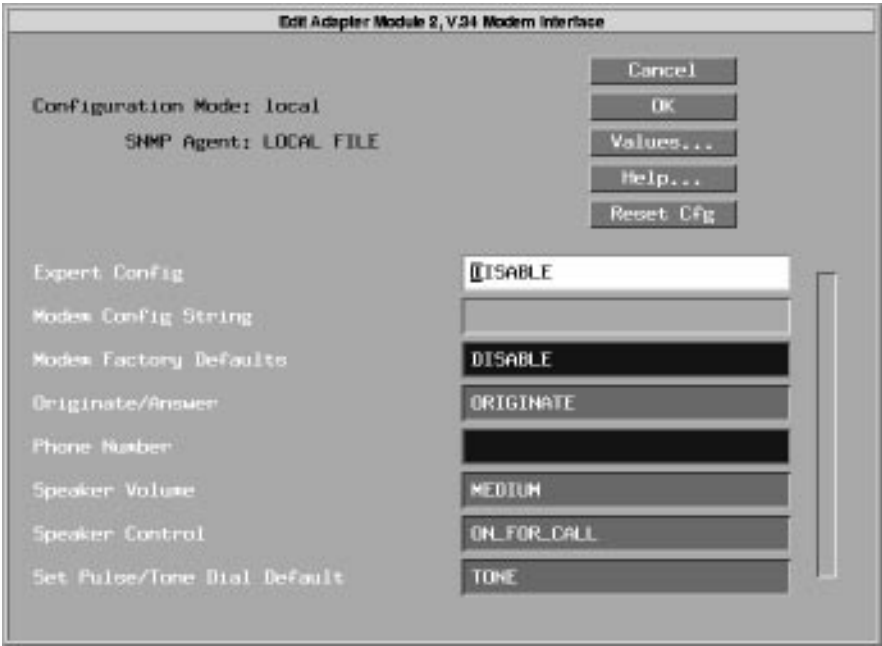


Figure 10. Edit V.34 Modem Interface Parameters Window

6. Enter the number for the modem to dial in the Phone Number field.



Note: Although you entered this phone number when setting up dial services, you must also enter the number in the Edit V.34 Modem Interface window.

7. Accept the factory default configuration for the other modem parameters (recommended), or edit them using the descriptions that follow.

V.34 Modem Interface Parameters

Parameter:	Expert Config
Default:	Disabled
Options:	Disabled Enabled
Function:	Enables or disables configuration of the Modem Config String parameter.
Instructions:	To use only the factory default configuration, leave this set to Disabled. Set to Enabled to enter an AT command string in the Modem Config String field.
Parameter:	Modem Config String
Default:	None
Options:	An ASCII text string of 3 to 34 characters
Function:	Specifies a modem initialization string to be sent to the modem <i>after</i> the default, factory-configured command string. Commands in this string take precedence over commands in the factory default string (AT&M2&Q2&D0&S1&R0S0=0M1L2T).
Instructions:	Enter an AT command string. Refer to Table 9 in “Customizing the V.34 Console Modem Initialization String” for a summary of AT commands.
MIB Object ID:	1.3.6.1.4.1.18.3.4.29.1.1#9



Caution: Entering an invalid command string could disable the modem. Site Manager can verify AT command string changes only when in dynamic mode.

Parameter: Modem Factory Defaults

Default: Enabled

Options: Enabled | Disabled

Function: Specifies whether exclusive use of the factory default initialization string is enabled or disabled. When enabled, the router sends only the default string (AT&M2&Q2&D0&S1&R0S0=0M1L2T) to the modem. When disabled, the router sends a user-specified initialization string (set in the Modem Config String parameter) after sending the default string. Commands in the user-specified string take precedence over the factory default command string.

Instructions: Enable or disable the exclusive use of the factory default modem initialization string.

MIB Object ID: 1.3.6.1.4.1.18.3.4.29.1.1#8

Parameter: Originate/Answer

Default: Originate

Options: Originate | Answer

Function: Determines whether the modem answers or originates calls.

Instructions: Set the modem to answer or originate calls.

Parameter: Phone Number

Default: None

Options: An ASCII text string

Function: Specifies the number to dial for calls that the modem originates.

Instructions: Enter a complete dial-out telephone number, including applicable country and area codes. Dial modifiers such as a comma, exclamation point, and ampersand (&) are valid, as are hyphen and parenthesis characters.

MIB Object ID: 1.3.6.1.4.1.18.3.4.29.1.1#18

Parameter: Speaker Volume

Default: Medium

Options: Off | Low | Medium | High

Function: Sets the volume of the modem speaker, or disables the speaker.

Instructions: Turn the modem speaker off, or set the volume to Low, Medium, or High.

Parameter: Speaker Control

Default: On For Call

Options: Off | On For Call | Always On | On For Answer

Function: Controls the modem speaker.

Instructions: Selecting On For Call turns the speaker on only when a call is established, and turns it off when the modem is receiving the carrier. Always On keeps the modem speaker on at all times. On for Answering turns the speaker on only when the modem is answering a call, and turns it off when the modem is receiving the carrier.

Parameter: Set Pulse/Tone Dial Default

Default: Tone

Options: Pulse | Tone

Function: Selects pulse or tone signals for the modem.

Instructions: Select Pulse only if your telephone line does not support Tone dialing.

Customizing the V.34 Modem Initialization String

To change the modem initialization string for the V.34 modem adapter module:

1. **In the Edit Adapter Module V.34 Modem Interface window (refer to [Figure 10](#)), set the Expert Config parameter to Enabled.**



Caution: Entering an invalid command string could disable the modem. Site Manager can verify AT command string changes only when in dynamic mode.

2. Enter a standard AT command string in the Modem Config String field.

Refer to [Table 9](#) for a summary of AT modem initialization commands.

3. Click on OK.

Table 9. Summary of AT Modem Initialization Commands

Command	Command Function
A/	Reexecute command.
A	Go off-hook and attempt to answer a call.
B0	Select V.22 connection at 1200 b/s.
B1	Select Bell 212A connection at 1200 b/s.
C1	Return OK message.
Dn	Dial modifier.
E0	Turn off command echo.
E1	Turn on command echo.
F0	Select auto-detect mode, equivalent to N1 (RC144).
F1	Select V.21 or Bell 103 (RC144).
F2	Reserved (RC144).
F3	Select V.23 line modulation (RC144).
F4	Select V.22 or Bell 212A 1200 b/s line speed (RC144).
F5	Select V.22 bis line modulation (RC144).
F6	Select V.32 bis or V.32 4800 line modulation (RC144).
F7	Select V.32 bis 7200 line modulation (RC144).
F8	Select V.32 bis or V.32 9600 line modulation (RC144).
F9	Select V.32 bis 12000 line modulation (RC144).
F10	Select V.32 bis 14400 line modulation (RC144).
H0	Initiate a hang-up sequence.
H1	If on-hook, go off-hook and enter command mode.
I0	Report product code.
I1	Report precomputed checksum.
I2	Report OK.
I3	Report firmware revision, model, and interface type.

(continued)

Table 9. Summary of AT Modem Initialization Commands *(continued)*

Command	Command Function
I4	Report response programmed by an OEM.
I5	Report the country code parameter.
I6	Report modem data pump model and code revision.
I7	Reports the DAA code (W-class models only).
L0	Set low speaker volume.
L1	Set low speaker volume.
L2	Set medium speaker volume.
L3	Set high speaker volume.
M0	Turn speaker off.
M1	Turn speaker on during handshaking and turn speaker off while receiving carrier.
M2	Turn speaker on during handshaking and while receiving carrier.
M3	Turn speaker off during dialing and receiving carrier and turn speaker on during answering.
N0	Turn off automode detection.
N1	Turn on automode detection.
O0	Go online.
O1	Go online and initiate a retrain sequence.
P	Force pulse dialing.
Q0	Allow result codes to DTE.
Q1	Inhibit result codes to DTE.
Sn	Select S-Register as default.
Sn?	Return the value of S-Register n.
=v	Set default S-Register to value v.
?	Return the value of default S-Register.
T	Force DTMF dialing.
V0	Report short form (terse) result codes.
V1	Report long form (verbose) result codes.
W0	Report DTE speed in EC mode.
W1	Report line speed, EC protocol, and DTE speed.

(continued)

Table 9. Summary of AT Modem Initialization Commands *(continued)*

Command	Command Function
W2	Report DCE speed in EC mode.
X0	Report basic call progress result codes. For example, OK, CONNECT, RING, NO CARRIER (also, for busy, if enabled, and dial tone not detected), NO ANSWER, and ERROR.
X1	Report basic call progress result codes and connection speeds. For example, OK, CONNECT, RING, NO CARRIER (also, for busy, if enabled, and dial tone not detected), NO ANSWER, CONNECT XXXX, and ERROR.
X2	Report basic call progress result codes and connection speeds. For example, OK, CONNECT, RING, NO CARRIER (also, for busy, if enabled, and dial tone not detected), NO ANSWER, CONNECT XXXX, and ERROR.
X3	Report basic call progress result codes and connection rate. For example, OK, CONNECT, RING, NO CARRIER, NO ANSWER, CONNECT XXXX, and ERROR.
X4	Report all call progress result codes and connection rate. For example, OK, CONNECT, RING, NO CARRIER, NO ANSWER, CONNECT XXXX, BUSY, NO DIAL TONE, and ERROR.
Y0	Disable long space disconnect before on-hook.
Y1	Enable long space disconnect before on-hook.
Z0	Restore stored profile 0 after warm reset.
Z1	Restore stored profile 1 after warm reset.
&C0	Force RLSD active regardless of the carrier state.
&C1	Allow RLSD to follow the carrier state.
&D0	Interpret DTR ON-to-OFF transition per &An:.
&Q0, &Q5, &Q6	The modem ignores DTR.
&Q1, &Q4	The modem hangs up.
&Q2, &Q3	The modem hangs up.
&D1	Interpret DTR ON-to-OFF transition per &Qn:.
&Q0, &Q1, &Q4, &Q5, &Q6	Asynchronous escape.
&Q2, &Q3	The modem hangs up.
&D2	Interpret DTR ON-to-OFF transition per &Qn:.
&Q0 through &Q6	The modem hangs up.

(continued)

Table 9. Summary of AT Modem Initialization Commands *(continued)*

Command	Command Function
&D3	Interpret DTR ON-to-OFF transition per &Qn:.
&Q0, &Q1, &Q4, &Q5, &Q6	The modem performs soft reset.
&Q2, &Q3	The modem hangs up.
&F0	Restore factory configuration 0.
&F1	Restore factory configuration 1.
&G0	Disable guard tone.
&G1	Disable guard tone.
&G2	Enable 1800-Hz guard tone.
&J0	Set S-Register response only for compatibility.
&J1	Set S-Register response only for compatibility.
&K0	Disable DTE/DCE flow control.
&K3	Enable RTS/CTS DTE/DCE flow control.
&K4	Enable XON/XOFF DTE/DCE flow control.
&K5	Enable transparent XON/XOFF flow control.
&K6	Enable both RTS/CTS and XON/XOFF flow control.
&L0	Select dial-up line operation.
&M0	Select direct asynchronous mode.
&M1	Select sync connect with async off-line command mode. *
&M2	Select sync connect with async off-line command mode and enable DTR dialing of directory zero. *
&M3	Select sync connect with async off-line command mode and enable DTR to act asTalk/Data switch.
&P0	Set 10 p/s pulse dial with 39%/61% make/break.
&P1	Set 10 p/s pulse dial with 33%/67% make/break.
&P2	Set 20 p/s pulse dial with 39%/61% make/break.
&P3	Set 20 p/s pulse dial with 33%/67% make/break.
&Q0	Select direct asynchronous mode.
&Q1	Select sync connect with async off-line command mode. *
&Q2	Select sync connect with async off-line command mode and enable DTR dialing of directory zero. *

(continued)

Table 9. Summary of AT Modem Initialization Commands *(continued)*

Command	Command Function
&Q3	Select sync connect with async off-line command mode and enable DTR to act asTalk/Data switch. *
&Q4	Select Hayes AutoSync mode.
&Q5	Modem negotiates an error corrected link.
&Q6	Select asynchronous operation in normal mode.
&R0	CTS tracks RTS (async) or acts per V.25 (sync).
&R1	CTS is always active.
&S0	DSR is always active.
&S1	DSR acts per V.25.
&T0	Terminate any test in progress.
&T1	Initiate local analog loopback.
&T2	Returns ERROR result code.
&T3	Initiate local digital loopback.
&T4	Allow remote digital loopback.
&T5	Disallow remote digital loopback request.
&T6	Request an RDL without self-test.
&T7	Request an RDL with self-test.
&T8	Initiate local analog loop with self-test.
&V	Display current configurations.
&W0	Store the active profile in NVRAM profile 0.
&W1	Store the active profile in NVRAM profile 1.
&X0	Select internal timing for the transmit clock.
&X1	Select external timing for the transmit clock.
&X2	Select slave receive timing for the transmit clock.
&Y0	Recall stored profile 0 upon power up.
&Y1	Recall stored profile 1 upon power up.
&Zn=x	Store dial string x (to 34) to location n (0 to 3).
%E0	Disable line quality monitor and auto retrain.
%E1	Enable line quality monitor and auto retrain.
%E2	Enable line quality monitor and fallback/fall forward.

(continued)

Table 9. Summary of AT Modem Initialization Commands *(continued)*

Command	Command Function
%L	Return received line signal level.
%Q	Report the line signal quality.
+MS	Select modulation.
+H0	Disable RPI.
+H1	Enable RPI and set DTE speed to 19200 b/s.
+H2	Enable RPI and set DTE speed to 38400 b/s.
+H3	Enable RPI and set DTE speed to 57600 b/s.
+H11	Enable RPI+ mode.
-SDR=0	Disable Distinctive Ring.
-SDR=1	Enable Distinctive Ring Type 1.
-SDR=2	Enable Distinctive Ring Type 2.
-SDR=3	Enable Distinctive Ring Type 1 and 2.
-SDR=4	Enable Distinctive Ring Type 3.
-SDR=5	Enable Distinctive Ring Type 1 and 3.
-SDR=6	Enable Distinctive Ring Type 2 and 3.
-SDR=7	Enable Distinctive Ring Type 1, 2, and 3.
-SSE=0	Disable DSVD.
-SSE=1	Enable DSVD.

*. Serial interface operation only.

Resetting the V.34 Modem Configuration

If you encounter problems with the operation of a V.34 modem, you can reset the modem parameters to line driver defaults.



Caution: Resetting the modem configuration clears the dial phone number and disables any user-defined modem initialization string.

To reset the modem configuration:

1. Click on the COM connector for the V.34 Modem adapter module.

2. **Click on Edit Modem.**

The Edit V.34 Modem Interface window appears (refer to [Figure 10](#)).

3. **Click on Reset Cfg.**

The router and modem hardware remain unchanged, but the modem reinitializes with the following AT command string:

AT&M2&Q2&D0&S1&R0S0=0M1L2T

Configuring Routers

The following section is an amendment to *Configuring Routers*.

Configuring the BayStack ARN

The steps for using Site Manager to create an ARN configuration file are slightly different from those described for other routers in the *Configuring Routers* guide. This section provides information on

- [Selecting the Base ARN Configuration](#)
- [Configuring ARN Interfaces](#)
- [Customizing the ARN Service Console](#)

Refer to [Figure 11](#), and to Tables [10](#) and [11](#), to determine the Site Manager connector names for your ARN interfaces.

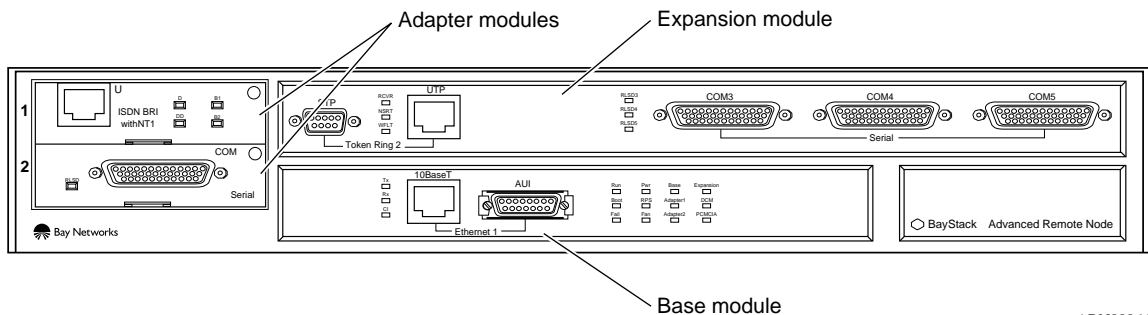


Figure 11. ARN Module Locations

[Table 10](#) lists the Configuration Manager names for ARN adapter modules. [Table 11](#) indicates how the physical interface labels on ARN expansion modules correspond to connector names in the Configuration Manager window.

Table 10. Site Manager Names for ARN Adapter Module Interfaces

Adapter Module Label	Site Manager Connector Name	
	Module Location 1	Module Location 2
DSUCSU	COM1	COM2
ISDN BRI U	ISDN1	ISDN2
ISDN BRI S/T	ISDN1	ISDN2
V.34	COM1	COM2
Serial	COM1	COM2

Table 11. Site Manager Names for ARN Expansion Module Interfaces

Expansion Module Label	Site Manager Connector Name
AUI	XCVR2
10Base-T	XCVR2
UTP	TOKEN2
STP	TOKEN2
COM3	COM3*
COM4	COM4*
COM5	COM5*

*. Site Manager numbers the ARN COM interfaces exactly as they are labeled. If there are no adapter modules installed in COM1 or COM2, COM3 through COM5 could be the first three serial ports in the ARN.

Selecting the Base ARN Configuration

To create a Site Manager configuration file for the ARN in local mode:

- 1. Select the Configuration Manager from the Tools menu by entering a local file name.**

The Select Router Model window appears.

2. Select Advanced Remote Node ([Figure 12](#)).

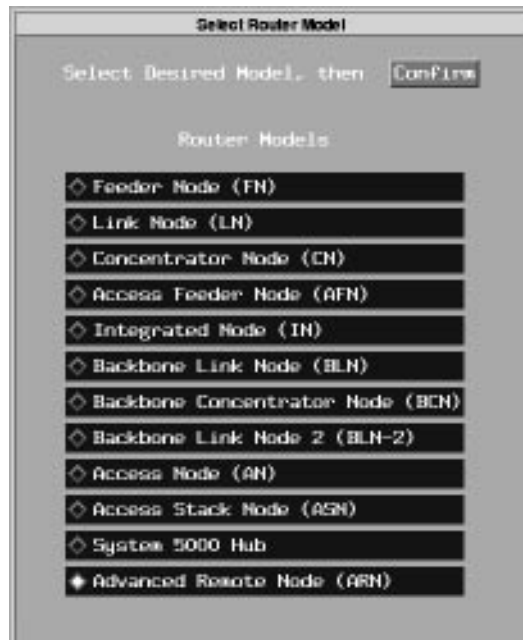


Figure 12. Selecting the ARN Router Model

A blank Configuration Manager screen for the ARN appears ([Figure 13](#)).

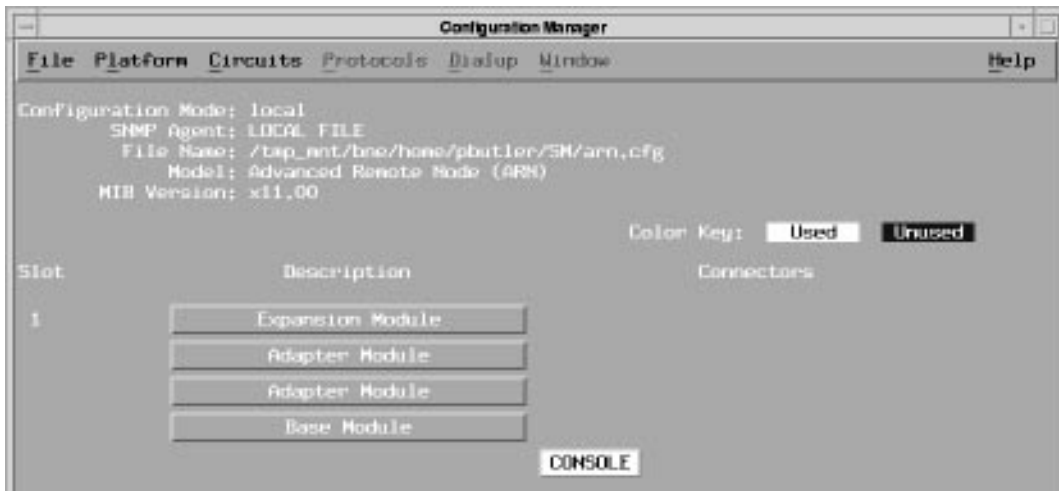


Figure 13. Blank ARN Configuration Manager Window

3. Click on Base Module in the Configuration Manager window.

The Module List for the ARN appears ([Figure 14](#)).

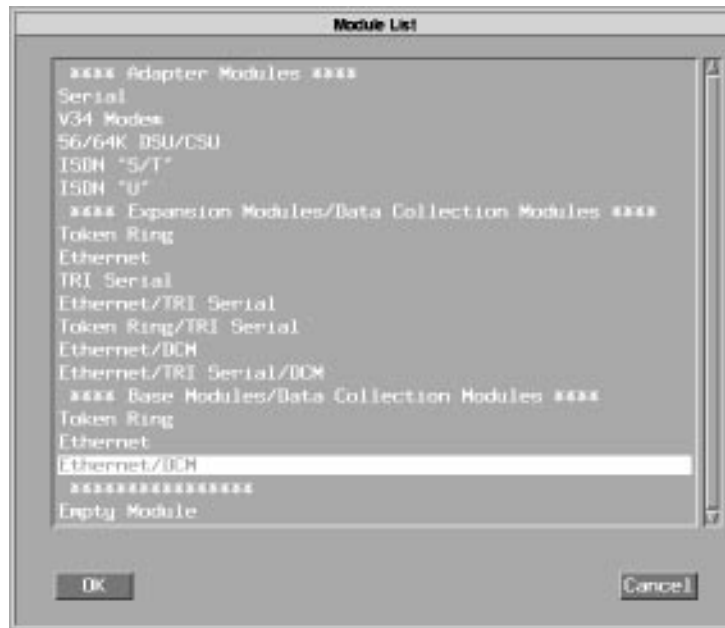


Figure 14. Selecting an ARN Base Module

4. **Select the base module configuration from the Base Modules/Data Collection Modules list.**

Refer to [Figure 11](#) for the physical location of the base module. If the ARN base module contains an installed DCM, select Ethernet/DCM.

5. **Click on OK.**

The Configuration Manager window appears, now displaying the interfaces for the base module selected.

6. **If the ARN contains no expansion or adapter modules, configure the base module interfaces next.**

Skip to “Configuring ARN Interfaces,” later in this section.

7. **If the ARN contains only an expansion module, skip to Step [13](#).**

8. **If the ARN contains a WAN adapter module installed in a front panel slot, click on Adapter Module in the Configuration Manager window.**

The Module List appears ([Figure 15](#)).

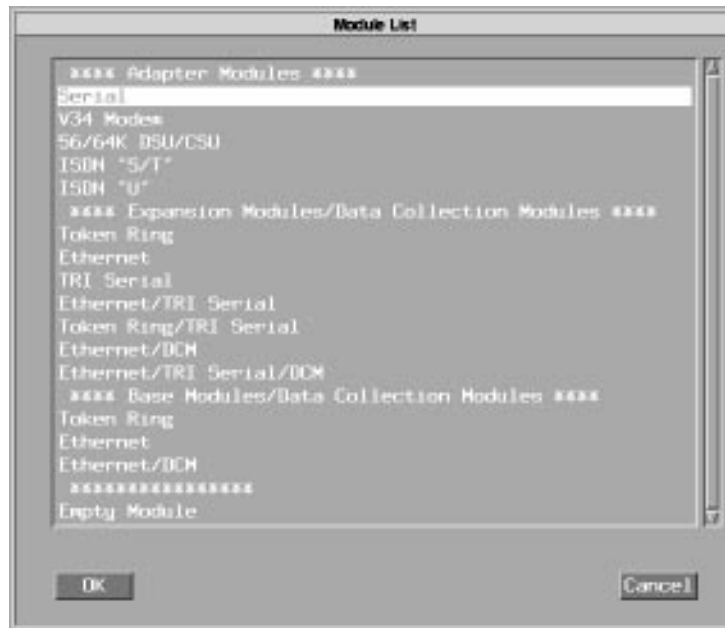


Figure 15. Selecting an ARN Adapter Module

- 9. Select the WAN module type from the Adapter Modules list at the top of the window.**

Refer to [Figure 11](#) for the physical location of adapter modules.

The Configuration Manager window appears, now displaying an interface for the selected adapter module.

- 10. To select a second WAN adapter module, repeat Steps [8](#) and [9](#).**
- 11. If the ARN contains no expansion module, configure the ARN module interfaces next.**

Skip to “Configuring ARN Interfaces,” later in this section.

- 12. Click on Expansion Module in the Configuration Manager window.**

The Module List appears ([Figure 16](#)).

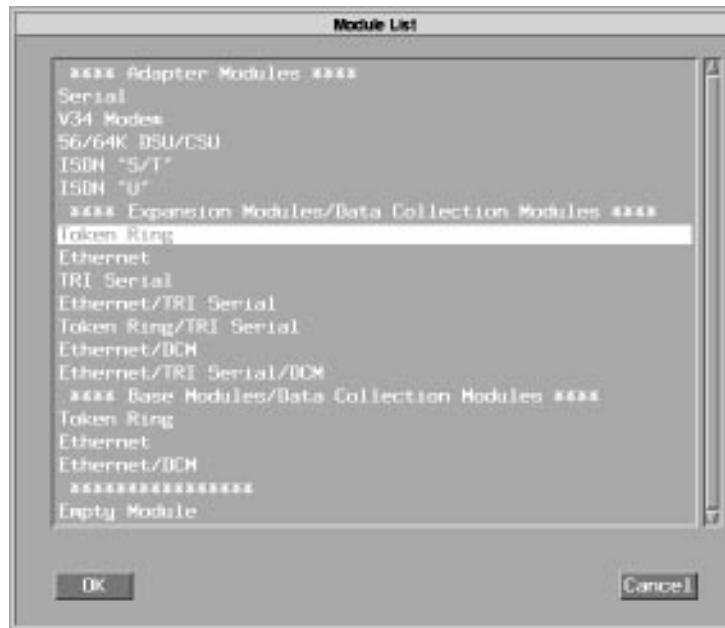


Figure 16. Selecting an ARN Expansion Module

13. Select the expansion module type from the Expansion Modules/Data Collection Modules list.

Refer to [Figure 11](#) for the physical location of expansion modules.

14. Click on OK.

The Configuration Manager window appears, now displaying the expansion module interfaces. [Figure 17](#) shows the interfaces for a sample configuration.



Figure 17. Sample ARN Configuration

Configuring ARN Interfaces

Once you select the ARN modules, configure the interfaces in each module. For information on using Site Manager to configure ARN interfaces:

ARN Interface Type	Find Information Here
Ethernet, Token Ring, Serial	The <i>Configuring Routers</i> and <i>Configuring Line Services</i> guides, or the online help text.
DSU/CSU	"Configuring a DSU/CSU Interface," later in this document.
ISDN	The <i>Configuring Routers</i> and <i>Configuring Dial Services</i> guides, or the online help text. Note that the section on ISDN BRI services for AN, ANH, and ASN routers in <i>Configuring Dial Services</i> also applies to the ARN.
V.34 Modem	"Configuring a V.34 Modem Interface," later in this document.

Refer to *Installing and Operating BayStack ARN Routers* or to *Configuring Remote Access* for instructions on using the **inst_arn.bat** Technician Interface script to configure ARN interfaces.

Customizing the ARN Service Console

For a service console, the ARN supports an ASCII-based or PC software-emulated terminal, an asynchronous modem, or an optional integrated V.34 modem.



Note: When the V.34 console modem is installed in the ARN, the serial modem port is disabled.

Refer to *Installing and Operating BayStack ARN Routers* for information about cabling a service console device and configuring a serial terminal or modem.

Refer to *Configuring Routers* for information about customizing the Site Manager Console parameters that are accessible from the Configuration Manager window (refer to [Figure 17](#)).

Refer to the next section to change the default modem initialization string for a V.34 Console Modem.

Customizing the V.34 Console Modem Initialization String

The integrated V.34 modem is set to operate as a remote console using a factory default configuration. Bay Networks recommends using the factory default modem configuration.

The modem defaults are set by the following factory default AT command initialization string:

ATT&d0&k4&X0S0=2S2=43

[Table 12](#) lists the default settings for the V.34 console modem.

Table 12. V.34 Console Modem Defaults

Modem Signal/Parameter	Value
Clear To Send (CTS)	On
Data Terminal Ready (DTR)	Set to answer all incoming calls.
Data Carrier Detect (DCD) or RLSD	On while carrier is present (the ARN uses DCD to detect modem connect and disconnect).
Data Set Ready (DSR)	On
Ready to Send (RTS)	Ignored
Synchronous/Asynchronous Mode	Asynchronous
AutoAnswer	Answer on 2 rings with DTR active.
Local Character Echo	Off
Supervisory Functions	Off
Baud Rate	9600
Data Bits	8
Stop Bits	1
Parity	None

To change the default modem initialization string for a V.34 Console Modem:

1. From the Configuration Manager, select Platform > V34 Modem.

The Configuration Manager displays the following warning message about editing the AT modem initialization string.



2. Read the message and click on OK.

The Configure Console V.34 Modem window appears [\(Figure 18\)](#).



Figure 18. Configure Console V.34 Modem Window

3. Set the Modem Factory Defaults parameter to Disable.
4. Enter a standard AT command string in the Modem Config String field.



Caution: Entering an invalid command string could disable the modem. Site Manager can verify AT command string changes only when in dynamic mode.

Refer to [Table 9](#) for a summary of AT modem initialization commands.

5. Click on OK.

Configuring Traffic Filters and Protocol Prioritization

The following sections are new in *Configuring Traffic Filters and Protocol Prioritization*:

- [Number of Traffic Filter Rules](#)
- [New Criteria](#)

Number of Traffic Filter Rules

Site Manager now supports up to 127 traffic filter rules on each IP interface. Earlier software versions support a maximum of 31 IP traffic filter rules per interface.

New Criteria

You filter IP traffic based on specified bit patterns contained in the IP header or in the header of the upper-level protocol carried within the IP datagram (TCP or UDP, for example).

In addition to the criteria described in *Configuring Traffic Filters and Protocol Priorization*, Site Manager supports new predefined criterion options ([Table 13](#)).

Table 13. New Predefined Criteria for IP Traffic Filters

Criterion Name	Reference Field	Offset	Length	Description
IP source and destination address	HEADER_START (0)	96	64	Allows filtering on both IP Source and IP Destination fields using only one filter rule.
UDP or TCP source port	HEADER_END (1)	0	16	Allows filtering on either TCP or UDP packets by specifying TCP or UDP source port numbers.
UDP or TCP destination port	HEADER_END (1)	16	16	Allows filtering on either TCP or UDP packets by specifying TCP or UDP destination port numbers.
Established TCP	HEADER_END (1)	107	3	Allows filtering on the ACK and RESET bits within the TCP HEADER by providing predefined ranges. You do not enter a filter range.

Event Messages for Routers and BNX Platforms

[Table 14](#) lists the service and entity names that correspond to the new or amended sections to *Event Messages for Routers and BNX Platforms*:

Table 14. New and Amended Event Messages

Service	Entity	Section	Page
Data Link Switching	DLS	DLS Warning Events DLS Trace Events	-73 -73
DSU/CSU	DSUCSU	DSUCSU Fault Event DSUCSU Info Events	-75 -75
Fujitsu Network Transmission Systems ATM	FNTS_ATM	FNTS_ATM Fault Event FNTS_ATM Warning Events FNTS_ATM Info Events	-77 -77 -79
Frame Relay	FR	FR Event	-81
Data Encryption - Key Manager - WAN Encryption Protocol	KEYMGR WEP	KEYMGR Fault Event KEYMGR Warning Events KEYMGR Info Events WEP Fault Event WEP Warning Events WEP Info Events	-81 -82 -82 -89 -89 -91
V.34 Modem service	MODEM	MODEM Fault Events MODEM Warning Events MODEM Info Events	-83 -83 -84
Point-to-Point	PPP	PPP Info Events PPP Trace Events	-85 -86
X.25/QLLC	QLLC	QLLC Fault Event	-86
Switched Services (Dial-on-Demand, Dial Backup and Bandwidth-on-Demand)	SWSERV	SWSERV Info Events	-87
Technician Interface	TI	Technician Interface Info Event Messages	-88
Teletype	TTY	TTY Info Event Message	-89

DLS Warning Events

The following is a new Fault event message for the Data Link Switching (DLSw) service, referred to as the DLS entity. The entity code assigned to DLS events is 50.

Entity Code/Event Code **50/57**

Decimal Identifier **16790073**

Severity: Warning

Message: Received ALERT indication from SDLC, <alert>, port = <port no.>, ls_ref = <link station>

Meaning: An alert was received from an SDLC link station. The alert can be Link Failed, Port Failed, or Info Only.

DLS Trace Events

The following are new Warning event messages for the Data Link Switching (DLSw) service, referred to as the DLS entity. The entity code assigned to DLS events is 50.

Entity Code/Event Code **50/98**

Decimal Identifier **16790114**

Severity: Trace

Message: Peer <ip_address> type is <type>.

Meaning: Indicates the DLSw Peer IP address and the type of connection; either RFC 1434 or RFC 1795.

Entity Code/Event Code **50/99**

Decimal Identifier **16790115**

Severity: Trace

Message: Received LLC <name> frame: dmac = <address>, smac = <address> saps = <service access points>

Meaning: Indicates that an LLC Command (UI) type frame was received. The event indicates the associated destination and source MAC addresses and service access points (SAPs).

Entity Code/Event Code **50/100**

Decimal Identifier **16790116**

Severity: Trace

Message: Received SSP *<name>* frame: tmac = *<address>*, omac = *<address>* saps = *<service access points>*

Meaning: Indicates the received DLSw Switch-to-Switch Protocol (SSP) frame type with the target and origin MAC addresses and SAPs.

Entity Code/Event Code **50/101**

Decimal Identifier **16790117**

Severity: Trace

Message: Received SSP *<name>* frame: data link correlator = *<connection address>*

Meaning: Indicates the received DLSw SSP frame type and the connection address.

Entity Code/Event Code **50/102**

Decimal Identifier **16790118**

Severity: Trace

Message: State change in *<name>*: connection = *<name>*, old state = *<state>*, new state = *<state>*

Meaning: Indicates that a DLSw state change occurred. The message provides the old and new state. The active subsystem (LLC, SDLC, or NetBIOS) is listed with the address of the changed connection.

Entity Code/Event Code **50/103**

Decimal Identifier **16790119**

Severity: Trace

Message: Sent *<type>* frame: tmac = *<address>*, omac = *<address>*, saps = *<service access points>*

Meaning: Indicates the type of transmitted frame with the associated target and origin MAC addresses and SAPs.

DSUCSU Fault Event

The following is a new Fault event message for the DSU/CSU service, referred to as the DSUCSU entity. The entity code assigned to DSUCSU events is 111.

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.

DSUCSU Info Events

The following are new Info event messages for the DSU/CSU service, referred to as the DSUCSU entity. The entity code assigned to DSUCSU events is 111.

Entity Code/Event Code	111/2
Decimal Identifier	16805634
Severity:	Info
Message:	DSU/CSU initialization started on Slot< <i>slot no.</i> > COM< <i>connector_no.</i> >
Meaning:	The router began driver initialization on the DSU/CSU module in the connector indicated (Slot 1; COM1, COM2, or COM3).

Entity Code/Event Code	111/3
Decimal Identifier	16805635
Severity:	Info
Message:	DSU/CSU initialization completed on Slot< <i>slot no.</i> > COM< <i>connector_no.</i> >
Meaning:	The router completed driver initialization on the DSU/CSU module in the connector indicated (Slot 1; COM1, COM2, or COM3).

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 connector indicated (Slot 1; COM1, COM2, or COM3). The DSU/CSU loopback states are

- Local Analog Loopback
- Local Digital Loopback
- Local Analog Loopback with Pattern
- Remote Digital Loopback
- Remote Digital Loopback with Pattern
- Pattern (2047) Generator

Entity Code/Event Code **111/5**
Decimal Identifier **16805637**

Severity: Info

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

Meaning: The router terminated loopback operation on the DSU/CSU module in the connector indicated (Slot 1; COM1, COM2, or COM3). The DSU/CSU loopback states reported are

- Local Analog Loopback
- Local Digital Loopback
- Remote Digital Loopback
- Pattern (2047) Generator

Entity Code/Event Code **111/6**
Decimal Identifier **16805638**

Severity: Info

Message: <loop_state> completed for without errors on Slot<slot no.> COM<connector_no.>

Meaning: Indicates that a loopback test completed without errors on the DSU/CSU module in the connector indicated (Slot 1; COM1, COM2, or COM3). The DSU/CSU loopback test states reported are

- Local Analog Loopback with Pattern
- Remote Digital Loopback with Pattern

Entity Code/Event Code **111/7**
Decimal Identifier **16805639**

Severity: Info

Message: <loop_state> completed with <number_of_errors> errors on Slot<slot no.>
COM<connector_no.>

Meaning: Indicates that a loopback test on the DSU/CSU module in the connector indicated (Slot 1; COM1, COM2, or COM3) failed, and indicates the number of errors reported during the test. The DSU/CSU loopback test states reported are

- Local Analog Loopback with Pattern
- Remote Digital Loopback with Pattern

FNTS_ATM Fault Event

The following are new Fault event messages for the Fujitsu Network Transmission Systems ATM service, referred to as the FNTS_ATM entity. The entity code assigned to FNTS_ATM events is 116.

Entity Code/Event Code **116/1**
Decimal Identifier **16806913**

Severity: Fault

Message: Service error, service attempting restart.

Meaning: The ATM driver experienced a fatal error and is restarting automatically. The driver attempts to restart up to five times.

Action: Contact the Bay Networks Technical Response Center if this condition persists.

FNTS_ATM Warning Events

The following are new Warning event messages for the Fujitsu Network Transmission Systems ATM service, referred to as the FNTS_ATM entity. The entity code assigned to FNTS_ATM events is 116.

Entity Code/Event Code **116/3**
Decimal Identifier **16806915**

Severity: Warning

Message: Connector <connector_no.> out of range.

Meaning: The connector configuration is invalid.

Action: Modify the configuration file to accurately describe the module and connector.

Entity Code/Event Code **116/5**
Decimal Identifier **16806917**

Severity: Warning

Message: Incorrect router type for the FNTS_ATM driver.

Meaning: The driver was loaded on a non-FNTS router. You cannot use the FNTS_ATM driver on any but the FNTS Integrated Node.

Action: Loading the FNTS driver on a non-FNTS router does not affect the performance of the device. However, we recommend that you use this driver only on FNTS Integrated Nodes. If this message appears when you load the FNTS_ATM driver on an FNTS Integrated Node, contact the Bay Networks Technical Response Center.

Entity Code/Event Code **116/6**
Decimal Identifier **16806918**

Severity: Warning

Message: Failure binding to the ATM-DXI interface record.

Meaning: The ATM_FNTS driver could not locate the ATM-DXI MIB record.

Action: Contact the Bay Networks Technical Response Center.

Entity Code/Event Code **116/7**
Decimal Identifier **16806919**

Severity: Warning

Message: Connector <connector_no.>, gate id <gate_id>, could not get a buffer.

Meaning: The specified connector could not obtain a buffer while sending a message to the module driver using the specified gate id.

Action: Contact the Bay Networks Technical Response Center.

Entity Code/Event Code **116/8**
Decimal Identifier **16806920**

Severity: Warning

Message: Connector <connector_no.>, gate id <gate_id>, encountered an RPC timeout.

Meaning: The specified connector encountered a remote procedure call (RPC) timeout while sending a message to the module driver using the specified gate id. This means that the connector could not communicate with the module driver.

Action: Contact the Bay Networks Technical Response Center.

Entity Code/Event Code **116/9**
Decimal Identifier **16806921**
Severity: Warning
Message: Connector <connector_no.>, invalid mode 1a.
Meaning: The FNTS_ATM driver uses ATM DXI Mode 2 encapsulation.
Action: Reconfigure the connector to use ATM DXI Mode 2 encapsulation.

Entity Code/Event Code **116/10**
Decimal Identifier **16806922**
Severity: Warning
Message: Connector <connector_no.>, invalid mode 1b.
Meaning: The FNTS_ATM driver operates only in ATM DXI Mode 2.
Action: Reconfigure the connector to operate in ATM DXI Mode 2.

Entity Code/Event Code **116/11**
Decimal Identifier **16806923**
Severity: Warning
Message: Connector <connector_no.>, ATM IP Address: <IP_address>.
Meaning: The IP address of the ATM adapter has changed.

FNTS_ATM Info Events

The following are new Info event messages for the Fujitsu Network Transmission Systems ATM service, referred to as the FNTS_ATM entity. The entity code assigned to FNTS_ATM events is 116.

Entity Code/Event Code **116/12**
Decimal Identifier **16806924**
Severity: Info
Message: Service initializing.
Meaning: ATM service is initialization.

Entity Code/Event Code **116/13**
Decimal Identifier **16806925**

Severity: Info
Message: Connector <connector_no.> disabled.
Meaning: The specified connector is disabled.

Entity Code/Event Code **116/14**
Decimal Identifier **16806926**

Severity: Info
Message: Connector <connector_no.> enabled.
Meaning: The specified connector is enabled.

Entity Code/Event Code **116/15**
Decimal Identifier **16806927**

Severity: Info
Message: Connector <connector_no.> configuration deleted.
Meaning: The record for the specified connection is no longer part of the configuration.

Entity Code/Event Code **116/16**
Decimal Identifier **16806928**

Severity: Info
Message: Connector <connector_no.> providing LLC1 service.
Meaning: The connector is running logical link control version 1 (LLC1) service. LLC1 is a connectionless datagram service. The connector provides this service following the proper initialization of the driver.

Entity Code/Event Code **116/17**
Decimal Identifier **16806929**

Severity: Info
Message: Connector <connector_no.> LLC1 service withdrawn.
Meaning: The connector is no longer running logical link control version 1 (LLC1) service. This service is withdrawn when the driver is not operating.

Entity Code/Event Code	116/18
Decimal Identifier	16806930
Severity:	Info
Message:	Connector <connector_no.>, valid mode 2.
Meaning:	The connector is running ATM DXI Mode 2 encapsulation.

FR Event

The following is a new Fault event message for the Frame Relay service, referred to as the FR entity. The entity code assigned to FR events is 25.

Entity Code/Event Code	25/133
Decimal Identifier	16783749
Severity:	Warning
Message:	Line <line_number> <low_level_index>: VC <VC_number> has circuit of 0, setting to <value>.
Meaning:	The software has assigned a value of <value>, which is the circuit of the default service record, to the specified VC. On a multislot router, when you learn VCs dynamically, change them, and save the configuration file, the software may assign the default service record to the VC circuit number when you reboot the router.
Action:	Reset the circuit number for this VC to the correct value, and save the configuration file.

KEYMGR Fault Event

The following is a new Fault event message for the Key Manager service, referred to as the KEYMGR entity. The entity code assigned to KEYMGR events is 118.

Entity Code/Event Code	118/1
Decimal Identifier	16807425
Severity:	Fault
Message:	System error, service attempting restart.
Meaning:	The router experienced a fatal error and is restarting automatically. The router will attempt to restart up to five times.
Action:	Verify that the configuration is correct. Call the Bay Networks Technical Response Center if the router fails to restart.

KEYMGR Warning Events

The following are new Warning event messages for the Key Manager service, referred to as the KEYMGR entity. The entity code assigned to KEYMGR events is 118.

Entity Code/Event Code **118/4**

Decimal Identifier **16807428**

Severity: Warning

Message: NPK exists; config missing NPK hash.

Meaning: The encryption configuration is incomplete. The **kset NPK** command has been executed, but the parameters have not been set.

Action: If you want to use encryption, configure all parameters.

Entity Code/Event Code **118/5**

Decimal Identifier **16807429**

Severity: Warning

Message: Hash of NPK doesn't match config's NPK hash.

Meaning: The NPK on the router does not match the NPK in the MIB.

Action: Use the **kset NPK** command to change the NPK on the router, or use the **ktranslate** command to change the NPK value in the MIB. Refer to *Configuring Encryption Services* for instructions.

Entity Code/Event Code **118/6**

Decimal Identifier **16807430**

Severity: Warning

Message: Config has NPK hash; NPK is missing.

Meaning: The NPK is in the MIB, but not on the router.

Action: Enter the NPK on the router.

KEYMGR Info Events

The following are new Fault event messages for the Key Manager service, referred to as the KEYMGR entity. The entity code assigned to KEYMGR events is 118.

Entity Code/Event Code **118/2**
Decimal Identifier **16807426**
Severity: Info
Message: KEYMGR checks starting.
Meaning: The Key Manager is initializing.

Entity Code/Event Code **118/3**
Decimal Identifier **16807427**
Severity: Info
Message: KEYMGR checks completed.
Meaning: The Key Manager is active.

MODEM Fault Events

The following is a new Fault event message for the Modem service, referred to as the MODEM entity. The entity code assigned to MODEM events is 110.

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.

MODEM Warning Events

The following are new Warning event messages for the Modem service, referred to as the MODEM entity. The entity code assigned to MODEM events is 110.

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.

MODEM Info Events

The following are new Info event messages for the Modem service, referred to as the MODEM entity. The entity code assigned to MODEM events is 110.

Entity Code/Event Code **110/3**
Decimal Identifier **16805379**

Severity: Info

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

Meaning: The router began driver initialization on the modem module in the connector indicated (Slot 1; COM1 or COM2).

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 connector 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,” earlier in this document). Call the Bay Networks Technical Response Center if the modem fails to initialize on restart.

PPP Info Events

The following are new Info event messages for the Point-to-Point Protocol service, referred to as the PPP entity. The entity code assigned to PPP events is 44.

Entity Code/Event Code **44/207**
Decimal Identifier **16788687**

Severity: Info

Message: Callback Client Delay expired circuit: <circuit_no.>, freeing buffers

Meaning: The time that the client waits for a return call from the server has expired. The client will discard the contents of the buffers and resume placing outgoing calls when new data arrives.

Entity Code/Event Code **44/208**
Decimal Identifier **16788688**

Severity: Info

Message: Callback Server Delay expired circuit: <ircuit_no.>, attempting Callback

Meaning: The time the server waits to call the client back has expired. The server will now call back the client.

Entity Code/Event Code **44/209**
Decimal Identifier **16788689**

Severity: Info

Message: Received ANI station_num:<phone_no.> sub_addr:<address> from LM

Meaning: The router has received the phone number and subaddress from the Line Manager using caller ID.

PPP Trace Events

The following are new Trace event messages for the Point-to-Point Protocol service, referred to as the PPP entity. The entity code assigned to PPP events is 44.

Entity Code/Event Code **44/212**
Decimal Identifier **16788692**

Severity: Trace

Message: <protocol> Naking <option> option <option_value> sub-option <suboption_value> with option <option_value> sub-option <suggested_suboption_value> on line <line_no.>:, circuit <circuit_no.>.

Meaning: The router received a protocol packet that contained a protocol option and suboption. The router accepted the option but not the suboption. As a result, the router returned a configure negative acknowledgment (NAK) packet containing a suggested value for the suboption.

QLLC Fault Event

The following is a new Fault event message for the X.25/QLLC service, referred to as the QLLC entity. The entity code assigned to QLLC events is 120.

Entity Code/Event Code **120/1**
Decimal Identifier **16807937**

Severity: Fault

Message: QLLC System error, service attempting restart.

Meaning: The router experienced a fatal error and is restarting automatically. The router will attempt to restart up to five times.

Action: Verify that the configuration is correct. Call the Bay Networks Technical Response Center if the router fails to restart.

SWSERV Info Events

The following are new Info event messages for the SWSERV entity. The entity code assigned to SWSERV events is 58.

Entity Code/Event Code **58/161**
Decimal Identifier **16792225**

Severity: Info

Message: Resolved wfSwservInPhone NumCct to circuit <*circuit_no.*>

Meaning: The router determined the circuit number requesting a callback by matching the incoming phone number with the numbers in the incoming phone list.

Entity Code/Event Code **58/162**
Decimal Identifier **16792226**

Severity: Info

Message: Signaling PPP to initiate Callback

Meaning: The circuit is configured for callback and the server notifies PPP to call back the client.

Technician Interface Info Event Messages

The following are new Info event messages for the Technician Interface service, referred to as the TI entity. The entity code assigned to TI events is 0.

Entity Code/Event Code **0/55**

Decimal Identifier **16777271**

Severity: Info

Message: User <*user_ID*> logged in successfully on port <*port_no.*>.

Meaning: The designated user (User|Manager) logged into the Secure Shell successfully on the designated serial port.

Entity Code/Event Code **0/56**

Decimal Identifier **16777272**

Severity: Info

Message: User <*user_ID*> logged out from port <*port_no.*>.

Meaning: The designated user (User|Manager) logged out of the Secure Shell on the designated serial port.

Entity Code/Event Code **0/57**

Decimal Identifier **16777273**

Severity: Info

Message: User <*user_ID*> logged out (via timeout) from port <*port_no.*>.

Meaning: The designated user (User|Manager) was logged out automatically by the system due to an inactivity timeout on the designated serial port.

TTY Info Event Message

The following is a new Info event message for the Teletype service, referred to as the TTY entity. The entity code assigned to TTY events is 17.

Entity Code/Event Code **17/15**

Decimal Identifier **16781583**

Severity: Info

Message: Modem initialization failed in the <state> state <state_no.> on port <port_no.>

Meaning: The modem on the designated port failed in one of the following states while attempting to initialize:

- START_UP
- GET_INFO
- AT_DEFAULT
- AT_INIT

WEP Fault Event

The following is a new Fault event for the WAN Encryption Protocol service, referred to as the WEP entity. The entity code assigned to WEP events is 117.

Entity Code/Event Code **117/1**

Decimal Identifier **16807169**

Severity: Fault

Message: System error, service attempting restart.

Meaning: The router experienced a fatal error and is restarting automatically. The router will attempt to restart up to five times.

Action: Verify that the configuration is correct. Call the Bay Networks Technical Response Center if the router fails to restart.

WEP Warning Events

The following are new Warning events for the WAN Encryption Protocol service, referred to as the WEP entity. The entity code assigned to WEP events is 117.

Entity Code/Event Code **117/2**
Decimal Identifier **16807170**

Severity: Warning
Message: Unable to allocate WEP VC. Maximum number of VCs reached.
Meaning: The maximum number of VCs allowed, 1024, are already configured for encryption. The circuit just configured cannot use encryption.
Action: If you want to use encryption on this VC, you must delete encryption from at least one other VC.

Entity Code/Event Code **117/3**
Decimal Identifier **16807171**

Severity: Warning
Message: Maximum number of wfWepCircuitEntry reached. Ignoring entry.
Meaning: The maximum number of circuits allowed, 1024, are already configured for encryption. The circuit just configured cannot use encryption.
Action: If you want to use encryption on this circuit, you must delete encryption from at least one other circuit.

Entity Code/Event Code **117/4**
Decimal Identifier **16807172**

Severity: Warning
Message: Invalid encryption mode. Service disabled.
Meaning: The Cipher Mode Mask parameter is set to a value that your system does not support.
Action: Check your configuration and reset the Cipher Mode Mask parameter.

Entity Code/Event Code **117/9**
Decimal Identifier **16807177**

Severity: Warning
Message: Error in LTSS decryption.
Meaning: Either the MIB is corrupted, or the NPK in the MIB and in the router do not match.
Action: Delete the circuit, recreate it, and reconfigure encryption.

Entity Code/Event Code **117/10**
Decimal Identifier **16807178**

Severity: Warning
Message: Error in LTSS authentication.
Meaning: Either the MIB is corrupted, or the NPK in the MIB and in the router do not match.
Action: Delete the circuit, recreate it, and reconfigure encryption

Entity Code/Event Code **117/11**
Decimal Identifier **16807179**

Severity: Warning
Message: Engine Registration failed for line <*line number*>, encryption down on this line.
Meaning: A system error has occurred while initializing encryption on the specified line. The system will retry up to five times.
Action: If the router does not successfully start encryption, reboot.

Entity Code/Event Code **117/12**
Decimal Identifier **16807180**

Severity: Warning
Message: Engine Change failed for line <*line number*>, encryption down on this line.
Meaning: A system error has occurred on the specified line. The system will retry up to five times.
Action: If the retry is not successful, reboot the router.

WEP Info Events

The following are new Info events for the WAN Encryption Protocol service, referred to as the WEP entity. The entity code assigned to WEP events is 117.

Entity Code/Event Code **117/13**
Decimal Identifier **16807181**

Severity: Info
Message: Service initializing.
Meaning: Encryption is initializing.

Entity Code/Event Code **117/14**
Decimal Identifier **16807182**

Severity: Info
Message: Export 40-bit version.
Meaning: The system is using 40-bit encryption.

Entity Code/Event Code **117/15**
Decimal Identifier **16807183**

Severity: Info
Message: Not-for-export 56-bit version.
Meaning: The system is using 56-bit encryption.

Entity Code/Event Code **117/16**
Decimal Identifier **16807184**

Severity: Info
Message: Service is up.
Meaning: Encryption is running.

Entity Code/Event Code **117/19**
Decimal Identifier **16807187**

Severity: Info
Message: Attempt to connect line <line number>, circuit <circuit number>, vcid <VC number> has
 timed out.
Meaning: The attempt to connect to the VC has timed out.

Quick-Starting Routers and BNX Platforms

When configuring RIP on an interface, you must now specify the version of RIP that you are running. You can choose from the following options:

RIP1 (default)	RIP version 1
RIP2	RIP version 2 without the aggregation of subnets that RIP1 provides
RIP2_AGGR	RIP version 2 with automatic aggregation of subnets

Upgrading Routers from Version 7-10.xx to Version 11.0

The following sections are amendments to *Upgrading Routers from Version 7-10.xx to Version 11.0*:

- [Technician Interface dcmload Script](#)
- [BOOT and Diagnostic PROM Upgrades for 11.01](#)

Technician Interface dcmload Script

The **dcmload** command upgrades the software image for an Ethernet Data Collection Module (DCM) installed in a BayStack AN, ANH, or ARN. Use this command to download a new software image from the router Flash memory to the DCM Flash memory.



Caution: Running this script temporarily disables and then reenables the DCM board.

Respond to prompts in the **dcmload** script as follows:

- When prompted for either a base module or expansion module DCM board, select base module (**b**) for AN or ANH routers. Only the ARN has a DCM option for an expansion Ethernet module (**e**).
- When prompted for the image file name, use the form *<volume:filename>*.
- When prompted whether to save the image on the DCM Flash, answer yes (**y**) to overwrite the existing image on the DCM Flash with the new image. Answer no (**n**) to use the downloaded image once, but lose it at the next boot.

Sample Display – dcmload

Use this script to download a DCM image from the router's Flash to a DCM board.

When prompted for the image file name, use the form <volume:filename>.

When prompted whether to save the image on the DCM Flash, answer yes (y) to overwrite the existing image on the DCM Flash with the new image. Answer no (n) to use the downloaded image once, but lose it at the next boot.

Do you want to download an image to the Base Module DCM or the Expansion Module DCM? (b/e)[b]: **b**

Specify DCM image name (volume:filename): **1:in11_140.obj**

Do you want DCM to save this image on its FLASH? (y/n)[y]: **y**

Image Name is 1:in11_140.obj

Image will be saved by DCM in its FLASH

Do you want to start the download process? (y/n)[y]: **y**

Downloading of DCM image has started. It will take few seconds to complete

BOOT and Diagnostic PROM Upgrades for 11.01

[Table 15](#) shows the routers that require a new version of boot and diagnostic PROMs for router software version 11.01. Upgrade the PROMs if the features you need depend on a PROM version more recent than the version now in your router.

Table 15. Boot and Diagnostic PROMs for Router Software Version 11.01

Router Model	Boot PROM Version	Boot PROM File Name	Reason for Upgrading PROM	Diagnostic PROM File Name	Diagnostic PROM Version
AN	9.00	<i>anboot.exe</i>	Upgrade diagnostic PROM to support new serial daughter cards: V34 modem, csudsu, and ISDN/U options	<i>anddiag.exe</i>	V7.24
AN200	11.01	<i>an200boot.exe</i>	New hardware platform support	<i>an200diag.exe</i>	V1.00
ARE	9.01	<i>areboot.ppc</i>	New hardware platform support	<i>arediag.ppc</i>	V1.12
ARN	V1.12	<i>arnboot.exe</i>	Support for ARN platform and miscellaneous bug fixes	<i>arndiag.exe</i>	V1.22
ARN_PDBROM.ROM	-----	-----	Support for PDB diagnostics for the ARN platform	<i>arndiag.exe</i>	V1.13
ASN	10.00	<i>asnboot.exe</i>		<i>asndiag</i>	V2.18
BN	8.10	<i>freboot.exe</i>		<i>frediag.exe</i>	4.10
VME	8.11	<i>vmeboot.exe</i>		None	None
ARE s5000	11.00	<i>s5000boot.exe</i>		<i>S5000diag.exe</i>	V0.04

Using the Bay Command Console

The following sections are amendments to *Using the Bay Command Console*:

- [Errata](#)
- [Using the BCC to Install a BN Router](#)

Errata

This section describes corrections that apply to *Using the Bay Command Console* (part number 115976-A Rev. A).

The following corrections apply to Chapter 1:

- Figure 1-2 shows a “trusted-host” object under global IP access policies. Release 11.01 does not support the trusted-host configuration object.
- In the section “Naming and Numbering Conventions,” three of the attributes in the list for IP on an ethernet interface are not supported in Release 11.01. The attributes are
 - arp-mode
 - arp-server-address
 - arp-server-reg-interval

The following corrections apply to Chapter 2:

- In the sections “Getting Help for Configurable Objects and Attributes” and “Getting Help for Configurable Attribute Values,” the same three ARP attributes not supported in Release 11.01 appear erroneously in the example help listings for IP on an Ethernet interface. The attributes are
 - arp-mode
 - arp-server-address
 - arp-server-reg-interval

- In the section “Getting Root-Level (System) Help,” the following list of configurable objects appear in the example of system-level help you invoke at the `bcc>` prompt:

```
Configurable objects in this context:
    ethernet tokenring sync hssi fddi
    ip snmp ftp tftp telnet ntp
```

The **board** and **console** objects are missing from this list.

- In the sections “Displaying the Total Device Configuration” and “Displaying Binary Configuration Files as BCC Syntax,” slot 7 of the **show config** command output should indicate a board type of 8448 (board-type srl1).
- In the sections “Displaying the Total Device Configuration” and “Displaying Binary Configuration Files as BCC Syntax,” the **show config** examples list three ATM modules in slots 1, 8, and 9, respectively. The BCC in Release 11.01 does not support ATM-related configuration objects.
- In the section “Displaying Binary Configuration Files as BCC Syntax,” the Technician Interface (**tic**) **save** command near the end of that section requires a space between **config** and `<volume>`, as follows:

```
tic save config <volume>:<filename>
```

- In the section “Specifying Multiple Attribute-Value Pairs,” the following BCC prompt is incorrect:

```
ip/1/2/3/4> ospf area 2.3.4.54 hello-interval 5
```

The prompt should be:

```
ip/1.2.3.4> ospf area 2.3.4.54 hello-interval 5
```

- In the section “Command Operators,” the following statement is inaccurate: “Deleting OSPF from the global IP context also deletes any instances of OSPF configured on any interface.” Deleting OSPF from the global IP context does not delete OSPF from any interface.

The following corrections apply to Chapter 3:

- In the opening paragraph of Chapter 3, the following item appears erroneously in the list of bullets describing the chapter contents:
“Assign an alias name to any configured object”

- In step 4 at the opening of the section “Creating a New Configuration,” note that you do not have to explicitly configure TCP as a global/box-wide protocol. The BCC adds TCP automatically when you add the first instance of IP on an interface. Also in step 4: TFTP, NTP, and Telnet client are additional global protocols not enabled automatically when you add interfaces (step 2) in the device configuration sequence.
- In step 7 of the section “Creating a New Configuration,” the “address” attribute is now DERIVED (the BCC supplies a value) rather than REQUIRED (you supply a value).
- In the sections “Creating a New Configuration” and “Modifying an Existing Configuration,” the Technician Interface (**tic**) **save** command near the end of that section requires a space between config and <volume>, as follows:

```
tic save config <volume>:<filename>
```

- Step 1 of the section “Modifying an Existing Configuration” should read as follows:

“Navigate to the context of **ospf** on **ip/1.2.3.4** as follows:

```
bcc> ethernet/2/1;ip/1.2.3.4;ospf area 0.0.0.0
ospf/1.2.3.4>
```

Note that each semicolon (;) serves as a Return in the command line.”

The following corrections apply to Chapter 4:

- Near the end of the example for “Configuring a Token Ring Interface with IP and RIP,” the following comment appears: “You can configure attributes of tokenring/6/1 or add an instance of ip and/or ipx on the interface.” The BCC does not support IPX as a configurable object in Release 11.01.
- In the example for “Configuring OSPF and BGP,” the following attributes are not configurable:

```
-- rs-request
-- rs-topology
-- route-server-cluster
```

The following attributes are not configurable for BGP peers:

```
-- rs-mode
-- rs-identifier
```

These attributes appear as **help** entries in the example.

The “stub” attribute also appearing in this example now has the name “non-stub.”

Finally, the following command line and comment is incorrect, since the BCC does not require you to configure an adjacent host for IP on PPP:

```
ppp/3/3> ip address 192.168.10.1    Add IP (address 192.168.10.1) and an  
adjhost 192.168.10.2                adjacent host (address 192.168.10.2) to  
                                      ppp/3/3.
```

Instead, the command line should read as follows:

```
ppp/3/3> ip address 192.168.10.1    Add IP (address 192.168.10.1) to ppp/3/3.
```

- In the example for “Configuring PPP, IP, and an Adjacent Host (Sync Interface),” the following errors exist:
 - The example should not include the configuration of an adjacent host, since PPP handles this task during line negotiation. Hence, the heading for the example should be “Configuring PPP and IP on a Sync Interface.” In addition, the introductory sentence immediately following the heading should read as follows:

“This brief example configures PPP and IP on a synchronous interface, as follows:”
 - Immediately preceding the command configuring IP on PPP, the following command line and comment appears erroneously:

```
rip/3.3.3.3> sync 3/2      Add to the device configuration a synchronous
                        interface on slot 3, connector 2.
```

- The following command line and comment, which appear midway through this example, are incorrect because you do not explicitly configure an adjacent host for IP on PPP:

```
ppp/3/2> ip address 192.168.4.1  Add IP (address192.168.4.1) and an
adjhost 192.168.4.2             adjacent host (address 192.168.4.2) to
                                ppp/3/2.
```

Instead, the command line should read as follows:

```
ppp/3/2> ip address 192.168.4.1  Add IP (address192.168.4.1) to ppp/3/2.
```

Using the BCC to Install a BN Router

The following example shows a sequence of commands you can use to bring up a BN router on a network. Assumptions for this example are that you first complete physical installation of the router, then boot the router using the image (*bn.exe*) and the minimum configuration file, *ti.cfg*.

The example includes command inputs and outputs resulting from BCC configuration commands, **help** and **info** commands, and **show config** commands. The example also shows where BCC error messages provide extended help information.

Prompts, Commands, and Responses

bcc> **info**

```
type 16896
mib-version 110001
build-location ""Built in ..<location>
build-date ""2.00 (49) Wed Jan 29 18:52:24
EST 1997""
verbose 0
box-type frecn
```

bcc> **show config**

```
box type 16896
board type 80 slot 5
  board-type sync
cwc ..
board type 8448 slot 7
  board-type srml
cwc ..
board type 176 slot 9
  board-type dtok
cwc ..
board type 192 slot 11
  board-type wffddi2m
cwc ..
board type 162 slot 13
  board-type qenf
cwc ..
```

Comments

Check the chassis (box) type.

“frecn” = Bay Networks BCN router

Check the board configuration inside the router.

- Quad Synchronous link module in slot 5
- System Resource Module in slot 7
- Dual Token Ring link module in slot 9
- Multimode FDDI link module in slot 11
- Quad Ethernet with Filters in slot 13

Prompts, Commands, and Responses

```
console portnum 1
state enabled
prompt {"[%slot%:1]$ "}
auto-manager-script {automgr.bat}
auto-user-script {autouser.bat}
```

CWC ..

bcc> **ethernet slot 13 connector 1**

ethernet/13/1> **help**

Attributes of this object:

bofl: Allows breath-of-life polls to be disabled.
bofl-retries: BOFL Retry Count.
bofl-timeout: Specifies the number of seconds for the BOFL timer.
bofl-tmo-divisor: BOFL TMO divisor.
circuit-name: Circuit Name of this port.
connector: -REQUIRED- connector of the interface.
hardware-filter: Enables the hardware bridge filter if available.
has: Objects this object contains.
name: The name given to the object.
on: Parents of this object.
receive-queue-length: Number of receive buffers dedicated to the chip.
slot: -REQUIRED- Slot of the port.
state: State enable disable.
transmit-queue-length: Number of transmit buffers dedicated to the chip.

Configurable objects in this context:

ip

ethernet/13/1> **ip 192.168.133.114**

Comments

- Console device on port 1

Choose a port (interface type, slot, and connector) for the initial IP interface to the router.

Check to see what you can configure at this level.

You can configure (modify) values currently assigned to attributes of ethernet/13/1, or you can add IP to this interface.

Add IP (address 192.168.133.114) to ethernet/13/1.

Prompts, Commands, and Responses

```
ip/192.168.133.114> info
group {ethernet/13/1}
state enabled
sub-protocols {arp/192.168.133.114/1}
address 192.168.133.114
mask 255.255.255.0
assocaddr 0.0.0.0
cost 1
broadcast 0.0.0.0
mtu-discovery off
mask-reply off
all-subnet-broadcast off
address-resolution arp
proxy off
aging cacheoff
udp-checksum on
tr-end-station off
redirects on
cache-size 128
ip/192.168.133.114> mask 255.255.255.224
```

Comments

Check values currently assigned to attributes of IP on this interface.

BCC automatically enabled ARP on this interface.

BCC set a default subnet mask of 255.255.255.0. You determine that you need to modify the mask to meet the requirements of your network.

Modify the subnet mask for ip/192.168.133.114.

Prompts, Commands, and Responses

ip/192.168.133.114> **info mask**

255.255.255.224

ip/192.168.133.114> **help**

Attributes of this object:

address: -REQUIRED- Address.

address-resolution: Specifies address resolution type.

aging: Specifies in seconds the host cache aging rate.

all-subnet-broadcast: Enables flooding of ASB packets out this interface.

assocaddr: Unnumbered Associated Ip Address.

broadcast: Specifies the IP broadcast address.

cache-size: Specifies the max number of cached routes.

cost: Specifies the RIP interface cost.

has: Objects this object contains.

mask: Mask.

mask-reply: Enables ICMP address-mask-reply messages.

mtu-discovery: Enables the Reply MTU option on this interface.

name: The name given to the object.

on: Parents of this object.

proxy: Enables Proxy ARP on this interface.

redirects: Enables sending of ICMP redirects.

state: State enable disable.

tr-end-station: Enables TRES on this interface.

udp-checksum: Enables UDP checksumming on this interface.

Configurable objects in this context:

rip ospf rdisc arp igmp

Comments

Check the value currently assigned to the mask attribute.

Check to see what you can configure at this level.

You can configure (modify) values currently assigned to attributes of ip/192.168.133.114, or you can add RIP, OSPF, Router Discovery, ARP, or IGMP to this interface.

ip/192.168.133.114> **rip**

Add RIP as the routing protocol (by default , RIP1) on this interface.

Prompts, Commands, and Responses

Comments

rip/192.168.133.114> **cwc**

Return to root (box) level to configure global system services.

bcc> **help**

Check to see what global services (protocols) you can configure at this level.

.
. .
.

Configurable objects in this context:

board ethernet fddi hssi sync tokenring virtual
ip ftp ntp snmp telnet tftp

You can view the configuration of a **board** in any slot, but you cannot modify the attributes of any board object.

You can add any of the following interfaces:

Ethernet, FDDI, HSSI, Sync, Token Ring, or Virtual

And any of the following global services (affecting all slots): IP, FTP, NTP, SNMP, TELNET, and TFTP.

bcc> **snmp**

Add SNMP globally to the box.

snmp> **help**

Check to see what you can configure next at this level.

Attributes of this object:

authentication-traps: Sends trap for sets from false Mgr or Community.

has: Objects this object contains.

lock: Allows the locking mechanism to be disabled.

lock-address: Allows the lock address to be cleared.

lock-timeout: Max number of seconds the agent can be locked.

name: The name given to the object.

on: Parents of this object.

state: State enable disable.

type-of-service: Allows the agent to use reliable UDP datagrams.

Configurable objects in this context:

community trap-entity trap-event

You can configure (modify) values currently assigned to attributes of SNMP, and you can add a community, define a trap entity, or define a trap event.

snmp> **community public**

Define the SNMP community named "public."

Check the values currently assigned to attributes of this SNMP community.

community/public> **info**

Check the values currently assigned to community "public."

group {snmp}

label public

access readonly

community/public> **access readwrite**

To allow network management applications (such as Site Manager) to modify the device configuration, modify the value of the access attribute to **readwrite**.

Prompts, Commands, and Responses

community/public> **manager**
Required attribute "address" was not specified for class: SnmpManager.
Usage: "manager address <value>"
Or: "manager <address>")

community /public> **manager 0.0.0.0**

manager/public/0.0.0.0> **telnet**
telnet>

telnet> help
Attributes of this object:
 auto-user-script: At login, automatically executes user's script.
 command-timeout: Number of minutes before disconnecting.
 force-logout: Prevent user from breaking out of user's script.
 has: Objects this object contains.
 history: Max number of commands stored in history table.
 lines: Specifies the number of lines per screen.
 login-retries: Number of login attempts before disconnecting.
 login-timeout: Number of minutes before disconnecting before login.
 manager-script: Manager login script.
 more: Allows you to disable the screen More.
 name: The name given to the object.
 on: Parents of this object.
 password-timeout: Timeout in minutes on Password entry.
 prompt: Specifies the prompt to use.
 state: State enable disable.
Configurable objects in this context:
 client

telnet> **client**

Comments

Define an SNMP manager for the router.

The BCC error message indicates what you left out and automatically provides extended "Usage" help on how to configure an SNMP manager.

Try again to add the manager, this time supplying a value for its required attribute, **address**. (You must enter a value but not the name for a required attribute.)

Configure another global system service.

You cannot configure telnet within the context of this snmp manager, but the BCC searches backward (toward root level) to find the context suitable for TELNET, then adds that object globally to the device configuration. Note the new "telnet>" prompt.

Check to see what you can configure next at this level.

You can configure (modify) values currently assigned to attributes of telnet, or you can add the telnet client.

Add the telnet client

Prompts, Commands, and Responses

```
client> tftp  
tftp>
```

```
tftp> info  
group {box}  
state enabled  
default-volume 2
```

```
tftp> default-volume 5
```

```
tftp> ftp  
ftp>
```

```
ftp> info  
group {box}  
state enabled  
default-volume 2
```

```
ftp> def 5  
ftp>
```

```
ftp> def  
default-volume 5
```

Comments

Add TFTP globally to the router.

You cannot configure TFTP within the context of the telnet client, but BCC automatically searches back (toward root) to find the parent context suitable for TFTP, then adds that object to the device configuration. Note the new (tftp>) prompt.

Check values currently assigned to attributes of TFTP. You determine that you want to change the default volume number for TFTP from 2 to 5.

Change the default volume to 5

Add FTP globally to the router.

You cannot configure FTP within the context of TFTP, but BCC automatically searches back (toward root) to find the parent context suitable for FTP, then adds that object to the device configuration. Note the new (ftp>) prompt.

Check values currently assigned to attributes of FTP. You determine that you want to change the default volume number for FTP from 2 to 5.

Entering only “def” and a value (abbreviated syntax for **default-volume 5**), change the default volume number to 5.

Verify the change to the **default-volume** number, again using abbreviated syntax.

Prompts, Commands, and Responses

ftp> **show config**

```
box type 16896
  board type 80 slot 5
    board-type sync
  cwc ..
  board type 8448 slot 7
    board-type srml
  cwc ..
  board type 176 slot 9
    board-type dtok
  cwc ..
  board type 192 slot 11
    board-type wffddi2m
  cwc ..
  board type 162 slot 13
    board-type qenf
  cwc ..
console portnum 1
  state enabled
  prompt {"[%slot%:1]$ "}
  auto-manager-script {automgr.bat}
  auto-user-script {autouser.bat}

ethernet slot 13 connector 1
  state enabled
  circuit-name E131
  ip address 192.168.133.114
    state enabled
    mask 255.255.255.224
    assocaddr 0.0.0.0
  arp
    state enabled
  cwc ..
  rip address 192.168.133.114
    state enabled
  cwc ..
  cwc ..
  cwc ..
ip
  state enabled

  arp
    state enabled
  cwc ..
  cwc ..
```

Comments

Check the total configuration of the device to this point.

- Added Synchronous link module in slot 5
- Moved back one level
- Added a System Resource Module in slot 7
- Moved back one level
- Added a Dual Token Ring link module in slot 9
- Moved back one level
- Added a FDDI link module in slot 11
- Moved back one level
- Added a Quad Ethernet with Filters in slot 13
- Moved back one level
- Added the console device on port 1
- Defined the ethernet interface on connector 1 of slot 13
- Added IP (address 192.168.133.114) on ethernet/13/1
- BCC added ARP on ip/192.168.133.114
- Moved back one level
- Added RIP on ip/192.168.133.114
- Moved back one level
- Moved back one level
- Moved back one level
- BCC added global IP as a result of defining ip/192.168.133.114 (first instance of IP on an interface) in the router configuration.
- BCC added global ARP for the same reason.
-
- Moved back one level
- Moved back one level

Prompts, Commands, and Responses

```
snmp
  state enabled
  community label public
  access readwrite
  manager address 0.0.0.0
cwc ..
cwc ..
telnet
  state enabled
  manager-script automgr.bat
client
  state enabled
cwc ..
cwc ..
tftp
  state enabled
  default-volume 5
cwc ..
ftp
  state enabled
  default-volume 5
cwc ..
cwc ..
ftp>
```

ftp> **cwc**

bcc> **tic save config base_114.cfg**

bcc> **tic ping 192.168.133.114**

IP ping: 192.168.133.114 is alive (size = 16 bytes)

Comments

- Added SNMP globally to the router
- Added an SNMP community named "public"
- Changed access from readonly to readwrite
- Added a "wildcard" manager (address 0.0.0.0)
- Moved back one level
- Moved back one level
- Added Telnet globally to the router
- Added client to the global Telnet object
- Moved back one level
- Moved back one level
- Added TFTP globally to the router, with default volume = 5
- Moved back one level
- Added FTP globally to the router, with default volume = 5
- Moved back one level
- Moved back one level

The command shows the total device configuration in terms of BCC syntax (commands and data), and returns you to the current context.

Return to root level or context.

Save the file using a name other than "config" until you can test the configuration. Inserting the **tic** command causes the BCC to pass the **save** command and its arguments back to the Technician Interface for processing.

Test the initial IP interface. As with the previous command, inserting the **tic** command causes the BCC to pass the **ping** command and its arguments back to the Technician Interface for processing.

Prompts, Commands, and Responses

bcc> **tic ping 192.168.133.97**
IP ping: 192.168.133.97 is alive (size = 16 bytes)

bcc> **exit**

Comments

Ensure that the initial IP interface connects to another device on the network

Do not exit BCC immediately. Continue to add other interfaces. When you finish, exit the BCC, which returns you to the Technician Interface prompt for this router.

You may subsequently use Site Manager to add protocols that BCC does not currently support.

Using Technician Interface Scripts

The following scripts are new or amendments to *Using Technician Interface Scripts*:

- enable/disable dcm
- show dcm
- show ipx
- show isdn
- show sws
- show sync
- show wep
- show x25

enable/disable dcm

The **enable/disable dcm** script was renamed from **enable/disable dcmmw** for Router Software Version 11.01. It provides the new command options **base module**, **expansion module**, and **middleware**.

Use the **enable dcm** <options> command to enable DCM components. Use the **disable dcm** <options> command to disable the same components.

The **enable/disable dcm** command supports the following subcommand options:

base_module	expansion_module
middleware	

base_module

Enables or disables the DCM board (*probe*) installed on a BayStack AN, ANH, or ARN Ethernet base module.

Sample Display – enable dcm base_module

```
DCM on Base Module has been Enabled.
```

expansion_module

Enables or disables the DCM board installed on an ARN Ethernet expansion module.

Sample Display – disable dcm expansion_module

```
DCM on Expansion module has been Disabled.
```

middleware

Enables or disables 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.

Sample Display – enable dcm middleware

```
DCM Middleware and all probes have been Enabled.
```

show dcm

The **show dcm** script was renamed from **show dcmmw** for Router Software Version 11.01. They provide the new command options **base module**, **expansion module**, and **middleware**.

Use the **show dcm <option>** command to display information about

- 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 **show dcm** command supports the following subcommand options:

base module	expansion module
middleware	

base module

Displays configuration information about a DCM board installed on an Ethernet base module.

Sample Display – 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
```

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 <i>DCMMW.mib</i> .
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.
Boot Option	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).
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.

expansion module

Displays configuration information about a DCM board installed on an Ethernet expansion module.

Sample Display – 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

middleware

Displays configuration information about the router's DCM software subsystem (DCM middleware, *DCMMW*). The DCMMW driver runs on the router base module; it controls the DCM and provides access to collected RMON statistics.

Sample Display – show dcm middleware

DCM Middleware Information

Application: DCMMW

State: Enabled

Number of DCMs: 1

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

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

show ipx

The **show ipx** command can now include a slot mask to examine routes and services on a specific slot. To display a list of all Dial Optimized Routing (DOR) circuits, use the following new option:

dor

Displays a list of all Dial Optimized Routing (DOR) circuits.

Sample Display - show ipx dor

IPX Dial Opportunity Routing (DOR) Circuit Information

Circuit		IPX	RIP update	SAP update	Stabilize	Watchdog	SPX
Circuit	Index	Interface	Interval	Interval	Timer	Spoof Cnt	Spoof Cnt

Demand 7	6	0x2E025550	3600	3600	120	0	0

1 DOR Circuits in table.

show isdn

The **show isdn** script command has been modified.

inphone

Displays the configuration setup for incoming phone numbers. The display includes the following information:

Index	Index number for this line instance.
Incoming Phone Number	Telephone number of the remote router.
Sub-Addr	Subaddress for a main telephone number.
Callback Circuit Number	Circuit number the router uses to return calls if the Callback Mode is Server One Charge or Server One Charge Call ID.

Sample Display - show isdn inphone

ISDN Incoming Phone Number Configuration

Index	Incoming Phone Number	Sub-Addr	Callback Circuit Number

1	5084361003	None	4

Total of 1 Incoming Phone Entries found.

show sws

The following option is new for the **show sws** script command.

ondemand_dialing callback

Displays information about demand circuits configured for callback. The display includes the following information:

Demand Circuit	Name of the demand circuit. Note that the demand circuit uses a default name as a place holder. When the demand circuit is in use, its name changes to the actual name of the circuit that is in use.
Callback Mode	Role of the router for a callback circuit.
Server Delay	Value of the Callback Server Delay Time parameter. This parameter specifies the time (in seconds) that the server waits to call back the client.
Client Delay	Value of the Callback Client Delay Time parameter. This parameter specifies the time (in seconds) that the client waits for a call from the server.

Sample Display - show sws ondemand_dialing callback

```
Switched Services Dial OnDemand Callback Circuit Information
-----
Demand          Callback          Server    Client
Circuit         Mode              Delay      Delay
-----
Demand 4 Server-one-charge-callid          15         5

Total of      1 Dial OnDemand Callback Circuits.
```

show sync

The **show sync** command has the following new subcommand options in Router Software Version 11.01:

dsucsu_stats	modem_state
dsucsu_config	modem_config

dsucsu_stats

Displays status information about a DSU/CSU module installed in a BayStack AN, ANH, or ARN router.

Sample Display – Example Display - 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 columns displayed have the following meanings:

Slot	Base module slot that contains the DSU/CSU module. For BayStack routers, the value is always 1.
Conn	COM connector number (1, 2, or 3).

Op State	<p>Current V.54 loopback operating state of the interface. States are</p> <ul style="list-style-type: none"> • Normal (no loopback) -- The DSU/CSU is able to forward data. • Local (analog) Loopback -- The DSU/CSU is performing a self-diagnostic local loopback. While operating the local loop test, the CSU loops back the network so as not cause a carrier alarm. • Digital Loopback -- The DSU/CSU is performing a diagnostic test of the local DSU/CSU and the facility circuit. This test typically requires a pattern generator on the remote side to transmit a test pattern, which is returned through the CSU/DSU. • Remote Digital Loopback -- The DSU/CSU is performing a diagnostic test of the local DSU/CSU, facility circuit, and the remote DSU/CSU. This test is a coordinated test with both sides of the facility. The router DSU/CSU sends a signal to the facility to initiate a Digital Loop at the remote DSU/CSU, and then sends a test pattern through the far side of the loop and checks the returned data for errors. • Pattern-2047 -- The DSU/CSU is performing a pattern-only test without initiating loopback. The router DSU/CSU sends a BERT 2047 test pattern to the network.
Service Status	<p>Current status of the DSU/CSU module, as reported by Out of Service or Maintenance Mode codes from the Telco or network carrier. Service states are</p> <ul style="list-style-type: none"> • In Service -- The DSU/CSU and carrier facility are synchronized. • Out of Service (OOS) -- There is trouble with the carrier facility circuit. The circuit from the DSU/CSU module through local loop to the carrier is working, but the circuit is down beyond the central office. • Out of Frame (OOF) -- There is a framing problem on the carrier circuit. • Loss of Line (LOL) -- The local loop to the central office is no longer present. For example, the cable is not connected to the router DSU/CSU interface. • Telco Loopback -- The carrier facility placed the DSU or CSU in a loopback test.
Out of Service Errors	Number of OOS control codes (bipolar violations) received from the central office.
Out of Frame Errors	On Clear Channel 64-K 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.

dsucsu_config

Displays configuration information about a DSU/CSU module installed in a BayStack AN, ANH, or ARN router.

Sample Display – Example Display - 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 columns displayed have the following meanings:

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.

modem_state

Displays status information about a V.34 Modem adapter module installed in a BayStack ARN router:

Init Slot	Base module slot that contains the V.34 modem module. For the BayStack routers, the value is always 1.
Conn	COM connector that contains the V.34 modem module (1 or 2).

Init State	<p>Current state of modem initialization. States are</p> <ul style="list-style-type: none"> • Startup (1) • SCCInit (2) • GetInfo (3) • SetDefaults (4) • Initialization (5) • PhoneNumber (6) • Loopback (7) • InitComplete (8)
Line State	<p>Current operational state of modem interface. States are</p> <ul style="list-style-type: none"> • Unknown (1) • On Hook (2) • Off Hook (3) • Connected (4) • Busy Out (5) • Reset (6)

Sample Display – Example Display - show sync modem_state

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

modem_config

Displays configuration information about a V.34 Modem adapter module installed in a BayStack ARN router:

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.

Sample Display – Example Display - 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
```

show wep

The **show wep** <option> commands display information about the WAN Encryption Protocol and services. For detailed information on the Bay Networks implementation of encryption services, refer to *Configuring Encryption Services*.

The **show wep** command supports the following subcommand options:

circuits <circuit_name>	stats [errors] [line_number.llindex.circuit_number.vc_ _id]
lines <line_number.llindex>	version
vcs <line_number.llindex.circuit_number.vc_ _id>	

circuits <circuit_name>

Displays the state of the circuits.

circuit_name Limits the display to the specified circuit.

The table includes the following information:

Circuit Name	Name of the circuit
Circuit Number	Number of the circuit
Enable	Encryption set to Enable or Disable
Cipher Mode	Encryption strength set to 40-bit 56-bit Inherit from Line Both
TEK Update Rate (bytes)	Number of data bytes between change in the value of the Traffic Encryption Key (TEK)
TEK Update Rate (seconds)	Number of seconds between change in the value of the TEK

Sample Display – show wep circuits

WEP Circuit Entries

Circuit Name	Circuit Number	Enable	Cipher Mode	TEK Update Rate (bytes)	TEK Update Rate (seconds)
S21	2	Enabled	Inherit	65535	10
S22	3	Enabled	Inherit	65535	10

2 WEP circuit(s) configured.

lines <line_number.llindex>

Displays the state of the lines.

line_number.llindex Limits the display to the specified line.

The table includes the following information:

Line Number	Line number
LL Index	Instance identifier
Slot	Slot identifier
Module	Module identifier
Conn	Connector identifier
Cipher Mode	Encryption strength set to 40-bit 56-bit Both
TEK Update Rate (bytes)	Number of data bytes between change in the value of the Traffic Encryption Key (TEK)
TEK Update Rate (seconds)	Number of seconds between change in the value of the TEK

Sample Display – show wep lines

WEP Line Entries

Line Number	LL Index	Slot	Module	Conn	Enable	Cipher Mode	TEK Upd Rate (bytes)	TEK Upd Rate (seconds)
202101	0	2	1	COM1	Enabled	40bitDES	65535	10
202102	0	2	1	COM2	Enabled	40bitDES	65535	10

2 WEP line(s) configured.

VCS

Displays the state of the virtual circuits configured for encryption. The table includes the following information:

Line Number	Line number
LL Index	Instance identifier
Circuit Name	Name of the circuit
VC ID	VC identifier
Connection State	State of the connection: Up Down Initializing
Actual Cipher Mode	Encryption strength the VC is using: 40-bit 56-bit
TEK Update Rate (bytes)	Number of data bytes between change in the value of the Traffic Encryption Key (TEK)
TEK Update Rate (seconds)	Number of seconds between change in the value of the TEK

Sample Display – show wep vcs

WEP Virtual Circuit Entries

Line Number	LL Index	Cct Name	Vc Id	Connection State	Actual Cipher Mode
202101	0	S21	0	Init	None
202102	0	S22	123	Up	40-bit DES

2 WEP virtual circuit(s) configured.

stats

Displays statistical information about encryption services. The table includes the following information.

Line Number	Line number
LL Index	Instance identifier
Circuit	Name of the circuit
VC ID	VC identifier
Connection State	State of the connection: Up Down Initializing
Bytes Encrypted	Number of data bytes that have been encrypted on this circuit
Bytes Decrypted	Number of data bytes that have been decrypted on this circuit

Sample Display – show wep stats

WEP Performance And Data Statistics

Line Number	LL Index	Circuit	Vc Id	# Bytes Encrypted	# Bytes Decrypted
202101	0	S21	0	0	0

Line Number	LL Index	Circuit	Vc Id	# Bytes Encrypted	# Bytes Decrypted
202102	0	S22	123	7339	12539

2 entries.

version

Displays the current version number and modification date of the *WEP.bat* script.

Sample Display – show wep version

WEP.bat Version: 1.1 Date: 6/6/96.

show x25

Version 11.01 adds QLLC as an X.25 Service Type. The X.25 **show** command includes the following changes and additions.

configuration [*<slot.connector>*]

Displays the basic configuration information for all X.25 lines or displays only the slot and connector specified. Each line is associated with the services available on that line and the number of virtual circuits configured. The table includes the following information for the protocol:

Slot.Connector.Line.LLIndex	The identity of the line. This includes four parts as follows: slot number, connector number, number of the line that the driver X.25 runs on, lower-layer index from the layer immediately below X.25 on the protocol stack. If the lower layer is a driver, the index is 0.
LCN's Configured	Number of logical channels configured; includes LCNs for incoming, bidirectional, and outgoing VCs.
Services Available	Type of service available on this line: PDN, DDN, PTOP, IPEX, or QLLC.

Sample Display - show x25 configuration

Protocol	Slot.Connector.Line.LLIndex	LCN's Configured	Services Available
X.25	5.2.205102.0	10	QLLC
X.25	5.3.205103.0	10	QLLC
X.25	5.4.205104.0	10	PDN

3 Configuration Entries.

qlc maps

Displays the QLLC mappings for the router. Each entry consists of two lines.

Cct	Specifies the circuit of the QLLC connection.
State PID	Specifies the protocol ID used in the first byte of the Call User Data of the X.25 Call Request packet.
Adjacent X.121 Address	Specifies the X.121 address of the device that connects to the interface running the QLLC/X.25 software.
Partner X.121 Address	Specifies the X.121 address of the device that connects through the DLSw network.
Adjacent MAC Address	Specifies the MAC address assigned to the QLLC device.
Partner MAC Address	Specifies the MAC address assigned to the SNA device.
Adjacent SAP Address	The SAP address associated with a communication subsystem on an adjacent device.
Partner SAP Address	The SPA address associated with a communication subsystem on a partner device.
PU Type	The type of the adjacent SNA node.
Gen XID	Indicates if the Gen XID parameter is enabled or disabled.
Node ID	Identifies the Node.
Map Name	Specifies the name of the QLLC mapping entry.
Option	Specifies when to forward an XID to the adjacent device.
Trace	Specifies the type of debugging enabled.

Sample Display - QLLC Address Mappings

Circuit	State PID	Adjacent X121 Partner X121	Adjacent MAC Partner MAC	aSAP pSAP	PU Type GenXID	Node ID Map Name	Option Trace
xvc5.3.2	Active	1111122222	40000000DEAD	0x04	PU 2.0	00171182	0x0000
*05103.0	0xCB	3333344444	4000C1024264	0x04	Disable	Lab3174	0xFF1
xvc5.2.2	Active	3333344444	4000C1024264	0x04	PU 2.0	(nil)	0x0001
*05102.0	0xCB	1111122222	40000000DEAD	0x04	Disable	Host	0xFF1

2 QLLC Mapping Entries

Using Technician Interface Software

The following sections are new in *Using Technician Interface Software*:

- [ARN Diagnostics On/Off Option](#)
- [AN and ANH Powerup Diagnostic Option](#)
- [Secure Shell Commands](#)

ARN Diagnostics On/Off Option

For ARN platforms only, the Technician Interface **diags** command supports an option to enable or disable diagnostics, effective on the next power-up cycle. Disabling the diagnostics results in a faster boot time, but leaves the hardware components unverified.

The syntax for this option is as follows:

diags [-<on/off>] [<slot_id>]

<code>diags -on [<slot_id>]</code>	The ARN executes all power-up diagnostics at subsequent restarts.
<code>diags -off [<slot_id>]</code>	The ARN skips power-up diagnostics at subsequent restarts.
<code>diags</code>	The ARN restarts immediately and executes complete diagnostics.

AN and ANH Powerup Diagnostic Option

You can use the **set** command on AN and ANH routers to disable or reenble the powerup diagnostics.

set [-P0 | P1]

<code>set -P0</code>	The router skips powerup diagnostics at subsequent restarts.
<code>set -P1</code>	The router executes all powerup diagnostics at subsequent restarts.

Pressing the Reset button on the back panel of the AN for more than 5 seconds initiates a cold boot; powerup diagnostics execute even when disabled by the **set -P1** command.

Secure Shell Commands

This release includes some new Technician Interface commands that you use to work in the secure shell of the router.

Command	System Response
kexit	Exits the secure shell.
kget <subcommand>	Obtains a parameter in the secure shell. Example: kget ppp s21 obtains parameter values for PPP circuit 21. Example: kget fr <arguments> obtains parameters for Frame Relay circuit <arguments>.
kpassword	Changes the password of the secure shell.
kseed	Initializes the cryptographic random number generator while in the secure shell.
ksession	Initiates a secure shell session.
kset <sub_command> [<flags>]	Sets parameter values in the secure shell. Example: kset npk <value> sets the router Node Protection Key.
ktranslate <old_NPK>	Translates a configuration from an old NPK value to the current NPK value. Example: ktranslate <old_npk> <new_npk>

For more information on these commands, refer to *Configuring Encryption Services*.

