Documentation Changes Notice for Router Version 11.02 and Site Manager Version 5.02

Router Software Version 11.02
Site Manager Software Version 5.02

Part No. 115506-A Rev. B
June 1997

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

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

About This Guide

If you are responsible for configuring and managing Bay Networks® routers, you need to read this guide to learn about changes to router software and hardware since release 11.0/5.0. Table 1 of this guide lists the manuals included in the 11.01/5.01 and 11.02/5.02 releases, identifies new and revised manuals since release11.0/5.0, and lists those manuals that we have not revised, and which are affected by sections in this documentation change notice.

Conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &** Example: Use the **dinfo** command. Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.

`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu. Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show at routes** | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers:

- Phone--U.S./Canada: 1-888-422-9773
- Phone--International: 1-510-490-4752
- FAX--U.S./Canada and International: 1-510-498-2609

Bay Networks Customer Service

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

Region	Telephone number	Fax number
United States and Canada	1-800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 1-508-916-8880 (direct)	1-508-670-8766
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

How to Get Help

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

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

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	1-800-2LANWAN	508-670-8765
Santa Clara, CA	1-800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

For More Information

For information about Bay Networks and its products, visit the Bay Networks World Wide Web (WWW) site at http://www.baynetworks.com. To learn more about Bay Networks Customer Service, select Customer Service on the opening Web page.

Documentation Changes Notice

Table 1 lists the manuals included in the 11.01/5.01 and 11.02/5.02 releases, identifies new and revised manuals since release 11.00/5.00, and those manuals affected by sections in this documentation change notice.

Table 1. 11.01 and 11.02 Documentation

Document Title	New or Revised Book for 11.01/5.01	New or Revised Book for 11.02/5.02	Affected by Section in DCN
Cable Guide			
Configuring AppleTalk Services			
Configuring APPN Services			
Configuring ATM Services			✔
Configuring ATM DXI Services			
Configuring Bridging Services			✔
Configuring BSC Transport Services			✔
Configuring Data Compression Services			
Configuring Data Encryption Services	✔		✔
Configuring Dial Services		✔	✔
Configuring DECnet Services			
Configuring DLSw Services		✔	✔
Configuring Ethernet, FDDI, and Token Ring Services		✔	

(continued)

Table 1. 11.01 and 11.02 Documentation *(continued)*

Document Title	New or Revised Book for 11.01/5.01	New or Revised Book for 11.02/5.02	Affected by Section in DCN
Configuring Frame Relay Services			✔
Configuring Interface and Router Redundancy	✔		
Configuring IP Multicasting Services		✔	
Configuring IP Services			✔
Configuring IP Utilities			✔
Configuring IPX Services			✔
Configuring LLC Services			
Configuring LNM Services			
Configuring OSI Services			
Configuring PPP Services			✔
Configuring RADIUS		✔	✔
Configuring Routers			✔
Configuring SDLC Services			
Configuring SMDS			
Configuring SNMP, RMON, BOOTP, DHCP, and RARP Services		✔	
Configuring Traffic Filters and Protocol Prioritization			✔
Configuring WAN Line Services		✔	✔
Configuring VINES Services			
Configuring X.25 Services	✔		✔
Connecting ASN Routers and BNX Platforms to a Network			
Connecting BayStack AN and ANH Systems to a Network			
Connecting AN200 Routers to a Network			✔

(continued)

Table 1. 11.01 and 11.02 Documentation *(continued)*

Document Title	New or Revised Book for 11.01/5.01	New or Revised Book for 11.02/5.02	Affected by Section in DCN
Event Messages for Routers and BNX Platforms			✔
Managing Routers and BNX Platforms			
Modifying Software Images for Routers			✔
Quick-Starting Routers and BNX Platforms			✔
Troubleshooting Routers			
Upgrading Routers from Version 7-10.xx to Version 11.0			✔
Using the Bay Command Console	✔		✔
Using Site Manager Software			
Using Technician Interface Scripts			✔
Using Technician Interface Software			✔
Writing Technician Interface Scripts			

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
- Specifying the Emulated LAN Segment ID
- Protocol Support
- Enabling or Disabling Per-VC Clipping
- Modifications to ATM Signaling Parameter Defaults
- IP and NULL Encapsulated PVC Service Records

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 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

Specifying the Emulated LAN Segment ID

You must specify an Emulated LAN Segment ID when

- The LAN emulation (LANE) client is a token ring endstation. A LANE client is a token ring endstation when it resides at the edge of a token ring network.
- You are routing IP or IPX across a source route bridge (SRB) token ring network.

The Emulated LAN Segment ID defines the ring ID (in decimal) on which the LANE client resides. By default, this value is set to zero (0). However, you can specify a value from 0 to 4095 for the token ring segment ID.

Parameter: Emulated LAN Segment ID

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

Default: 0

Options: 0 to 4095

Function: Defines the ring ID (in decimal) on which this token ring client resides. You need only set this parameter for IEEE 802.5 LANE clients that are:

- Token ring endstations
- Routing IP or IPX across a source route bridge (SRB) token ring network

Instructions: Accept the default, 0, or enter a value from 0 to 4095.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.5.20.1.1.20

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

(continued)

Table 2. Supported Protocols *(continued)*

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
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 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*.

Enabling or Disabling Per-VC Clipping

Per-VC clipping provides an added traffic-shaping option that allows you to modify how your ATM line responds to oversubscribed traffic. By default, per-VC clipping is disabled on a line. However, you can enable or disable per-VC clipping at any time.

When enabled, this option clips frames intended for an oversubscribed VC when the number of frames in memory exceeds a predetermined limit.

Note: Changing the state of this parameter tears down all active VCs on the interface. The new state takes affect after reestablishing VC connections.

Parameter:	**Per-VC Clipping**
Path:	Configuration Manager > Circuits > Edit Circuits > **Edit** > **Line Attributes**
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables cell clipping on a per-VC basis.
Instructions:	Accept the default, Disable, for normal VC clipping. Enable this parameter if you want to clip cells on a per-VC basis.
MIB Object ID:	1.3.6.1.4.1.18.3.4.23.3.1.1.17

Modifications to ATM Signaling Parameter Defaults

The default value for the “Max Number of SVC Applications” parameter changed from 20 to 96. The “Max Point to Multipoint Connections” parameter changed from 40 to 64. These modifications allow for a default, per circuit value of up to 32 applications or connections.

Refer to the following signaling parameter descriptions for details.

Parameter: Max Number of SVC Applications

Path: Configuration Manager > Protocols > ATM > ATM Signaling

(This parameter also appears in the Initial ATM Signaling Config window.)

Default: 96

Options: 1 to 32767

Function: Identifies the maximum number of service access points (SAPs) allowed for this circuit. The number of SAPs corresponds to the number of LAN emulation or IP (RFC 1577) clients allowed for the circuit.

Instructions: Accept the default, 96, or enter a value from 1 to 32767.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.1.7.1.6

Parameter: Max Point to Multipoint Connections

Path: Configuration Manager > Protocols > ATM > ATM Signaling

(This parameter also appears in the Initial ATM Signaling Config window.)

Default: 64

Options: 0 to 32767

Function: Identifies the maximum number of simultaneous point-to-multipoint connections allowed for this circuit.

Instructions: Accept the default, 64, or enter a value from 0 to 32767.

MIB Object ID: 1.3.6.1.4.1.18.3.4.23.1.7.1.8

IP and NULL Encapsulated PVC Service Records

When running IP over a NULL encapsulated PVC service record, you must change the Address Resolution parameter to NONE. You must then add an IP adjacent host with the MAC address equal to the VPI/VCI of the PVC. Refer to *Configuring IP Services* for information about the Address Resolution parameter.

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. Instead 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 BSC Transport Services

The following section is an amendment to *Configuring BSC Transport Services*.

Bisync Over TCP

Bisync over TCP (BOT) is now supported on the Advanced Remote Node™ (ARN™) using the Tri-Serial Expansion Module, Ethernet and Tri-Serial Expansion Module, and the Token and Tri-Serial Expansion Module.

Configuring Data Encryption Services

Software data encryption was a new feature in Release 11.01/5.01. The following sections are amendments to *Configuring Data Encryption Services*:

- Data Encryption Availability
- Installing Software Encryption on an HP Platform
- Data Encryption and Dial Services

Data Encryption Availability

Data encryption is available for purchase as a separate CD-ROM in one of two versions, 40-bit or 56-bit. Each version requires a special version of Site Manager, which is included on the appropriate CD.

The 56-bit encryption option is generally available only in the United States and Canada. U.S. law allows export of 56-bit encryption only with a U.S. export license. For more information on the export, import, and use of encryption outside the United States and Canada, refer to the software license agreement.

Installing Software Encryption on an HP Platform

When you copy the *wep.exe* file to an HP platform, it is automatically renamed *WEP.EXE;1*. You must rename the file back to *wep.exe*. You can do this by issuing the following command:

mv “WEP.EXE;1” wep.exe

Note that you must use quotation marks before and after *WEP.EXE;1*.

Data Encryption and Dial Services

You can configure PPP dial backup for a Frame Relay circuit that uses data encryption. Be aware, however, that if the primary circuit fails, data that travels over the backup circuit is unencrypted.

Configuring DLSw Services

The following section is an amendment to *Configuring DLSw Services*.

DLSw XID Enable/Disable Parameter

Release 11.02 contains a new MIB attribute that allows you to enable and disable PU2.1 circuit XIDs to pass through to SDLC when the local router is connected to a token ring network and the remote router is connected over SDLC. Use the Technician Interface to set the value to enabled or disabled. The default is disabled.

```
wfDlsLocalDeviceEnableXidPassthru OBJECT-TYPE
    SYNTAX INTEGER {
            enabled(1),
            disabled(2)
          }
    ACCESS  read-write
    STATUS  mandatory
    DESCRIPTION
          "XID passthru Enable/Disable parameter. Default is disabled. "
    DEFVAL  { disabled }
    ::= { wfDlsLocalDeviceEntry 19 }
```

To set the attribute to enable:

set wfDlsLocalDeviceEntry.wfDlsLocalDeviceEnableXidPassthru.cct.sdlc_address 1;commit

To set the attribute to disable:

set wfDlsLocalDeviceEntry.wfDlsLocalDeviceEnableXidPassthru.cct.sdlc_address 2;commit

Configuring Dial Services

The following sections are amendments to *Configuring Dial Services*.

Modifications to Dial Services Parameter Descriptions

The following parameter descriptions have been modified:

- Port Application Mode Parameter (BRI)

  The Dialup - Floating B option has been revised to include the ARN router.

- BRI T3 Timer

  The BRI T3 Timer parameter has been modified to include references to the U interface.

- BRI B Channel Loopback

  The BRI B Channel Loopback parameter has been modified to include references to the U interface.

- ISDN Numbering Plan (local phone numbers)

  The default value for the ISDN Numbering Plan parameter is incorrect. The correct default is Telephony.

- Backup Pool ID

  The MIB object ID for the Backup Pool ID parameter is incorrect. The correct MIB object ID is 1.3.6.1.4.1.18.3.5.1.4.5.1.5.

- Primary Down Time

The corrected parameter descriptions follow.

Note: For simplicity, the Port Application Mode parameter description lists only the revised option.

Parameter: Port Application Mode

Path: Configuration Manager > **ISDN Connector** > Port Application

Default: Dialup - 2B+D

Options: Dialup - Floating B: This option is available only on the AN, ANH, and ARN routers. It specifies that although this is an ISDN switched line that provides two B channels, the software makes the necessary adjustments if only one channel is in use. Use this option if you can purchase only 2B + D service, but only want to use one B channel, or your application requires two synchronous ports and only one B channel.

Function: Determines how the BRI service operates.

Instructions: If you have a dialup application, choose one of the dialup options.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.8.9.1.34

Parameter: BRI T3 Timer

Path: **ISDN Connector** > ISDN Dialup > **Edit D Chan** > BRI Interface Configuration

Default: 10 seconds

Options: 1 to 30 seconds

Function: Indicates the amount of time that the router has to try and activate the ISDN S/T or U interface (ARN only). The router starts this timer while the ISDN interface is deactivated and the router tries to activate it, for example, when the router wants to send data. During this period, the router sends INFO 1 frames across the ISDN interface until the network responds with a signal or the timer expires. This timer prevents the router from attempting to activate the ISDN interface interminably.

Instructions: Enter a time limit that is sufficient for the router to activate the ISDN S/T or U interface. This value should be greater than the time it would take to activate the ISDN interface under normal conditions. You may want to ask your ISDN provider for guidelines regarding the subscriber loop transmission, which might affect the value you enter.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.8.9.1.14

Parameter: **BRI B Channel Loopback**

Path: **ISDN Connector** > ISDN Dialup > **Edit D Chan** > BRI Interface Configuration

Default: Disable

Options: Enable | Disable

Function: This parameter is for Layer 1 ISDN BRI conformance testing. It allows the external equipment to send data to the router over the B channels and loop it right back out the S/T or U interface (ARN only). The external equipment can verify its physical connection to the router.

Instructions: Select Enable if you want to run a loopback test between the network and the S/T or U interface on the router. Do not enable this parameter when the router is in normal operational mode.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.8.9.1.13

Parameter: **ISDN Numbering Plan**

Path: Dialup > Local Phone Numbers > ISDN Local Phone Lines > **Local Phones** > ISDN Local Phone Numbers

Default: Telephony

Options: Unknown | Telephony | X121 | Telex | Standard | Private

Function: Indicates the standard that the phone number plan follows. The router passes this information to the ISDN switch.

Instructions: If you set the Switch Type parameter to BRI NTT, BRI KDD, or BRI NI1, select the value, Unknown. For all other switches, Site Manager uses the default value Telephony. Accept Telephony unless your service provider instructs otherwise.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.8.12.1.10

Parameter: **Backup Pool ID**

Path: Dialup > Backup Pools > Pools > **Add** > Backup Pool Configuration

Default: None

Range: 1 to 255

Function: Identifies the line pool by assigning it a number.

Instructions: Enter a number from 1 to 255 as the line pool ID.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.5.1.5

Parameter: **Primary Down Time**

Path: Dialup > Backup Circuits > Frame Relay > FR Primary Interface Definition

and

Dialup > Demand Circuits > **PPP Circuits** > PPP Demand Circuits

Default: 5 minutes

Range: 1 to 999,999 minutes

Function: Specifies the amount of time the router waits, at boot time, before activating a backup connection. This timer ensures that the primary connection is not operational before the router activates a backup connection.

Instructions: Enter the amount of time the router should wait before activating a backup connection.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.5.1.17

Configuring Frame Relay Services

The following sections are amendments to *Configuring Frame Relay Services*. They compare service records with the access modes that formerly defined Bay Networks Frame Relay services.

Group Access Mode

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

Group access mode advantages are that it

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

Its disadvantages are that it

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

Service Records and Group Mode

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

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

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

Service Records and Direct Access Mode

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

Direct access mode advantages are that it

- Limits broadcasts to one PVC
- Enables multiple Layer 3 networks per interface

Direct access mode disadvantages are that it

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

Service Records and Direct Mode

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

Service Records and Hybrid Access Mode

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

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

Default Service Record

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

Configuring IP Services

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

- Opening the IP Accounting Window
- Controlling the Notification of a Full IP Accounting Table

The section, “Configuring an OSPF Neighbor on a Standard Point-to-Multipoint Interface,” is new for Release 11.01/5.01.

The following sections are new for Release 11.02/5.02:

- Configuring OSPF Interface Parameters Dynamically
- Enabling Equal-Cost Multipath Support
- Enabling ISP Mode and Selecting a Slot for the BGP Soloist

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 the 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.

After 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 OSPF Interface Parameters Dynamically

In OSPF versions earlier than 11.02, configuring OSPF interface parameters dynamically with Site Manager causes OSPF to restart.

Beginning with version 11.02, you can configure OSPF interface parameters dynamically without causing OSPF to restart.

The following restrictions apply:

- The OSPF backup soloist must be disabled. (The backup soloist is disabled by default.)
- The dynamic configuration must modify the OSPF interface record only. For example, if you change the cost of the OSPF interface dynamically, you are modifying the interface record only. OSPF does not restart. If you change the router ID, however, you are modifying the OSPF general group and OSPF restarts.

Enabling Equal-Cost Multipath Support

IP equal-cost multipath support is a load-balancing feature that allows IP to distribute traffic over multiple (up to five) equal-cost paths to the same destination.

By default, multipath support is disabled on the router: for each routing protocol, IP stores the best next hop to a destination in the routing table. If traffic arrives on an interface, IP determines the best route to the destination and forwards all packets out the next-hop interface.

Selecting the Multiple Next-Hop Calculation Method

If multipath support is enabled, IP will distribute traffic among equal-cost routes (if such routes are available). You can use Site Manager to enable multipath support on the router and to specify whether IP distributes packets in a round-robin fashion or uses a distribution method based on the source and destination address of the packets.

- In *round-robin* distribution, IP forwards each packet to a different next hop until it reaches the end of the list of available next hops; then it repeats the list. Round-robin distribution makes full use of available resources but may cause packets to be delivered out of order.
- In *source-destination hash* distribution based on the source and destination address, IP forwards all packets with a given source and destination address to the same next hop. This method increases the chances that the packets will be delivered in order.
- In *destination-hash* distribution based on the destination address only, IP forwards all packets with a given destination address to the same next hop.

To select a multiple next-hop calculation method with Site Manager:

1. **Open the IP Global Parameters window.**
2. **Select the Multiple Next-Hop Calculation Method parameter.**
3. **Click on Values.**
4. **Select a method.**

Configuring RIP and OSPF for Equal-Cost Multipath Support

By default, the IP routing table contains a single “best” RIP route and single best OSPF route to a given destination. If either protocol submits another route to the same destination, IP compares the new route with the current one. If the new route is better, IP replaces the current route with the new one. If not, IP discards the new route.

If you have enabled equal-cost multipath support on the router, IP can store multiple equal-cost best RIP and OSPF routes in the routing table. When RIP or OSPF submits a route to a destination, one of the following events occurs:

- IP determines that the current route to that destination is better than the new route. IP discards the new route.
- IP determines that the new route is better than the current route. IP discards the current route and replaces it with the new one. In the event that the routing table contains multiple equal-cost best routes, IP discards all of these routes.
- IP determines that the new and current routes have the same cost. IP adds the new route to the routing table -- up to a maximum number that you specify. If the routing table already contains the maximum number of equal-cost routes from RIP or OSPF, IP discards the route.

To specify the maximum number of equal-cost RIP and OSPF routes that IP stores in the routing table:

1. **Open the IP Global Parameters window.**
2. **Select the RIP Maximum Equal Cost Paths parameter.**
3. **Click on Values, select the number of paths, and click on OK.**
4. **Select the IP OSPF Maximum Paths parameter.**
5. **Click on Values, select the number of paths, and click on OK.**
6. **Click on OK in the IP Global Parameters window.**

Enabling ISP Mode and Selecting a Slot for the BGP Soloist

Beginning with version 11.02, IP provides an Internet Service Provider (ISP) mode of operation.

In ISP mode, IP

- Enables the BGP soloist. By default, BGP runs on all slots configured with IP interfaces. In ISP mode, BGP runs as a soloist.
- Disables IP forwarding caches. By default, IP maintains a forwarding cache on each IP interface. IP maintains this table as a cache for routes that are frequently used to forward data packets that arrive on the interface. However, if the number of frequently used routes exceeds the size of the forwarding table, the router will continually update the forwarding cache by removing old routes and installing new route entries. ISP mode disables all forwarding caches on all IP interfaces, and optimizes the routing table to allow direct forwarding, avoiding the overhead of cache misses and updates. If you select ISP mode, you do not have to explicitly disable the forwarding tables on each interface.

By default ISP mode features are disabled on the router. To enable these features (and to select a slot for the BGP soloist) with Site Manager:

1. **Open the IP Global Parameters window.**
2. **Select the ISP Mode parameter.**
3. **Click on Values and select Enable.**
4. **Click on OK in the IP Global Parameters window.**

   The Edit Soloist Slot window opens.
5. **Click on Values and select a slot.**
6. **Click on OK.**

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 the Delete Peer button has changed to the Delete button.

Configuring IPX Services

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

- Configuring the IPX Interface Cost Parameter
- Configuring Max Path and Max Path Splits for IPX
- Configuring the Next Hop Parameter
- Using IPX Dial Optimized Routing (DOR)

Configuring the 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 the Next Hop Parameter

The next-hop host address is the MAC address of the next hop on the way to the destination. A revised Next Hop Host parameter description follows:

Parameter:	**Next Hop Host (hex)**
Default:	None
Options:	Any valid host address in hexadecimal notation
Function:	Specifies the address of the next-hop host in the static routing path.
Instructions:	Enter a next-hop host address of up to 12 hexadecimal characters. The next-hop host address is the MAC address of the next hop on the way to your destination.

Using IPX Dial Optimized Routing (DOR)

The following information will help you use DOR optimally.

Inactivity Mode

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

RIP/SAP Pace and Packet Size Parameters

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

Diagnostic Packets and Time Synchronization

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

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

Configuring PPP Services

The following sections are amendments to *Configuring PPP Services*. These amendments apply to switched services only:

- Changing the PPP MRU Size Setting for Routers Running Version 11.02 and Earlier
- PPP Interoperability with CLAM

Changing the PPP MRU Size Setting for Routers Running Version 11.02 and Earlier

For Version 11.02, we changed the PPP default MRU Size for switched services from 1590 to 1500 bytes. If you have a network with both 11.02 and earlier Bay Networks routers, or Bay Corporate LAN Access Module (CLAM™) routers configured with dial-on-demand, standby, dial backup, or bandwidth-on-demand circuits, make sure that the value you set for the PPP MRU Size parameter is the same for the central-site and remote-site routers.

To accomplish this task, consider one of the following options:

- Upgrade all routers to version 11.02 simultaneously.

  We strongly recommend this option.

- Upgrade the central site router to version 11.02, leaving the remote site routers untouched. Then change the default MRU Size on the central site router to 1590 bytes.
- As you upgrade each remote site router software to version 11.02, set its MRU Size to 1590, unless you can segregate the 11.02 remote sites into their own demand pool. You can do this if some of the remote-site routers are Bay CLAMs, provided they are running a CLAM release earlier than 3.5x. CLAM routers running software earlier than 3.5x allow you to set the default MRU Size to 1590.
- If some remote site CLAM routers are running release 3.5x, then you cannot set the MRU Size to 1590. In this case, isolate those CLAM routers on their own demand pool on the 11.02 router and set the MRU Size of that pool to 1500.
- Upgrade the central-site router to Version 11.02, and set the default MRU Size to 1500. Then reconfigure all remote-site routers dialing into that demand pool with the same MRU Size.

  For pre-11.02 routers, change the MRU Size to 1500.

- Change the MRU Size in the Sync Driver MTU attribute (the 1510 value becomes 1500 after subtracting CRC and PPP headers) of the pre-11.02 router to 1510. CLAMs running Version 3.5x use the default setting of 1500.
- If you upgrade the central site router to 11.02 and the default MRU Size of 1500 is taken on one pool (to satisfy 3.5x CLAMs or 11.02 routers), you can choose a different default value (for example, 1590) for a different pool that the 11.01 or pre-3.5x CLAM router dials into.

PPP Interoperability with CLAM

If you configure a CHAP local name on a Bay Networks router that connects to a CLAM, that local name is used to negotiate the link. If you do not configure a CHAP local name, the router uses *BAYNETWORKS* as a default CHAP local name.

Configuring RADIUS

The MIB Object ID for the Slot Number parameter is incorrect in *Configuring RADIUS*, Version 11.02/5.02. The correct number is 1.3.6.1.4.1.18.3.5.22.1.1.4.

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 1, and to Tables 3 and 4, to determine the Site Manager connector names for your ARN interfaces.

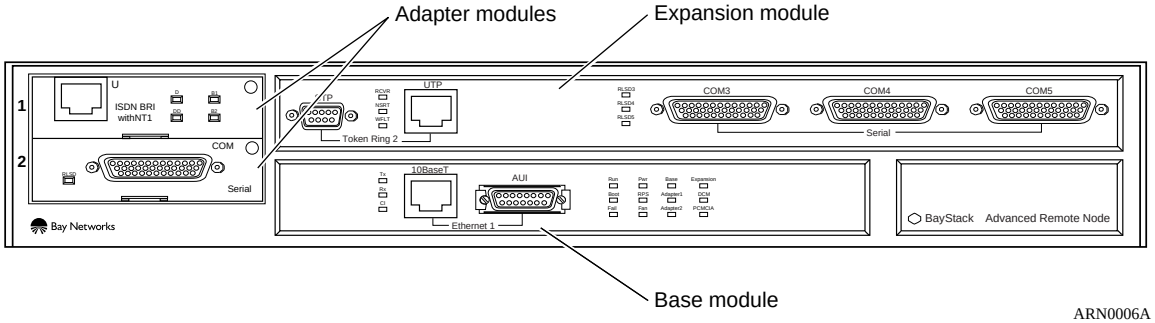

Figure 1. ARN Module Locations

Table 3 lists the Configuration Manager names for ARN adapter modules. Table 4 indicates how the physical interface labels on ARN expansion modules correspond to connector names in the Configuration Manager window.

Table 3. Site Manager Names for ARN Adapter Module Interfaces

	Site Manager Connector Name	
Adapter Module Label	**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 4. 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 to 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 2).**

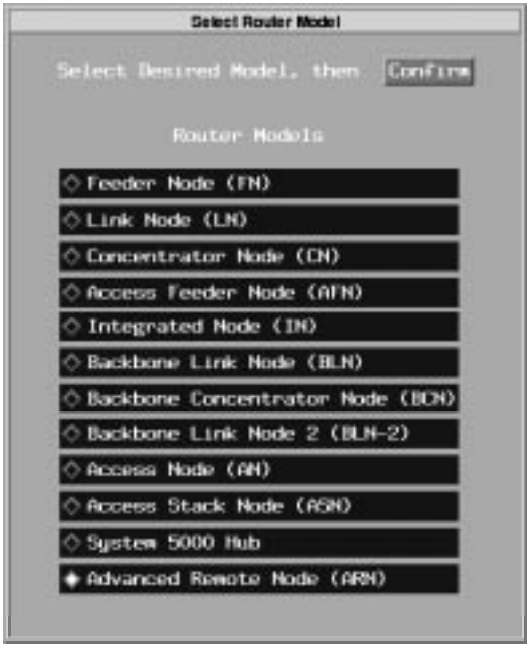

Figure 2. Selecting the ARN Router Model

A blank Configuration Manager screen for the ARN appears (Figure 3).

Figure 3. Blank ARN Configuration Manager Window

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

   The Module List for the ARN appears (Figure 4).

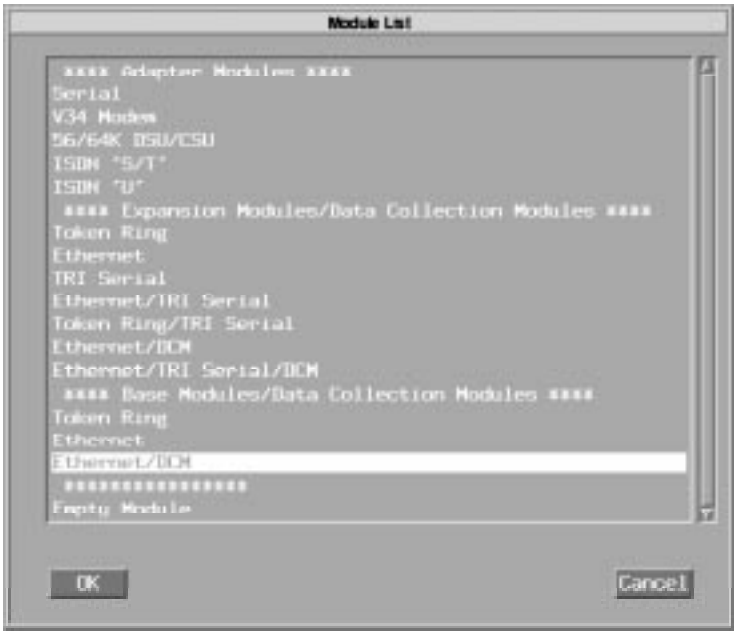

Figure 4. Selecting an ARN Base Module

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

   Refer to Figure 1 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 5).

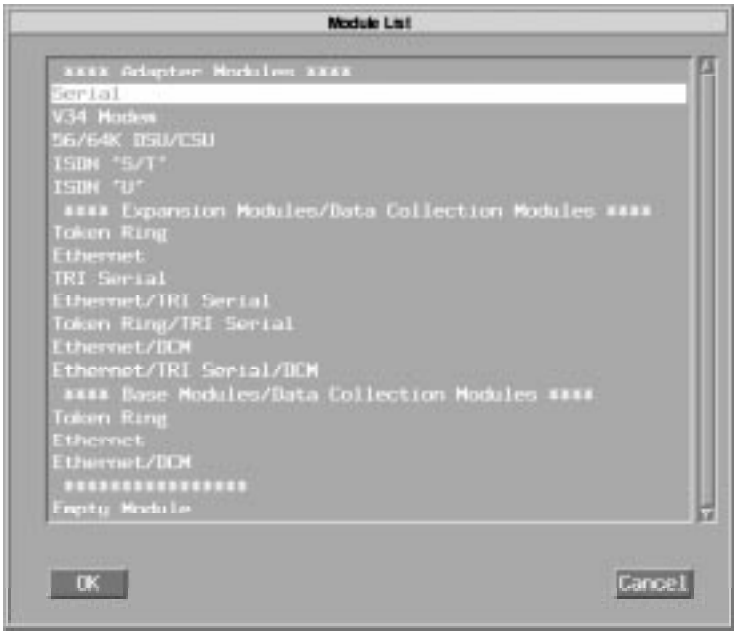

Figure 5. Selecting an ARN Adapter Module

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

   Refer to Figure 1 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 6).

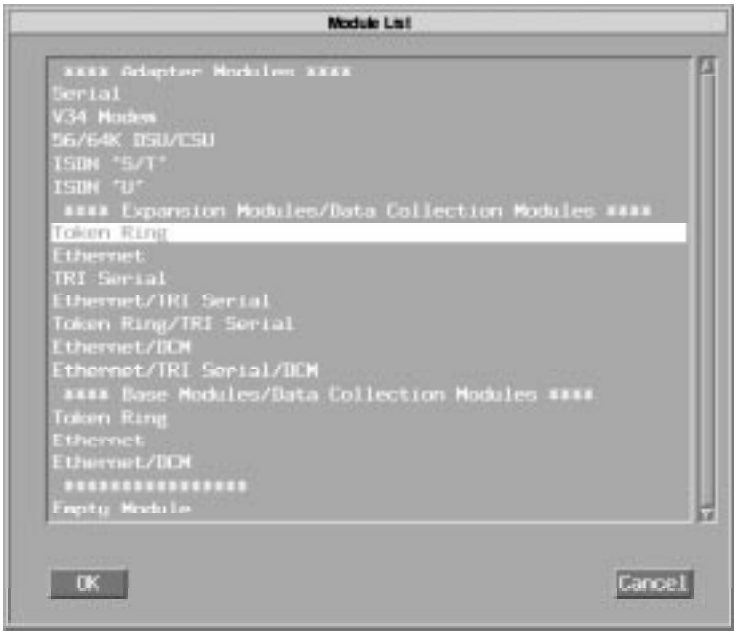

Figure 6. Selecting an ARN Expansion Module

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

    Refer to Figure 1 for the physical location of expansion modules.

14. **Click on OK.**

    The Configuration Manager window appears, now displaying the expansion module interfaces. Figure 7 shows the interfaces for a sample configuration.

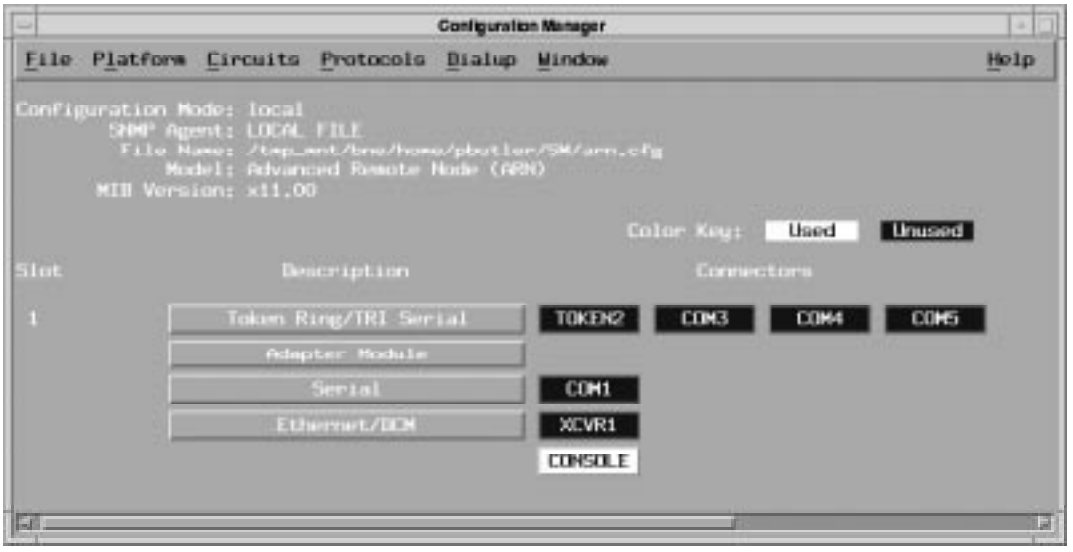

Figure 7. Sample ARN Configuration

Configuring ARN Interfaces

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

For this ARN interface type	Find information here
Ethernet, token ring	The *Configuring Routers* and *Configuring Ethernet, FDDI, and Token Ring Services* guides, or the online help text
Serial, DSU/CSU	The *Configuring Routers* and *Configuring WAN Line Services* guides, or the online help text
ISDN and V.34 Modem	The *Configuring Routers* and *Configuring Dial Services* guides, or the online help text. Note that the section on ISDN BRI services for AN, ANH, and ASN routers in *Configuring Dial Services* also applies to the ARN.

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 7).

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 this default configuration.

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

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

Table 5 lists the default settings for the V.34 console modem.

Table 5. 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 8).

Figure 8. 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 *Configuring Dial Services* for a summary of AT modem initialization commands for the ARN.

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 Prioritization*, Site Manager supports new predefined criterion options (Table 6).

Table 6. New Predefined Criteria for IP Traffic Filters

Criterion Name	Reference Field	Offset	Length	Description
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.

Configuring WAN Line Services

These sections are amendments to Chapter 7 of *Configuring WAN Line Services*:

- Configuring a DS0A Connection
- Setting a Port Loopback Configuration
- Enabling or Disabling Logical Line Loopback

Configuring a DS0A Connection

This section describes how to configure a T1 connection to a QMCT1 w/ DS0A link module to carry SDLC traffic.

Getting Required Information

You need the following information from the subscriber:

- The data rate of the SDLC connection between the IBM host and the CPE (see Figure 9).

  Use this rate to set the Rate Adaption logical line parameter for both the router connecting the host side and the router connecting the remote access side. Valid options are 9.6 or 19.2 Kb/s.

  To establish a connection, the subscriber must match this rate to that of the SDLC connection between the controller and CPE on the remote access side.

- The line encoding settings of both the host and CPE, and the controller and CPE on the remote access side.

  Use these settings to set the NRZI Enabled logical line parameter. Valid options are Enable to configure NRZI (nonreturn to zero inverted) or Disable to configure NRZ (nonreturn to zero).

  The setting of the NRZI Enable parameter on a router connecting a host side is unrelated to and can differ from that connecting a remote access side.

- The NRZI type setting for

  -- The host side if the line encoding settings of the host and CPE do not match.

  -- The remote access side if the line encoding settings of the controller and CPE do not match.

  You need these settings to set the NRZI Type logical line parameter. Valid options are Mark or Space.

  Like the NRZ Enabled parameter, the NRZI Type on a router connecting a host side is unrelated to and can differ from that connecting a remote access side. The subscriber's host and remote access settings can also be different.

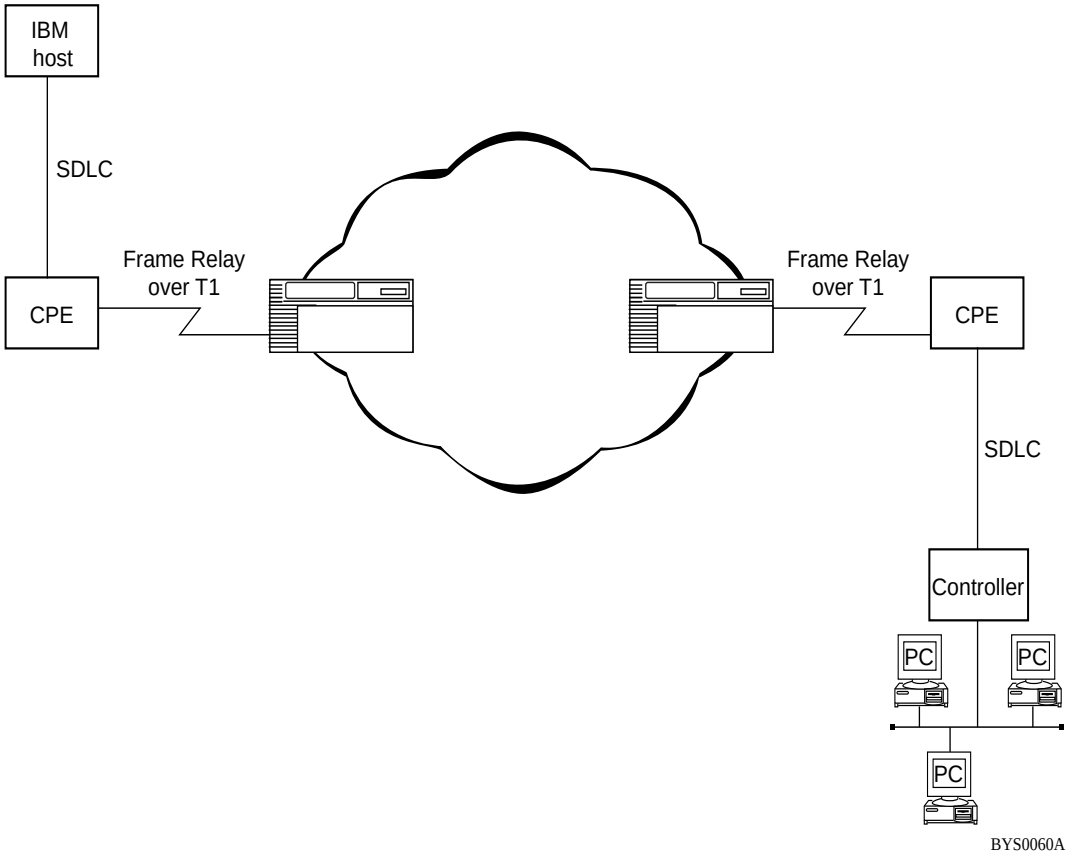

Figure 9. SDLC Connection via Frame Relay over T1 Lines

Setting Site Manager Parameters

To configure a T1 connection to an unconfigured port on a QMCT1 w/ DS0A link module to carry SDLC traffic:

1. **Click on the QMCT1 link module connector.**

   The Port Application window appears.

2. **Click on OK to accept the default value, Non-PRI.**

   The Edit Slot MCT1 window appears.

3. **Click on OK.**

The Slot MCT1 Port Parameters window appears.

4. **Click on OK to accept default port parameters, or edit them first as described in "Configuring MCE1 and MCT1 Ports."**

   The Slot MCT1 Logical Lines window appears.

5. **Click on Add.**

   The Add Circuit window appears.

6. **Click on OK.**

   The WAN Protocols window appears.

7. **Select SDLC and click on OK.**

   The Select Protocols window appears.

8. **Select DLSw and click on OK.**

   The Local Device Configuration window appears.

9. **Enter values for the parameters you want to modify for this SDLC to Frame Relay connection.**

   Click on the Help button or refer to *Configuring DLSw Services* for descriptions of the DLSw Local Device parameters.

10. **Click on OK.**

    The DLS Local Device Configuration window appears.

11. **Click on Done.**

    The DLSw Slot Configuration window appears.

12. **Click on Done.**

    The Slot MCT1 Logical Lines window appears.

13. **Scroll to Rate Adaption and set the value to 9.6 or 19.2 Kb/s.**

    After you set the data rate for an SDLC connection, you may assign only one time slot to the associated logical line.

14. **Scroll to the NRZI Enable parameter and set the value to Enable (for NRZI line coding) or Disable (for NRZ line coding), as given by the subscriber.**

15. **If you enabled NRZI, scroll to the NRZI Type parameter and set the value to Mark or Space frame format, as given by the subscriber.**

Table 7 provides a matrix of supported line encoding configurations.

Table 7. Line Encoding for SDLC Connections

IBM Host	IBM CPE	QMCT1 w/ DS0A Logical Line
NRZI, Mark	NRZ	NRZI, Mark
NRZ	NRZ	NRZ
NRZI, Space	NRZ	NRZI, Space
NRZ	NRZI, Mark	NRZ
NRZI, Mark	NRZI, Space	NRZ

16. **Click on Done.**

Setting a Port Loopback Configuration

Setting the Loopback Configuration parameter places the MCT1 port into loopback mode without a request from remote equipment. Set the loopback configuration by specifying one of the following options:

- Payload Loopback -- Received signals are looped through the T1 framer, then looped back for retransmission. This method maintains bit-sequence integrity for information bits, but does not maintain the integrity of frames or superframes.
- Line Loopback -- Received signals do not go through the framing device before being looped back out. This method ensures minimum penetration.
- No Loopback (the default) -- This option deactivates any current loopback.

Enabling or Disabling Logical Line Loopback

In logical line (*channelized*) loopback mode, the router retransmits received data for specified MCT1 timeslots only. This proprietary, SNMP-based form of loopback passes data through the HDLC controller, and therefore supports only HDLC data. Logical line loopback is disabled by default.

Configuring X.25 Services

The following sections are amendments to *Configuring X.25 Services*:

- Max Idle Parameter for QLLC Service Type
- X.25 Called Address Insertion Enhancement for IPEX
- X.25 Over the ISDN D Channel

Max Idle Parameter for QLLC Service Type

The X.25 Network Service Record parameter Max Idle specifies the maximum number of minutes that a virtual circuit can remain idle. When the Max Idle timer expires, X.25 services clear the circuit. The default value is 2 minutes, except for QLLC Service.

For QLLC Service the default value is 0, which means that the circuit can remain up but idle indefinitely. You may want to consider the cost of remaining connected to the X.25 backbone network while your QLLC sessions remain idle for an extended time.

X.25 Called Address Insertion Enhancement for IPEX

IP Encapsulation of X.25 (IPEX) is one of the X.25 services Bay Networks provides. IPEX allows two X.25 systems to exchange data by tunneling over a TCP/IP network. For further information about IPEX services, refer to *Configuring X.25 Services*.

Currently, many X.25 DTE devices cannot provide the called DTE X.121 address that IPEX requires. X.25 Called Address Insertion is an IPEX enhancement that allows these devices to communicate.

With this feature enabled, when an IPEX device receives an incoming X.25 call request packet that does not include a called DTE X.121 address, the IPEX software searches all the mapping records associated with its circuit interface until it locates a mapping record that is a source type SVC record with an X.121 called address. IPEX uses this mapping record for X.25 to TCP translation, copying the X.121 called address from the mapping record to the call request packet that lacks an X.121 address, and sending the packet to the remote IPEX router to establish the IPEX session.

Configuring X.25 Called Address Insertion

To configure X.25 Called Address Insertion:

1. **From the Configuration Manager, choose Protocols > IPEX > Global.**

   The Edit IPEX Global Parameters window appears.

2. **Edit the DTE Address Insertion parameter, and click on OK.**

Parameter:	**DTE Address Insertion**
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables X.25 Called Address Insertion for IPEX.
Instructions:	Choose Enable to enable address insertion.
MIB Object ID:	1.3.6.1.4.1.18.3.5.15.1.5

X.25 Over the ISDN D Channel

X.25 over the ISDN D channel allows the router to transport X.25 packets without incurring the expense of a leased line. You can use the ISDN line for normal switched service applications as well as for X.25 traffic.

The Bay Networks implementation of X.25 over the ISDN D channel is based on ITU-T (formerly CCITT) recommendation X.31.

How X.25 Over the ISDN D Channel Works

In ISDN terminology, the router behaves like terminal equipment Type 1 (TE1). The software integrates

- The X.25 Packet Layer Protocol (PLP) configured as the data terminal equipment (DTE).
- The ISDN Layer 2 Link Access Procedure on the D Channel (LAPD).
- An X.31 terminal adaptor (TA) that acts as a pseudo-ISDN Layer 3. It mediates between the PLP and the LAPD.

The router establishes an ISDN LAPD packet-mode connection on the D channel with the ISDN network. The X.31 TA mediates between that LAPD connection and the X.25 DTE to access the packet-switching Public Data Network (PSPDN) via the packet handler (PH) that the ISDN network provides.

The X.25 PLP that generates the X.25 packets that travel across the ISDN D channel and the ISDN software must reside on the same slot of the router.

Platforms Supported

X.25 over the ISDN D channel works with AN, ASN, and ARN routers, and with single or quad ISDN/BRI modules only.

Requirements and Limitations

X.25 over the ISDN D channel is subject to the following requirements and limitations:

- A slot configured with X.25 over the ISDN D channel must have both X.25 PLP and ISDN subsystems loaded.
- The maximum packet size is 256 octets (a result of the I-field length limitation of the LAPD information frame).
- The maximum throughput is 9600 b/s.
- This feature does not support ISDN leased lines where the D channel does not exist.
- The router does not prioritize ISDN signaling traffic and the X.25 traffic on the D channel.
- The Bay Networks implementation of X.25 over the ISDN D Channel complies with standards in effect in France, Germany, Spain, and Switzerland. It also works in the United States, which does not require certification.

Using Regular ISDN and X.25 Over the ISDN D Channel

Any slot on the router that you configure with X.25 over ISDN using the D channel can also use regular ISDN. However, dynamically enabling or disabling X.25 over ISDN using the D channel disconnects all active calls of the normal ISDN. Similarly, dynamically changing the ISDN switch-related MIBs (global rate-adaption or incoming call filter attributes) disconnects X.25 over ISDN using the D channel.

Configuring X.25 Over the ISDN D Channel

To configure X.25 over the ISDN D Channel, you must

1. **Configure ISDN.**

   Enable the X.25 Over ISDN-D Channel parameter. You can also edit two other X.25 Over ISDN D parameters.

2. **Configure X.25 on the same slot of the router.**

   If you enable the X.25 Over ISDN-D Channel parameter while you are configuring ISDN, the X.25 Packet Configuration window then automatically opens, followed by the X.25 Service Configuration window, giving you the opportunity to configure X.25.

Refer to *Configuring Dial Services* for information about configuring ISDN and X.25 Over ISDN. Refer to *Configuring X.25 Services* for information about configuring X.25. Refer to the next section, “IPEX and X.25 Over the ISDN D Channel,” for information about using single-node switching with X.25 over the D channel.

IPEX and X.25 Over the ISDN D Channel

The most common implementation of X.25 over the D channel uses IP encapsulation of X.25 (IPEX) single-node switching. You configure IPEX on the backplane of a single router. A normal IPEX configuration performs local X.25 switching, and a circuitless IP network simulates an IP cloud. Figure 10 illustrates this configuration.

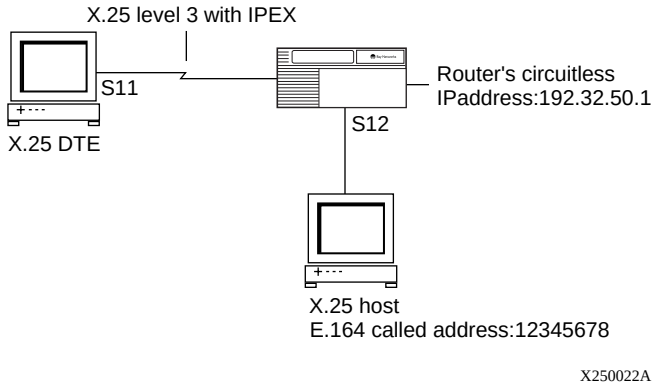

Figure 10. IPEX Single-Node Switching

If the router receives an X.121 called address for an SVC, with the call request coming from the X.25 port, it sends the packet to a TCP destination port and IP address that you choose. For this example, the router sends the packet to the circuitless IP address, or any other IP address on the local router.

If the router receives an incoming TCP/IPEX packet from the configured TCP port number, it sends the IPEX packet out on the X.25 port.

Configuring IPEX Local X.25 Switching

This example assumes that you have already configured a circuitless IP address. For information about configuring IP, refer to *Configuring IP Services*. For information about configuring X.25, refer to *Configuring X.25 Services*.

Configuring the SVC Connection

To configure the SVC connection:

1. **Click on a COM port, and click on OK.**
2. **Choose X.25 from the WAN Protocols menu.**
3. **Click on OK.**

   The X.25 Packet Configuration window appears.

4. **Select a Link Address Type DCE if the COM port connects to a DTE device (for example, an ATM machine). Select a Link Address Type of DTE if it connects to a DCE type device (for example, an X.25 switch).**
5. **Enter a PDN X.121 address.**

   This can be any legal X.121 address, but not the X.121 address that you are using for IPEX mapping (step 14).
6. **Enter the maximum number of logical channels that this interface requires.**
7. **Click on OK.**

   The X.25 Service Configuraiton window appears.
8. **Click on Add.**

   The X.25 Service window appears.
9. **In the Type parameter, click on Values, and choose IPEX as the service type.**
10. **Click on OK.**

    The IPEX Mapping Table Configuration window appears.
11. **Click on Add.**

    The IPEX Mapping Type window appears.
12. **Click on the Values button and select SVC as the Source Connection Type.**
13. **Click on OK.**

    The IPEX Mapping Parameters window for SVC appears.
14. **Enter an E.164 called address.**

    In this example, the address is 12345678.
15. **Accept the default, End_to_End, for the Mapping Type parameter unless you must perform X.121 address translation. Address translation is only possible in Local Mode.**
16. **Enter the Remote IP Address.**

    In this example, the address is 192.32.50.1.
17. **Enter the Remote TCP Port Number.**

This is the destination TCP port number that receives the IPEX packets. For this example, enter 13000 for COM1.

18. **Click on OK. Click on Done.**

    You have completed the IPEX configuration for COM1.

Configuring the TCP Connection

To configure the TCP connection:

1. **Repeat steps 1 to 11 in the previous section,"Configuring the SVC Connection," but select a different COM port.**
2. **Click on the Values button and select TCP as the Source Connection Type.**
3. **Click on OK.**

   The IPEX Mapping Parameters window for TCP appears.

4. **Enter the TCP port number.**

   In this example, the number is 13000.

5. **Accept the default, End_to_End, for the Mapping Type parameter unless you must perform X.121 address translation. Address translation is only possible in Local Mode.**
6. **Click on OK. Click on Done.**

   You have completed the IPEX configuration.

Note: This example allows calls from the X.25 DTE to the X.25 host. To make call requests flow in both directions, you must make the same configuration again, but in the opposite direction. That is, create an SVC mapping type on the X.25 host, and a TCP mapping type on the X.25 DTE. For the second configuration, use a different TCP port. Both mapping types can exist on the same interface.

Connecting AN200 Routers to a Network

The following section is an amendment to *Connecting AN200 Routers to a Network*. The AN200 is available only in Japan.

Customizing the AN200 Software Image

The AN200 software image ships as part of the corporate suite software. Because the AN200 router contains no PCMCIA flash card and a limited amount of fixed flash memory, we recommend that you use the Site Manager Image Builder software to customize the size of the image to include only protocols supported by the AN200. Refer to *Modifying Software Images for Routers* for more information about customizing software images.

The AN200 supports the following protocols:

- IP
- IP RIP
- IPX RIP and SAP
- AppleTalk, AppleTalk RTMP
- Bridge
- Wellfleet HDLC
- PPP
- ISDN (DBU, DoD, and BoD)
- Frame Relay
- Data compression
- Traffic prioritization and traffic filters

Event Messages for Routers and BNX Platforms

Table 8 lists the service and entity names that correspond to the new or amended sections in *Event Messages for Routers and BNX Platforms*.

Table 8. New and Amended Event Messages

Service	Entity	Section	Page
Data link switching	DLS	DLS Warning Event DLS Trace Events	-53 -53
DSU/CSU	DSUCSU	DSUCSU Fault Event DSUCSU Info Events	-55 -56
Fujitsu Network Transmission Systems ATM	FNTS_ATM	FNTS_ATM Fault Event FNTS_ATM Warning Events FNTS_ATM Info Events	-58 -58 -60
Frame Relay	FR	FR Fault Event	-62
Data Encryption			
Key Manager	KEYMGR	KEYMGR Fault Event KEYMGR Warning Events KEYMGR Info Events	-64 -64 -65
WAN Encryption Protocol	WEP	WEP Fault Event WEP Warning Events WEP Info Events	-91 -91 -93
Integrated Services Digital Network	ISDN	ISDN Info Events ISDN Trace Event	-62 -63
Internet Protocol	IP	IP Info Events	
V.34 modem service	MODEM	MODEM Fault Event MODEM Warning Event MODEM Info Events	-66 -66 -67
OSPF	OSPF	OSPF Warning Events OSPF Info Event	-68 -68
Point-to-Point	PPP	PPP Warning Events Revised PPP Trace Events PPP Info Events PPP Trace Events Revised PPP Trace Events	-69 -72 -70 -72 -74

(continued)

Table 8. New and Amended Event Messages *(continued)*

Service	Entity	Section	Page
RADIUS		RADIUS Fault Event RADIUS Warning Events RADIUS Info Events RADIUS Trace Events	-76 -76 -77 -85
X.25/QLLC	QLLC	QLLC Fault Event	-75
Switched services (dial-on-demand, dial backup, and bandwidth-on-demand)	SWSERV	SWSERV Info Events SWSERV Trace Event	-88 -89
Technician Interface	TI	Technician Interface Info Event Messages	-90
Teletype	TTY	TTY Info Event Message	-91

DLS Warning Event

The following is a new Warning 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 Trace 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 states. 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.

Entity Code/Event Code **50/120**

Decimal Identifier **16790136**

Severity: Trace

Message: Received SSP <*name*> frame in <*interface type*>. dl_correlator = <*connection address*>, halt reason code <code>.

Meaning: Indicates that a HALT_DL or HALT_DL_NOACK message was received on an LLC, SDLC, or DLC connection. <*name*> is HALT_DL or HALT_DL_NOACK and <*interface type* > is LLC, SDLC, or DLC.

Action: The message is associated with RFC 1795 and made available with DLSw Version 2. Refer to this RFC for the halt reason codes.

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 Solutions 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 <*slot no.*> COM <*connector_no.*>

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 <*slot no.*> COM <*connector_no.*>

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 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 Solutions 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 can use the FNTS_ATM driver only on FNTS Integrated Nodes.

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 Solutions 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 Solutions 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 Solutions 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 Solutions 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 Fault 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.

ISDN Info Events

The following are new Info event messages for the ISDN service, referred to as the ISDN entity. The entity code assigned to ISDN events is 79.

Entity Code/Event Code **79/21**

Decimal Identifier **16797461**

Severity: Info

Message: X.25 over ISDN D is configured on slot <*slot number*>.

Meaning: X.25 over the ISDN D Channel is configured on the specified slot.

Entity Code/Event Code **79/22**

Decimal Identifier **16797462**

Severity: Info

Message: X.25 over ISDN D is enabled on dsl <*ID_number*>.

Meaning: X.25 over the ISDN D Channel is enabled on the specified DSL (digital subscriber loop).

ISDN Trace Event

The following is a new Trace event message for the ISDN service, referred to as the ISDN entity. The entity code assigned to ISDN events is 79.

Entity Code/Event Code **79/23**

Decimal Identifier **16797463**

Severity: Trace

Message: Starting X.31 TA.

Meaning: The router is starting the X.31 TA.

IP Info Events

The following are new Info event messages for the IP service, referred to as the IP entity. The entity code assigned to IP events is 2.

Entity Code/Event Code **2/147**

Decimal Identifier **16777874**

Severity: Info

Message: IP traffic filter -- Rule <*rule_no*>, interface <*IP_address*>, circuit <*circuit_no*> (Accept packet)
Accepted packet -- src: <*IP_address*>, port: <number>, dst: <*IP_address*>, port: <number>

Meaning: This message provides information on TCP/UDP traffic filters.

Entity Code/Event Code **2/148**

Decimal Identifier **16777875**

Severity: Info

Message: IP traffic filter -- Rule <*rule_no*>, interface <*IP_address*>, circuit <*circuit_no*> (Accept packet)
Dropped packet -- src: <*IP_address*>, port: <number>, dst: <*IP_address*>, port: <number>

Meaning: This message provides information on TCP/UDP traffic filters.

Entity Code/Event Code **2/149**

Decimal Identifier **16777876**

Severity: Info

Message: IP traffic filter -- Rule <*rule_no*>, interface <*IP_address*>, circuit <*circuit_no*> (Accept packet)
Hit packet -- src: <*IP_address*>, port: <number>, dst: <*IP_address*>, port: <number>

Meaning: This message provides information on TCP/UDP traffic filters.

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 Solutions 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: 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 Data 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 Info 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 Event

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 Solutions Center if the modem driver fails to restart.

MODEM Warning Event

The following is a 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 Solutions 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 SCC_INIT (2), make sure that the modem is attached to the correct port. If the failure state is AT_INIT (5), reset the modem configuration in the Site Manager V.34 Modem Interface window. Call the Bay Networks Technical Solutions Center if the modem fails to initialize on restart.

OSPF Warning Events

The following are new Warning event messages for the OSPF service, referred to as the OSPF entity. The entity code assigned to OSPF events is 12.

Entity Code/Event Code **12/119**

Decimal Identifier **16780407**

Severity: Warning

Message: Last neighbor <*IP_address*> is down on interface <*IP_address*>.
src<*IP_address*> interface<*IP_address*>

Meaning: No OSPF neighbor is currently reachable on this interface.

Entity Code/Event Code **12/120**

Decimal Identifier **16780408**

Severity: Warning

Message: C2: Hello Rejected: HELLO RTRID CHANGED\n
src<*IP_address*> RTRID <*IP_address*> -> <*IP_address*>

Meaning: The router ID has been changed since OSPF established an adjacency with this neighbor.

Action: No action required. The adjacency will be reestablished after the dead interval elapses.

OSPF Info Event

The following is a new Info event message for the OSPF Protocol service, referred to as the OSPF entity. The entity code assigned to OSPF events is 12.

Entity Code/Event Code **12/117**

Decimal Identifier **16780405**

Severity: Info

Message: Primary up on slot <*slot_number*>

Meaning: The primary soloist is up on the specified slot.

PPP Warning Events

The following are new Warning 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 **44/213**

Decimal Identifier **16788693**

Severity: Warning

Message: MLC bundle of <*bundle_number*> for Cct <*circuit_number*> does not have line <*line_number*> specified in Session Info.

Meaning: The specified multilink bundle for the specified circuit does not have the line number in the Session Information.

Action: No action required. If you see this message, there will be no RADIUS accounting Stop message for this call.

Entity Code/Event Code **44/223**

Decimal Identifier **16788703**

Severity: Warning

Message: BAP: Port Available Query Failure, Reason: <*text*>.

Meaning: A Bandwidth Allocation Protocol query to find out if a port is available has failed for the specified reason.

Entity Code/Event Code **44/231**

Decimal Identifier **16788711**

Severity: Warning

Message: Terminating call because of unacceptable MRU/MRRU, <*circuit_number*>.

Meaning: The call on the specified circuit is terminating because of an unacceptable MRU value.

Action: Change the MRU value. Refer to the section, “Changing the PPP MRU Size Setting for Routers Running Version 11.02 and Earlier,” earlier in this guide.

Revised PPP Warning Event

Entity Code/Event Code **44/206**

Decimal Identifier **16788686**

Severity: Warning

Message: Initial call for Cct <*circuit_number*> received on Slot <*slot_number*> for the pool NOT configured on this slot.

Meaning: The router received the initial call for the specified circuit on the specified slot for a pool that is not configured on this slot.

Action: Make sure the outgoing phone numbers configured on the remote router correspond to pools on the correct slot of this router.

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: <*circuit_number.*>, 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.

Entity Code/Event Code **44/224**

Decimal Identifier **16788704**

Severity: Info

Message: CHAP Success on line <*line number and instance*> for cct <*circuit_number*>.

Meaning: CHAP is operating on the specified line and circuit.

Entity Code/Event Code **44/225**

Decimal Identifier **16788705**

Message: Authentication Phase complete on line <*line number and instance*> for cct <*circuit_number*>.

Meaning: Authentication has completed successfully on the specified line and circuit.

Entity Code/Event Code **44/226**

Decimal Identifier **16788706**

Message: Received incorrect CHAP response from <*line number and instance*> for cct <*circuit_number*>.

Meaning: The router has received an incorrect CHAP response from the specified line and circuit.

Entity Code/Event Code **44/227**

Decimal Identifier **16788707**

Message: Adding line <*line number and instance*> to cct <*circuit_number*>.

Meaning: The router is adding the specified line and instance ID to the specified circuit.

Entity Code/Event Code **44/228**

Decimal Identifier **16788708**

Message: Link Establishment Phase (multilink | PPP) complete for circuit <*circuit_number*>.

Meaning: The link establishment phase for either multilink or PPP is complete for the specified circuit.

Entity Code/Event Code **44/229**

Decimal Identifier **16788709**

Message: CHAP Failed from <*remote CHAP name*> on <*line number and instance*> for cct <*circuit_number*>.

Meaning: CHAP failed from the remote system on the specified line and circuit.

Entity Code/Event Code **44/230**

Decimal Identifier **16788710**

Message: PAP Failed, incorrect PAP ID <*ID*>' on <*line number and instance*> for cct <*circuit_number*>.

Meaning: PAP failed because of the specified incorrect PAP ID on the specified line and circuit.

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_number*>:, circuit <*circuit_number*>.

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.

Entity Code/Event Code **44/214**

Decimal Identifier **16788694**

Severity: Trace

Message: Sending BAP <*Call Request* | *Call_Status_Indication* | *Link_Drop_Query_Request*>, id: <*ID_Number*>, circuit <*circuit_number*>

Meaning: The router is sending this BAP request message with the given identifier number on the specified circuit.

Entity Code/Event Code **44/215**

Decimal Identifier **16788695**

Severity: Trace

Message: Sending BAP <*Call Response*| *Call_Status_Response*| *Link_Drop_Query_Response*> message, <*ACK* | *NAK* | *FULL_NAK*> id: <*ID_number*>, circuit <*circuit_number*>.

Meaning: The router is sending this BAP response message with the given identifier number, on the specified circuit.

Entity Code/Event Code **44/216**

Decimal Identifier **16788696**

Severity: Trace

Message: Received BAP <*Call Request* | *Call_Status_Indication* | *Link_Drop_Query_Request*> message, id: <*ID_number*>, circuit <*circuit_number*>.

Meaning: The router received this BAP request message with the given identifier number, on the specified circuit.

Entity Code/Event Code **44/217**

Decimal Identifier **16788697**

Severity: Trace

Message: Received BAP <*Call Response*| *Call_Status_Response*| *Link_Drop_Query_Response*> message, <*ACK* | *NAK* | *FULL_NAK*> id: <*ID_number*>, circuit <*circuit_number*>.

Meaning: The router received this BAP response message with the given identifier number, on the specified circuit.

Entity Code/Event Code **44/218**

Decimal Identifier **16788698**

Severity: Trace

Message: Call pkt (<*circuit_number*>): IP <*type of IP packet*>, src=< *IP_address*>, dst= <*IP address*>.

Meaning: The call packet for the specified circuit number is the given IP packet type; it has a source address of <*IP_address*>, and a destination address of <*IP_address*>.

Entity Code/Event Code **44/219**

Decimal Identifier **16788699**

Severity: Trace

Message: Call pkt (<*circuit_number*>): IP <*type of IP packet*>, src= <*IP_address*>, dst= <*IP_address*>

Meaning: The call packet for the specified circuit is the given IP packet type; it has the specified source and destination addresses.

Entity Code/Event Code **44/220**

Decimal Identifier **16788700**

Severity: Trace

Message: Call pkt (<*circuit_number*>): IPX, <*type of IPX packet*>, <*source address*>, <*destination address*>.

Meaning: The call packet for the specified circuit is the given IPX packet type; it has the specified IPX source and destination addresses.

Entity Code/Event Code **44/221**

Decimal Identifier **16788701**

Severity: Trace

Message: Call pkt (<*circuit_number*>): IPv6 <*type of IPv6 packet*>, PPP Protocol ID = <*ID_number*>

Meaning: The call packet for the specified circuit is the given Version 6 IP packet type, with the specified PPP Protocol ID.

Entity Code/Event Code **44/222**

Decimal Identifier **16788702**

Severity: Trace

Message: Call pkt (<*circuit_number*>):PPP Protocol ID = <*ID_number*>

Meaning: The call packet for the specified circuit has the specified PPP Protocol ID.

Revised PPP Trace Events

The following are revised 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 **44/68**

Decimal Identifier **16788548**

Severity: Trace

Message: Received PAP Authenticate-Request on line <*line_number*>, circuit <*circuit_number*>.

Meaning: The router received a PAP Authentication Request message on the specified line and circuit.

Entity Code/Event Code **44/69**

Decimal Identifier **16788549**

Severity: Trace

Message: Received PAP Authenticate-Ack on line <*line_number*>, *circuit* <*circuit_number*>.

Meaning: The router received a PAP Authentication Acknowledgment message on the specified line and circuit.

Entity Code/Event Code **44/203**

Decimal Identifier **16788683**

Severity: Trace (formerly Info)

Message: Attempting to locate <*text string*> in WHOAMI table.

Meaning: The router is attempting to locate the PAP ID or CHAP Name in the WHOAMI table. Either CHAP or PAP may be misconfigured.

Action: Check your configuration of PAP and CHAP.

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 Solutions Center if the router fails to restart.

RADIUS Fault Event

The following is a new Fault event message for the RADIUS service, referred to as the RADIUS entity. The entity code assigned to RADIUS events is 115.

Entity Code/Event Code **115/1**

Decimal Identifier **16806657**

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.

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

RADIUS Warning Events

The following are new Warning event messages for the RADIUS service, referred to as the RADIUS entity. The entity code assigned to RADIUS events is 115.

Entity Code/Event Code **115/2**

Decimal Identifier **16806658**

Severity: Warning

Message: RADIUS gate < *gate number*> failed to allocate buffer

Meaning: The specified gate failed to allocate buffer space.

Action: Check memory utilization and amount of global memory on slot. Call the Bay Networks Technical Solutions Center to help you decide if you need more memory or need to partition existing memory in some other way.

Entity Code/Event Code **115/3**

Decimal Identifier **16806659**

Severity: Warning

Message: RADIUS Master out of unique Accounting ID

Meaning: RADIUS Master could not assign the accounting gate the unique ID it must have to interact with the server. Too many sessions may be active at the same time.

Action: This message will not be issued when sessions go down. Check that all the accounting servers are up.

Entity Code/Event Code **115/4**

Decimal Identifier **16806660**

Severity: Warning

Message: RADIUS Server record not found, leaving UDP dest. port and ip address empty

Meaning: The RADIUS server MIB record has not been created, but RADIUS has been loaded on the slot.

Action: Create the appropriate *wfRadiusServer* entry.

RADIUS Info Events

The following are new Info event messages for the RADIUS service, referred to as the RADIUS entity. The entity code assigned to RADIUS events is 115.

Entity Code/Event Code **115/5**

Decimal Identifier **16806661**

Severity: Info

Message: RADIUS Initializing

Meaning: RADIUS is initializing.

Entity Code/Event Code **115/6**

Decimal Identifier **16806662**

Severity: Info

Message: RADIUS Authentication Service Started

Meaning: The RADIUS authentication service has started.

Entity Code/Event Code **115/7**

Decimal Identifier **16806663**

Severity: Info

Message: RADIUS Accounting Service Started

Meaning: The RADIUS accounting service has started.

Entity Code/Event Code **115/8**

Decimal Identifier **16806664**

Severity: Info

Message: RADIUS Terminating.

Meaning: RADIUS is terminating.

Entity Code/Event Code **115/9**

Decimal Identifier **16806665**

Severity: Info

Message: RADIUS Authentication Disabled on this slot.

Meaning: RADIUS authentication is disabled on this slot of the router.

Entity Code/Event Code **115/10**

Decimal Identifier **16806666**

Severity: Info

Message: RADIUS Authentication Enabled on this slot.

Meaning: RADIUS authentication is enabled on this slot of the router.

Entity Code/Event Code **115/11**

Decimal Identifier **16806667**

Severity: Info

Message: RADIUS Accounting Disabled on this slot.

Meaning: RADIUS accounting is disabled on this slot of the router.

Entity Code/Event Code **115/12**

Decimal Identifier **16806668**

Severity: Info

Message: RADIUS Accounting Enabled on this slot.

Meaning: RADIUS accounting is enabled on this slot of the router.

Entity Code/Event Code **115/13**

Decimal Identifier **16806669**

Severity: Info

Message: RADIUS Authentication Request Message received from gate <*gate ID_number*>.

Meaning: The specified gate has requested authentication services of the RADIUS client.

Entity Code/Event Code **115/14**

Decimal Identifier **16806670**

Severity: Info

Message: RADIUS Authentication Request Message received from line <*line_number*>.

Meaning: The specified line has requested authentication via RADIUS.

Entity Code/Event Code **115/15**

Decimal Identifier **16806671**

Severity: Info

Message: RADIUS Session gate for application gate <*gate ID_number*> died. Sending RADIUS reject message to the application.

Meaning: The RADIUS client process on the specified gate has exited abnormally. The router is sending an access reject to the application that is requesting authentication services from the RADIUS client.

Entity Code/Event Code **115/16**

Decimal Identifier **16806672**

Severity: Info

Message: Session Gate <*Session_ID_number*> assigned UDP source port <*source_port_ID*> by <*IP_address*>.

Meaning: The RADIUS client session has been assigned the specified dynamic UDP source port by the client at the specified Client IP address.

Entity Code/Event Code **115/17**

Decimal Identifier **16806673**

Severity: Info

Message: Session Gate <*session_ID*> failed UDP registration with <*IP address*>.

Meaning: The specified RADIUS client session failed to get a dynamic UDP port and register with the specified client IP address.

Action: Check whether the IP address is enabled or disabled.

Entity Code/Event Code **115/18**

Decimal Identifier **16806674**

Severity: Info

Message: RADIUS Master Soloist Gate Initialized.

Meaning: The RADIUS Master initialization process is complete.

Entity Code/Event Code **115/19**

Decimal Identifier **16806675**

Severity: Info

Message: RADIUS Master Soloist Gate exists on remote slot.

Meaning: RADIUS Master is up on a remote slot.

Entity Code/Event Code **115/20**

Decimal Identifier **16806676**

Severity: Info

Message: RADIUS Master Soloist Gate died.

Meaning: RADIUS Master has come down.

Entity Code/Event Code **115/21**

Decimal Identifier **16806677**

Severity: Info

Message: RADIUS Master Soloist service available.

Meaning: RADIUS Master is now up and running.

Entity Code/Event Code **115/22**

Decimal Identifier **16806678**

Severity: Info

Message: No unique identifier found for this RADIUS session

Meaning: A unique identifier could not be allocated to this RADIUS session.

Action: The maximum number of sessions (255) are up. Wait for an identifier to become available and restart this RADIUS session.

Entity Code/Event Code **115/23**

Decimal Identifier **16806679**

Severity: Info

Message: RADIUS session for gate id <*gate ID_number*> sending access request using identifier <*ID_number*> and client ip address <*IP_address*> to radius server <*server_IP_address*>.

Meaning: The RADIUS session at the specified gate is sending an access request using the specified ID number and client IP address to the specified RADIUS server.

Entity Code/Event Code **115/24**

Decimal Identifier **16806680**

Severity: Info

Message: RADIUS session for line <*line_number*> sending access request using identifier <*ID_number*> and client ip address <*IP_address*> to radius server <*server_IP_address*>.

Meaning: The RADIUS session for the specified line is sending an access request using the specified ID and client IP address to the specified RADIUS server.

Entity Code/Event Code **115/25**

Decimal Identifier **16806681**

Severity: Info

Message: RADIUS client reached the maximum number of simultaneous requests to the server.

Meaning: The RADIUS client has sent the maximum number of simultaneous requests (255) to the server.

Entity Code/Event Code **115/26**

Decimal Identifier **16806682**

Severity: Info

Message: RADIUS Accounting Gate assigned UDP source port <*port_IP_address*>.

Meaning: The RADIUS Accounting gate has been assigned the specified UDP source port address.

Entity Code/Event Code **115/27**

Decimal Identifier **16806683**

Severity: Info

Message: RADIUS Accounting Gate failed <*cause_code*> UDP registration with <*IP_address*>.

Meaning: The RADIUS Accounting gate failed during UDP registration at the specified IP address for the reason given.

Entity Code/Event Code **115/28**

Decimal Identifier **16806684**

Severity: Info

Message: All RADIUS Accounting server/s down.

Meaning: All RADIUS Accounting servers are down.

Action: Check RADIUS accounting servers.

Entity Code/Event Code **115/29**

Decimal Identifier **16806685**

Severity: Info

Message: RADIUS <*Accounting/Authentication*> server <*IP_address*> failed to respond.

Meaning: The specified RADIUS server failed to respond.

Entity Code/Event Code **115/30**

Decimal Identifier **16806686**

Severity: Info

Message: RADIUS Client IP Address <*IP_address*> is up for slot <*slot_ID*>.

Meaning: The RADIUS Client's IP address is active for the specified slot.

Entity Code/Event Code **115/31**

Decimal Identifier **16806687**

Severity: Info

Message: RADIUS Client IP Address <*IP_address*> is not up.

Meaning: The RADIUS client's IP address is not up.

Entity Code/Event Code **115/32**

Decimal Identifier **16806688**

Severity: Info

Message: RADIUS client setting timer to wait <*number*> seconds for a response from the server.

Meaning: The RADIUS client's timer is set to wait for the specified number of seconds for a response from the server.

Entity Code/Event Code **115/33**

Decimal Identifier **16806689**

Severity: Info

Message: No response received for access request identifier <*ID_number*>.

Meaning: The router has received no response to the specified access request.

Entity Code/Event Code **115/34**

Decimal Identifier **16806690**

Severity: Info

Message: Access request identifier <*request_ID_number*> current retry count is <*number_of_retries*>.

Meaning: The router has sent the specified access request the number of times this message indicates.

Entity Code/Event Code **115/35**

Decimal Identifier **16806691**

Severity: Info

Message: Maximum retries for access request id <*request_ID_number*> , attempting to find alternate server.

Meaning: The router has sent the specified access request the maximum number of times allowed and is now attempting to find an alternate RADIUS server.

Entity Code/Event Code **115/36**

Decimal Identifier **16806692**

Severity: Info

Message: RADIUS session <*ID_number*> received an access <*Accept/Reject*> from server <*IP_address*>. RADIUS session id <*ID_number*> complete, authentication <*successful|failed*>.

Meaning: The specified RADIUS session has received an access Accept|Reject of <number> from the server with the IP address of <IP address>. The RADIUS session with the specified ID has completed authentication successfully|unsuccessfully.

Entity Code/Event Code **115/37**

Decimal Identifier **16806693**

Severity: Info

Message: RADIUS Accounting Gate terminating

Meaning: The RADIUS accounting gate is terminating.

Entity Code/Event Code **115/38**

Decimal Identifier **16806694**

Severity: Info

Message: RADIUS Accounting Response received for <*ID_number*>.

Meaning: The router has received a RADIUS accounting response for the specified ID number.

Entity Code/Event Code **115/39**

Decimal Identifier **16806695**

Severity: Info

Message: RADIUS Accounting Request being sent for <*ID_number*>.

Meaning: The router is sending an accouting request for the specified ID number.

RADIUS Trace Events

The following are new Trace event messages for the RADIUS service, referred to as the RADIUS entity. The entity code assigned to RADIUS events is 115.

Entity Code/Event Code 115/40

Decimal Identifier

Severity: Trace

Message: RADIUS Server %d.%d.%d.%d MIB record has been modified.

Meaning: The RADIUS server MIB wfRADIUS Server Entry with the specified IP address has been modified.

Entity Code/Event Code 115/41

Decimal Identifier

Severity: Trace

Message: RADIUS wfRadiusEntry MIB record added.

Meaning: The specified RADIUS MIB record has been added.

Entity Code/Event Code 115/42

Decimal Identifier

Severity: Trace

Message: RADIUS Server added to the list of possible RADIUS servers.

Meaning: The router has added the RADIUS Server with the specified IP address to the list of possible RADIUS servers.

Entity Code/Event Code 115/43

Decimal Identifier

Severity: Trace

Message: RADIUS MIB Entry record modified.

Meaning: The RADIUS MIB wfRADIUS Entry record has been modified.

Entity Code/Event Code 115/44

Decimal Identifier

Severity: Trace

Message: Using RADIUS Server <*IP address*> found active.

Meaning: The specified RADIUS server is active.

Entity Code/Event Code 115/45

Decimal Identifier

Severity: Trace

Message: State of RADIUS server <*IP address*> is down. Searching for next active server.

Meaning: The specified RADIUS server is down. The router is searching for an active server.

Entity Code/Event Code 115/46

Decimal Identifier

Severity: Trace

Message: Valid RADIUS Response Authenticator, accepting response.

Meaning: The router has received a valid RADIUS authentication response, which it is accepting.

Entity Code/Event Code 115/47

Decimal Identifier

Severity: Trace

Message: Auth request received, ip_state and/or client state is false

Meaning: The router has received an authentication response, but it cannot process it. The reason is that the client IP address is not up.

Entity Code/Event Code 115/48

Decimal Identifier

Severity: Trace

Message: Rejecting Auth Req: primary server MIB record not found

Meaning: The router is rejecting an authentication request because it cannot locate the primary server MIB record.

Entity Code/Event Code 115/49

Decimal Identifier

Severity: Trace

Message: Rejecting Auth Req: primary server <*IP_address*> is disabled.

Meaning: The server is rejecting an authentication request because the primary server at the specified IP address is disabled.

Entity Code/Event Code 115/50

Decimal Identifier

Severity: Trace

Message: RADIUS server <*IP_address*> specified by application in Auth Req

Meaning: The authentication request sent by the application specifies the RADIUS server IP address <*IP_address*>.

Entity Code/Event Code 115/51

Decimal Identifier

Severity: Trace

Message: No MIB record for RADIUS server <*IP_address*>, ignoring application request

Meaning: The router is ignoring an application record because it lacks a MIB record for the RADIUS server specified by the application.

Entity Code/Event Code 115/52

Decimal Identifier

Severity: Trace

Meaning: RADIUS: radius_get_nwif_gh: returned cause <*cause_code*>

Meaning: RADIUS attempted to get the IP networking interface process ID. A cause_code value of 1 indicates that it succeeded.

Entity Code/Event Code 115/53

Decimal Identifier

Severity: Trace

Message: RADIUS: ip_nwif_alive: returned cause <*cause_code*>

Meaning: RADIUS attempted to discover if the networking interface is alive. A cause_code value of 1 indicates that it is alive.

Entity Code/Event Code **115/54**

Decimal Identifier

Severity: Trace

Message: RADIUS Client failed to register with <*IP_address*>, status <*status_code*>.

Meaning: The RADIUS client failed to register the UDP port with the client IP address.

Entity Code/Event Code **115/55**

Decimal Identifier

Severity: Trace

Message: Invalid message <*message_ID*> received by Accounting Gate

Meaning: The accounting gate received a buffer it was not expecting, or that was malformed.

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.

Entity Code/Event Code **58/165**

Decimal Identifier **16792229**

Severity: Info

Message: ISDN Call Connected from <*text*> to <*text*>, Channel B <*channel_number*>, Call ID <*ID_number*>, DSL <*DSL_number*>.

Meaning: This message describes the ISDN connection.

SWSERV Trace Event

Entity Code/Event Code **58/166**

Decimal Identifier **16792230**

Severity: Trace

Message: Any of the following messages can appear:

Received Request msg for additional bandwidth for circuit <circuit_number>.

Received Acknowledgement msg for additional bandwidth for circuit <circuit_number>.

Received Nack msg for additional bandwidth for circuit <circuit_number>.

Received Termination Request msg for additional bandwidth for circuit <circuit_number>.

Received Termination Ack msg for additional bandwidth for circuit <circuit_number>.

Received Forced Request msg for additional bandwidth for circuit <circuit_number>.

Received Forced Termination Request msg for additional bandwidth for circuit <circuit_number>.

Received Port Availability Query msg for additional bandwidth for circuit <circuit_number>.

Received UNKNOWN msg for additional bandwidth for circuit <circuit_number>.

Sent Request msg for additional bandwidth for circuit <circuit_number>.

Sent Acknowledgement msg for additional bandwidth for circuit <circuit_number>.

Sent Nack msg for additional bandwidth for circuit <circuit_number>.

Sent Termination Request msg for additional bandwidth for circuit <circuit_number>.

Sent Termination Ack msg for additional bandwidth for circuit <circuit_number>.

Sent Forced Request msg for additional bandwidth for circuit <circuit_number>.

Sent Forced Termination Request msg for additional bandwidth for circuit <circuit_number>.

Sent Port Availability Query msg for additional bandwidth for circuit <circuit_number>.

Sent UNKNOWN msg for additional bandwidth for circuit <circuit_number>.

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 Solutions 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) is 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.

Modifying Software Images for Routers

The following section is an amendment to *Modifying Software Images for Routers.*

ARN Software Image

The *Modifying Software Images* guide omits the name and location of the software image for the ARN platform. Table 1-1 in *Modifying Software Images* should include the following information:

Router	Router Software Image	Device the Image Runs On
ARN™	arn.exe	Flash Single Inline Memory Module (SIMM)

Information in the manual on using the Image Builder applies to the ARN as to any other router platform.

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 the 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
- DCM Hardware Dependencies for the ARN Router
- DCM Software Image and Router Software Compatibility
- BOOT and Diagnostic PROM Upgrades for 11.02

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_141.obj

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

```
Image Name is 1:in11_141.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
```

DCM Hardware Dependencies for the ARN Router

The Ethernet DCM board installed in an ARN router must have a Revision D or later part number.

To determine the hardware revision of a DCM installed in an ARN router:

1. **At the Technician Interface prompt, enter the following command:**

   [1:TN]$ list -i wfDCMEntry

   The Technician Interface displays the instance identifier of the DCM entry. For example:

   ```
   inst_ids  = 1
   ```

2. **Use the *inst_ids* result in the following get command:**

   [1:TN]$ get wfDCMEntry.wfDCMhwRev.1

   The Technician Interface displays the hardware revision of the DCM board. For example:

   ```
   wfDCMEntry.wfDCMhwRev.1 = "D"
   ```

3. **If the revision reported is C or earlier, you must upgrade the hardware to a revision D or later DCM.**

Refer to *Release Notes for Router Software Version 11.02* for additional information.

DCM Software Image and Router Software Compatibility

Router Software Version 11.02 ships with the Version 1.4.1 Ethernet DCM software image. The Version 1.4.1 DCM software image is backwards-compatible with Router Software Versions 9.0*x* and 10.0*x*.

To run RMON on an ARN router, you must upgrade the following:

- DCM software image to Version 1.4.1
- Router software to Version 11.02
- ARN Boot PROM to Version 1.17
- Diagnostic PROM to Version 1.30

If you have an AN or ANH router running router software version 11.00 or later, we also recommend that you upgrade to the Version 1.4.1 DCM software image. However, the AN and ANH routers will operate with the Version 1.4 DCM software image.

Before you attempt to upgrade a router to Version 11.0, we recommend that you first check the version of DCM software residing on the DCM.

To determine the version number of the DCM software image, enter the following command from the Technician Interface:

[1:1]$ get wfDCMmw.wfDCMAgentImageVersion.0

The Technician Interface displays a message similar to the following:

```
wfDCMmw.wfDCMAgentImageVersion.0 = "V1.4.1"
```

BOOT and Diagnostic PROM Upgrades for 11.02

Table 9 shows the routers that require a new version of boot and diagnostic PROMs for Router Software Version 11.02. Upgrade the PROMs if the features you need depend on a PROM version more recent than the version now in your router.

Table 9. Boot and Diagnostic PROMs for Router Software Version 11.02

Router Model	Boot PROM Version	Boot PROM File Name	Reason for Upgrading PROM	Diagnostic PROM File Name	Diagnostic PROM Version
AN	9.00b	*anboot.exe*	Upgrade diagnostic PROM to support csudsu adapter module	*andiag.exe*	V7.26
AN200	11.01	*an200boot.exe*	New hardware platform support	*an200diag.exe*	V1.00
ARE	11.00	*areboot.ppc*	New hardware platform support	*arediag.ppc*	V1.12
ARN	V1.17	*arnboot.exe*	Support for ARN platform and miscellaneous bug fixes	*arndiag.exe*	V1.30
ARN_PDBROM.ROM	-----	------	Support for PDB diagnostics for the ARN platform	*arndiag.exe*	V1.06
ASN	10.00	*asnboot.exe*	N/A	*asndiag.exe*	V2.24
BN	8.10	*freboot.exe*	N/A	*frediag.exe*	V4.10
VME	8.11	*vmeboot.exe*	N/A	None	None
ARE s5000	11.00	*s5000boot.exe*	N/A	*S5000diag.exe*	V0.04

Using the Bay Command Console

The following sections describe changes to *Using the Bay Command Console*:

- Interface Updates
- Errata
- BN Installation Example

Interface Updates

The following sections describe updates to using the BCC.

Configuration Command Responses

If you receive an error message in response to a BCC configuration command, you can use the Technician Interface **history** command as well as the command recall and editing keys to review and edit your entries.

To review the command history list, enter **tic history** at any BCC prompt, as shown in the following example:

```
ip>  tic history
     1  bcc-trial
     2  ip
     3  info
     4  help
     5  tic history
```

For more information about the **history** command, refer to *Using Technician Interface Software*. For more information about using command recall and editing keys, refer to the following sections in Chapter 2 of *Using the Bay Command Console*:

- Recalling Commands
- Editing Commands

Modified Attribute Names

Two special attributes visible in BCC-trial (11.01) were **group** and **subprotocols**. The names of these BCC attributes have changed, as follows:

- **group** is now **on**
- **subprotocols** is now **has**

On -- Identifies the parent of the current object. For example, ethernet/2/1 is configured *on* the box object (denoted by the bcc> prompt).

Has -- Just as a directory has files in a file system, an object in the BCC configuration system *has* other objects. For example, ethernet/2/1 *has* ip/1.2.3.4.

Since *on* and *has* can be attributes of any configurable object, you can get the current value of *on* or *has* by entering those attribute names at the current configuration prompt, and then pressing the Return key.

Note: The value of the **has** attribute can sometimes be an extensive list of objects (for example, a large number of ospf policies). A long list of this kind would require you to scroll through multiple BCC screens to see the values for the remaining configurable attributes of the current object. For this reason, the **has** attribute does not appear in any list of attributes generated by the BCC **info** command. To get the value of the **has** attribute for any object, enter **has** at the current prompt and press Return.

BCC Underscore Prompt

Some command symbols normally used in pairs to denote the beginning and the end of a list of data elements produce the underscore (or continuation) prompt; the symbols are braces {...}, brackets [...], and quotes "...". For example:

```
box> { ...
box_  ...}
box>
```

or

```
box> [...
box_  ...]
box>
```

or

```
box> "...
box_  ..."
box>
```

The BCC displays the underscore prompt after you type an opening symbol {, [, or " because it is expecting data plus the corresponding closing symbol, },], or ". If you inadvertently type one of the opening characters, just type the appropriate closing character to restore the ">" prompt.

Errata

These sections describe corrections that apply to *Using the Bay Command Console*.

Saving and Sourcing Command Listings

If you log in to the AN or BN platform from a UNIX workstation, PC, or MAC using Telnet or terminal emulation, you can use the native capabilities of that platform to

- Save the output of the BCC **show config** command from the screen to an ASCII file
- Save a sequence of manually entered BCC commands to an ASCII file

By capturing commands to a file from either source, you can then

- Edit the commands using a suitable ASCII text editor
- Add to the file comments that describe details of the configuration (see *Using the Bay Command Console*
- Save the edited file for later use
- Use the BCC **source** command to revise the active configuration of Bay Networks devices of the same type and hardware configuration (see also "Displaying the Total Device Configuration" in Chapter 2 and "Sourcing Configuration Commands from a File" in Chapter 3 of *Using the Bay Command Console*

Note: If you edit ASCII files containing BCC commands, you must adhere to BCC syntax requirements. This includes any commands necessary to navigate to each level of the device configuration tree, where you may want to add, modify, or delete objects in the existing device configuration.

Configuration Error Messages

The sections "Discovering the Sequence of Required Attributes for an Object" (Chapter 2) and "Creating a New Configuration" (Chapter 3) describe command usage messages incorrectly. For example, the following message appears in Chapter 2:

```
bcc> ethernet
ERROR: Required attribute "slot" was not specified for class: Ethernet.
```

Chapter 4 correctly describes the latest BCC command usage error messages, which have the format shown in the following example:

```
bcc> ethernet
Required attribute "slot" was not specified for class: Ethernet.
Usage: "ethernet slot <value> connector <value>"
Or:    "ethernet <slot>/<connector>"
bcc>
```

Router Configuration Tree -- Telnet Modifications

Figure 1-2 in *Using the Bay Command Console* shows a "telnet" object and a dependent "client" (telnet client) object. Both objects are accessible at the same (root or bcc>) level of the router configuration tree. You do not configure the "client" *on* "telnet" in this release of BCC-trial.

Other Corrections

The following corrections apply to Chapter 1:

- Figure 1-2 shows a "trusted-host" object under global IP access policies. Release 11.02 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 11.02. 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 11.02 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:
     board ethernet fddi hssi sync tokenring virtual
     ip client ftp ntp snmp telnet tftp console
```

  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 srml).
- 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 11.02 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 11.02.
- 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 adjhost 192.168.10.2**	Add IP (address 192.168.10.1) and an 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 adjhost 192.168.4.2**	Add IP (address192.168.4.1) and an 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.

BN Installation Example

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	**Comments**
bcc> **info**	Check the chassis (box) type.
build-location "int/11.02/38" build-date ""Thu May 22 19:39:28 EDT 1997"" verbose 0 type frecn	"frecn" = Bay Networks BCN router
bcc> **show config**	Check the board configuration inside the router.
box type frecn board slot 5 type sync	• Quad Synchronous link module in slot 5
cwc .. board slot 7 type srml	• System Resource Module in slot 7
cwc .. board slot 9 type dtok	• Dual Token Ring link module in slot 9
cwc .. board slot 11 type wffddi2m	• Multimode FDDI link module in slot 11
cwc .. board slot 13 type qenf	• Quad Ethernet with Filters in slot 13
console portnum 1 state enabled prompt {"[%slot%:1]$ "} auto-manager-script {automgr.bat} auto-user-script {autouser.bat} cwc ..	• Console device on port 1

Prompts, Commands, and Responses	Comments
bcc> **ethernet slot 13 connector 1**	Choose a port (interface type, slot, and connector) for the initial IP interface to the router.
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.	Check to see what you can configure at this level.
Configurable objects in this context: ip	You can configure (modify) values currently assigned to attributes of ethernet/13/1, or you can add IP to this interface.
ethernet/13/1> **ip 192.168.133.114**	Add IP (address 192.168.133.114) to ethernet/13/1.
ip/192.168.133.114> **info** group {ethernet/13/1} state enabled	Check values currently assigned to attributes of IP on this interface.
sub-protocols {arp/192.168.133.114/1}	BCC automatically enabled ARP on this interface.
address 192.168.133.114 mask 255.255.255.0	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.
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	

Prompts, Commands, and Responses	Comments
ip/192.168.133.114> **mask 255.255.255.224**	Modify the subnet mask for ip/192.168.133.114.
ip/192.168.133.114> **info mask** 255.255.255.224	Check the value currently assigned to the mask attribute.
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 checksuming on this interface. Configurable objects in this context: rip ospf rdisc arp igmp	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** 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.	Check to see what you can configure next at this level.
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** group {snmp} label public access readonly	Check the values currently assigned to community “public.”
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	Comments
community/public> **manager** Required attribute "address" was not specified for class: SnmpManager. Usage: "manager address <value>" Or: "manager <address>")	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.
community /public> **manager 0.0.0.0**	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.)
manager/public/0.0.0.0> **telnet** telnet>	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.
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: Timout in minutes on Password entry. prompt: Specifies the prompt to use. state: State enable disable.	Check to see what you can configure next at this level.
Configurable objects in this context: client	You can configure (modify) values currently assigned to attributes of Telnet, or you can add the Telnet client.
telnet> **client**	Add the Telnet client.

Prompts, Commands, and Responses	Comments
client> **tftp** tftp>	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.
tftp> **info** group {box} state enabled default-volume 2	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.
tftp> **default-volume 5**	Change the default volume to 5.
tftp> **ftp** ftp>	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.
ftp> **info** group {box} state enabled default-volume 2	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.
ftp> **def 5** ftp>	Entering only “def” and a value (abbreviated syntax for **default-volume 5**), change the default volume number to 5.
ftp> **def** default-volume 5	Verify the change to the **default-volume** number, again using abbreviated syntax.

Prompts, Commands, and Responses	Comments
ftp> **show config**	Check the total configuration of the device to this point.
box type 16896	
board type 80 slot 5	• Added Synchronous link module in slot 5
board-type sync	
cwc ..	• Moved back one level
board type 8448 slot 7	• Added a System Resource Module in slot 7
board-type srml	
cwc ..	• Moved back one level
board type 176 slot 9	• Added a Dual Token Ring link module in slot 9
board-type dtok	
cwc ..	• Moved back one level
board type 192 slot 11	• Added a FDDI link module in slot 11
board-type wffddi2m	
cwc ..	• Moved back one level
board type 162 slot 13	• Added a Quad Ethernet with Filters in slot 13
board-type qenf	
cwc ..	• Moved back one level
console portnum 1	• Added the console device on port 1
state enabled	
prompt {“[%slot%:1]$ “}	
auto-manager-script {automgr.bat}	
auto-user-script {autouser.bat}	
ethernet slot 13 connector 1	• Defined the ethernet interface on connector 1 of slot 13
state enabled	
circuit-name E131	
ip address 192.168.133.114	• Added IP (address 192.168.133.114) on ethernet/13/1
state enabled	
mask 255.255.255.224	
assocaddr 0.0.0.0	
arp	• BCC added ARP on ip/192.168.133.114
state enabled	
cwc ..	• Moved back one level
rip address 192.168.133.114	• Added RIP on ip/192.168.133.114
state enabled	
cwc ..	• Moved back one level
cwc ..	• Moved back one level
cwc ..	• Moved back one level
ip	• 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.
state enabled	
arp	• BCC added global ARP for the same reason.
state enabled	
cwc ..	• Moved back one level
cwc ..	• Moved back one level

Prompts, Commands, and Responses	Comments
snmp state enabled	• Added SNMP globally to the router
community label public access readwrite manager address 0.0.0.0 cwc ..	• 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
cwc ..	• Moved back one level
telnet state enabled manager-script automgr.bat	• Added Telnet globally to the router
client state enabled cwc ..	• Added client to the global Telnet object • Moved back one level
cwc ..	• Moved back one level
tftp state enabled default-volume 5	• Added TFTP globally to the router, with default volume = 5
cwc ..	• Moved back one level
ftp state enabled default-volume 5	• Added FTP globally to the router, with default volume = 5
cwc ..	• Moved back one level
cwc ..	• Moved back one level
ftp>	
	The command shows the total device configuration in terms of BCC syntax (commands and data), and returns you to the current context.
ftp> **cwc**	Return to root level or context.
bcc> **tic save config base_114.cfg**	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.
bcc> **tic ping 192.168.133.114** IP ping: 192.168.133.114 is alive (size = 16 bytes)	Test the intial 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	Comments
bcc> **tic ping 192.168.133.97** IP ping: 192.168.133.97 is alive (size = 16 bytes)	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.
bcc> **exit**	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*:

- ip routes
- enable/disable dcm
- show dcm
- show dls stats
- show fr demand
- show fr [circuits | service]
- show ipx
- show isdn
- show radius
- show ppp
- show sws
- show sync
- show wep
- show x25

ip routes

To display Equal Cost Multipath (ECMP) routes, you must use the **ip routes** command. You cannot view ECMP routes using the **show ip routes** command.

Sample Display - ip routes

```
Network/Mask        Proto        Age Slot     Cost  NextHop Address AS
------------------- ------ --------- ---- --------- --------------- >-----
0.0.0.0/0           OSPF         920    2    126992 192.32.174.97
0.0.0.0/0           OSPF         920    2    126992 192.32.174.98
1.0.0.0/8           OSPF       82825    2    126984 192.32.174.97
1.0.0.0/8           OSPF         920    2    126984 192.32.174.98
10.0.0.0/8          OSPF         920    2    127000 192.32.174.97
10.0.0.0/8          OSPF         920    2    127000 192.32.174.98
132.245.0.0/16      OSPF         920    2    126992 192.32.174.97
132.245.0.0/16      OSPF         920    2    126992 192.32.174.98
134.177.0.0/16      OSPF         920    2    126992 192.32.174.97
```

enable/disable dcm

The **enable/disable dcm** script was renamed from **enable/disable dcmmw** for Router Software Version 11.01 and later. 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. It provides 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
Create Matrix Control Table: Disabledmiddleware	

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: V1.4.1

Boot Option: Down Load
Image Name: 1:in11_141.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 *DCMMW.mib*.
Operational Status	Current state of the DCM (up or down).
Module Type	Type of DCM (Ethernet).
Memory Size	Size, in bytes, of the DCM board's memory.
Hardware Revision	Revision of the DCM hardware.
Firmware Revision	Revision of the DCM firmware.
Agent Image Version	Version of the Agent Image running on the DCM.

Boot Option	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	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	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	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	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	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: V1.4.1

Boot Option: Down Load
Image Name: 1:in11_141.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: Disabledmiddleware
```

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 dls stats

The **show dls stats** command now displays the source and destination service access point (SSAP and DSAP) fields.

Sample Display - show dls stats

```
DLSw statistics
---------------

                     Destination MAC/  Remote IP/  DSAP/Tx-IFrames/ Tx-RNRs
Circuit Status       Source MAC        local IP   SSAP/ Rx-IFrames  Rx-RNRs
-------- ---------- ----------------  ------------- ---- ---------- --------
S12      Established 40-00-00-03-17-22 154.154.154.15 0x040      0
                     40-00-00-00-00-D1 78.78.78.78    0x04  0          0
```

show fr demand

The **show fr** (show frame relay statistics) command supports a new **demand** option, as follows:

show fr demand [<*line*> | <*line.llindex*>]

This command displays information about all or some of the Frame Relay demand lines configured on the router.

<*line*> limits the display to the specified line identifier.

<*line.llindex*> limits the display to the specified instance identifier.

Line	LLIndex Line or instance identifier for the Frame Relay interface.
Circuit	Name of the main Frame Relay circuit this interface is associated with.
Mgt Type	See **show fr alerts** command.
Intf Type	Interface type: Normal (leased service with no backup service), Primary/Shared (the backup circuit uses the primary configuration), Primary/Secondary (the backup circuit uses its own configuration.
Status	See **show fr alerts** command. In addition to those listed, Status is Disabled (by a user).
Faults	Number of times the interface has been in fault status.
Discard	Number of outbound frames discarded because of errors.
Drop	Number of inbound frames dropped because of errors.

Sample Display - show fr demand

```
Line.LLIndex      Circuit   Mgt Type  Intf Type  Status  Faults  Discard  Drop
---------------  --------  --------- ---------  -------- ------ -------- ------
1010000002.0      FR Dema-  AnnexD    Demand     Init          0        0      0
nd 2
1 entry found
```

show fr [circuits | service]

The **show fr** [**circuits** | **service**] command output now includes information on Frame Relay demand circuits. (See the“Circuit” column in the following sample display.)

<*line*> limits the display to the specified line identifier.

<*line.llindex*> limits the display to the specified instance identifier.

<*line.llindex.cct*> limits the display to the specified circuit.

Sample Display - show fr circuits

```
Line.LLIndex.Cct Circuit   Status  Num VCs Default Multiline Name
---------------- -------- -------- ------- ------- --------- -----------------
1010000002.0.2   FR Dema- Active   1       Yes     No        1010000002.0.2
nd 2
1010000002.0.3   1010000- Active   1       No      No        1010000002.0.3
002.0.3
2 entries found
```

For more information on the **show fr circuits**|**service** commands, refer to *Using Technician Interface Scripts*,

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
----------------------------------------

             Incoming                    Callback
 Index     Phone Number      Sub-Addr  Circuit Number
 ----- -------------------- ---------- --------------
     1           5084361003       None              4

Total of    1 Incoming Phone Entries found.
```

show ppp

The following options are new for the **show ppp** script command.

show ppp multilink circuits

Displays information about PPP multilink circuits. The Configured Mode includes a new option, Dynamic-Monitor. The display includes the following information:

Circuit	Name of the circuit.
Configured Mode	Mode you configured for this circuit: • Normal - a nonmultilink circuit • ML - a multilink circuit • Monitor - The circuit is a multilink circuit, and the router for which this circuit is configured is the congestion monitor. • Dynamic-Monitor - The circuit is a multilink circuit using BAP. This option enables the router to function as the monitor when it initiates a call, and the non-monitor router when it receives a call.
Actual Mode	Actual mode in which this circuit is operating.
Tx Packets	Number of packets transmitted over the circuit.
Rx Packets	Number of packets received over the circuit.
Fragmented Packets	Number of packets that were fragmented.

Sample Display - show ppp multilink circuits

```
PPP Multilink Circuits

----------------------

          Configured                        Num Packets

Circuit      Mode       Actual Mode   Tx Packets  Rx Packets  Fragmented

 --------- --------------- -------------- ----------- -----------
Nept_BAP  Dynamic-Monitor Inactive      4432       863          0

Homer_MP  ML_Monitor      Inactive      0          0            0

Homer_T1  ML_Monitor      ML_Monitor    27481      109918       0

Bart_PPP  Normal          Normal        0          0            0
```

show ppp bacp

Displays information about BAP. The display includes the following information:

Circuit Number	Number of the circuit
Circuit Name	Name of the circuit
State	State of the circuit
No Phone Num Option	Whether the circuit is using the No Phone Number Option
Stats Record	Whether a statistics record is available

Sample Display - show ppp bacp

```
[2:1]$ show ppp bacp
PPP: BACP Information
----------------------
Cct#  Circuit        State    No PhoneNum Option  Stats Record
 ----- ------------- --------  ------------------- ------------
     2 Neptune_BAP   Starting  Disabled            None
     3 Bart_BAP      Starting  Disabled            Available
     4 Homer_MP      Disabled  Disabled            None
     5 Moe_BAP       Disabled  Disabled            None
     7 Homer_Sync    Disabled  Disabled            None
     8 Homer_T1      Opened    Disabled            Available
```

show radius

The **show radius** *<option>* commands display information about RADIUS. For detailed information about the Bay Networks implementation of RADIUS, refer to *Configuring RADIUS*.

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

alerts	statistics authentication *<slot_number>*
server	statistics accounting *<slot_number>*
config	version

alerts

Displays the server alerts. The table includes the following information:

IP Address	Server IP address
Mode	Indicates that the server is configured for authentication, accounting, or both
Type	Indicates that this server is primary or alternate
Auth State	Authentication up or down
Acct State	Accounting up or down

Sample Display - show radius alerts

```
RADIUS Server Alerts

--------------------

IP Address       Mode      Type     Auth State   Acct State

-------------- --------- ---------- ------------ ------------

192.168.131.53  Both      Primary    Down         Up


Total of 1 alert on configured server.
```

server

Displays information about the RADIUS server. The table includes the following options:

<*authentication*> limits the display to authentication information

<*accounting*> limits the display to accounting information

server authentication

Describes the state of the authentication servers. It includes the following information:

Server IP Address	Specifies the server's IP address.
Mode	Indicates that the server is configured for authentication, accounting, or both.
Type	Indicates that this server is primary or alternate.
State	Indicates that the server is up or down.
UDP Port	Specifies the authentication UDP port.
Response Timeout	Specifies the number of seconds the RADIUS client waits before retransmitting a request to the RADIUS server.
Max Retry	Specifies the number of times the RADIUS client retransmitted a request.
Reset Timer	Specifies the number of minutes the RADIUS client waits before retrying the primary server after it fails to respond. If the primary server fails to respond, the client considers it unreachable and switches to the alternate server. After this specified time period, the client tries to reconnect to the primary server.
Automatic Reset	Indicates whether the server can reset automatically.
Secret	Specifies the RADIUS password that the server and client share.

Sample Display - show radius server auth

```
RADIUS Server Information for Authentication
--------------------------------------------

  IP Address       Mode      Type      State  UDP Port
-------------- --------- ---------- -------- --------
192.32.77.11     Both      Primary    Up       1645
192.168.131.34   Both      Alternate  Up       1645


    Server               Response   Max.     Reset  Automatic
  IP Address       Mode   Timeout    Retry    Timer    Reset       Secret
-------------- --------- -------- -------- -------- --------- --------------
192.32.77.11     Both      3        2        10       Disabled  bayeast
192.168.131.34   Both      3        2        3        Disabled  bayeast

Total of 2 Authentication servers configured.
```

server accounting

Describes the state of the accounting servers. It includes the following information:

Server IP Address	Specifies the server's IP address.
Mode	Indicates that the server is configured for authentication, accounting, or both.
Type	Indicates that this server is primary or alternate.
State	Indicates that the server is up or down.
UDP Port	Specifies the authentication UDP port.
Response Timeout	Specifies the number of seconds the RADIUS client waits before retransmitting a request to the RADIUS server.
Max Retry	Specifies the number of times the RADIUS client retransmitted a request.
Reset Timer	Specifies the number of minutes the RADIUS client waits before retrying the primary server after it fails to respond. If the primary server fails to respond, the client considers it unreachable and switches to the alternate server. After this specified time period, the client tries to reconnect to the primary server.
Automatic Reset	Indicates whether the server can reset automatically.
Secret	Specifies the RADIUS password that the server and client share.

Sample Display - show radius server account

```
RADIUS Server Information for Accounting
-----------------------------------------

  IP Address       Mode      Type      State  UDP Port
--------------- --------- ---------- -------- --------
192.32.77.11      Both      Primary    Up       1646
192.168.131.34    Both      Alternate  Up       1646


    Server                Response   Max.     Reset  Automatic
  IP Address       Mode   Timeout    Retry    Timer    Reset       Secret
--------------- --------- -------- -------- -------- --------- --------------
192.32.77.11      Both      3        2        10       Disabled  bayeast
192.168.131.34    Both      3        2        3        Disabled  bayeast

Total of 2 accounting servers configured.
```

config

Displays the RADIUS configuration. The table includes the following information:

Slot	Slot number on the router.
Client IP Address	Client IP Address.
Auth Status	Whether authentication is enabled or disabled.
Acct. Status	Whether accounting is enabled or disabled.
Acct. Direction	Which calls generate an accounting session. All indicates that incoming and outgoing calls can establish an accounting session. Outgoing indicates that only outgoing calls can establish an accounting session. Incoming means that only incoming calls can establish an accounting session.
Debug Level	Level of RADIUS debug messages logged by the RADIUS client.

Sample Display - show radius config

```
RADIUS Slot Information
-----------------------
Slot     Client        Auth.    Acct.    Acct.     Debug
       IP Address     Status   Status  Direction   Level
---- --------------- -------- -------- --------- ----------
4    192.168.131.40  Enabled  Enabled  All       No Debug(4)
5    192.168.131.40  Enabled  Enabled  All       No Debug(4)

 RADIUS configured on 2 slots
```

stat auth

Display the RADIUS authentication statistics. The table includes the following information.

<*slot number*> limits the display to the specified slot

Server IP Address	IP address of the RADIUS server
Auth. Req. Count	Number of authentication session requests
Auth. Req. Outstanding	Number of authentication session requests outstanding
Auth. Resp. Accepted	Number of authentication responses accepted
Auth. Resp. Rejected	Number of authentication responses rejected
Auth. No Resp.	Number of authentication requests that received no response
Auth. Resp. Invalid	Number of invalid authentication responses
Auth. Resp. Timeouts	Number of times the client has tried to retransmit a request to the server
Alt. Server Retries	Number of times the client has tried to connect to an alternate server

Sample Display - show radius stat auth

```
RADIUS Authentication Statistics Information

-----------------------------------------

Server      Auth. Req.  Auth. Req. Auth. Resp Auth. Resp

  IP Address       Count   Outstanding  Accepted   Rejected

-----s---------- ---------- ----------- ---------- ----------

192.168.131.34           2           1          0          2

192.168.131.51           0           0          0          0

192.168.131.53           1           0          0          0



   Server         Auth.    Auth. Resp Auth. Resp Alt. Server

  IP Address     No Resp.     Invalid   Timeouts    Retries

--------------- ---------- ----------- ---------- -----------

192.168.131.34           0           0          0           0

192.168.131.51           0           0          0           0

192.168.131.53           0           0          3           1
```

radius stat acc

Display the RADIUS accounting statistics. The table includes the following information.

<*slot_number*> limits the display to the specified slot

Server IP Address	IP address of the RADIUS server
Acct. Req. Start	Number of accounting session requests
Acct. Req. Stop	Number of accounting sessions that have ended
Acct. Resp.	Number of times the accounting server has responded to a request
Acct. Resp.Timeouts	Number of accounting response timeouts that have occurred
Acct. Resp. Failed	Number of times the accounting response has failed
Alt. Server Retries	Number of times the client has tried to connect to the alternate server

Sample Display - show radius stat acc

```
Server      Acct. Req. Acct. Req. Acct. Acct. Resp Acct. Resp Alt. Server
  IP Address       Start      Stop    Resp   Timeouts    Failed Retries
--------------- ---------- ---------- ----- ---------- ---------- -----------
192.168.131.34           0          0     0          0 0          0
192.168.131.51           0          0     0          0 0          0
192.168.131.53           0          0     0          0 0          0

     Total               0          0     0          0 0          0

 RADIUS statistics displayed for 3 servers
```

version

Displays the RADIUS version.

Sample Display - show radius version

```
RADIUS.BAT Version: 1.1 Date: 02/12/97 .
```

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-called       15        5

 Total of    1 Dial OnDemand Callback Circuits.
```

show sync

The **show sync** command has the following new subcommand options:

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. The display includes the following information:

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	Current V.54 loopback operating state of the interface. States are • 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 to avoid 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	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 • 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.

Sample Display - show sync dsucsu_stats

```
                          Out of     Out of     Loss of
             Op       Service   Service    Frame      Line       Total
Slot Conn   State     Status    Errors     Errors     Errors     Errors
---- ---- ---------- ---------- -------    ------     -------    ------
1    2    normal     LOL        0          0          855        855
1 entry(s) found
```

dsucsu_config

Displays configuration information about a DSU/CSU module installed in a BayStack AN, ANH, or ARN router. The display includes the following information:

Hardware Revision	Hardware revision of the DSU/CSU module.
Software Revision	Firmware revision of the DSU/CSU module.
Opmode	Type of Telco service: 56K DDS1 or CC 64K.
Transmit Clock	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)	Whether the 64K Transmit Monitor is enabled. The Transmit Monitor suppresses data to prevent unintended duplication of network control codes.

Sample 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
```

modem_state

Displays status information about a V.34 Modem adapter module installed in a BayStack ARN router The display includes the following information:

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	Current state of modem initialization. States are • Startup (1) • SCCInit (2) • GetInfo (3) • SetDefaults (4) • Initialization (5) • PhoneNumber (6) • Loopback (7) • InitComplete (8)
Line State	Current operational state of modem interface. States are • Unknown (1) • On Hook (2) • Off Hook (3) • Connected (4) • Busied Out (5) • Reset (6)

Sample 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. Modems that do not display this information will display *N/A* (not applicable).
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 - 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 about the Bay Networks implementation of encryption services, refer to *Configuring Data 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 changes in the value of the Traffic Encryption Key (TEK)
TEK Update Rate (seconds)	Number of seconds between changes in the value of the TEK

Sample Display - show wep circuits

```
WEP Circuit Entries
-------------------

 Circuit Circuit           Cipher  TEK Update Rate  TEK Update Rate
  Name    Number  Enable    Mode       (bytes)        (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 changes in the value of the Traffic Encryption Key (TEK)
TEK Update Rate (seconds)	Number of seconds between changes in the value of the TEK

Sample Display - show wep lines

```
WEP Line Entries
----------------

   Line      LL                                Cipher  TEK Upd Rate TEK Upd Rate
  Number   Index Slot Module Conn   Enable     Mode     (bytes)     (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 changes in the value of the Traffic Encryption Key (TEK)
TEK Update Rate (seconds)	Number of seconds between changes in the value of the TEK

Sample Display - show wep vcs

```
WEP Virtual Circuit Entries
---------------------------

                                                 Actual
   Line      LL             Vc   Connection     Cipher
  Number   Index Cct Name   Id      State       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      LL             Vc    # Bytes     # Bytes
  Number   Index Circuit    Id   Encrypted   Decrypted
---------- ----- -------- ----- ----------- -----------
    202101     0      S21     0           0           0


   Line      LL             Vc    # Bytes     # Bytes
  Number   Index Circuit    Id   Encrypted   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

QLLC is a new 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.

<slot.connector> limits the display to the specified slot and connector.

The table includes the following information:

Slot.Connector.Line.LLIndex	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

```
                                LCN's    Services
Protocol Slot.Connector.Line.LLIndex Configured 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.
```

qllc maps

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

Cct	Circuit of the QLLC connection
State PID	Protocol ID used in the first byte of the call user data of the X.25 call request packet
Adjacent X.121 Address	X.121 address of the device that connects to the interface running the QLLC/X.25 software
Partner X.121 Address	X.121 address of the device that connects through the DLSw network
Adjacent MAC Address	MAC address assigned to the QLLC device
Partner MAC Address	MAC address assigned to the SNA device
Adjacent SAP Address	SAP address associated with a communication subsystem on an adjacent device
Partner SAP Address	SAP address associated with a communication subsystem on a partner device
PU Type	Type of the adjacent SNA node
Gen XID	Whether the Gen XID parameter is enabled or disabled.
Node ID	Identifies the node
Map Name	Name of the QLLC mapping entry
Option	Specifies when to forward an XID to the adjacent device
Trace	Type of debugging enabled

Sample Display - QLLC Address Mappings

```
State       Adjacent X121  Adjacent MAC aSAP PU Type Node ID  Option
Circuit   PID         Partner  X121  Partner  MAC pSAP GenXID  Map Name Trace
-------- ----------- -------------- ------------ ---- ------- -------- ------
xvc5.3.2 Active      1111122222      40000000DEAD 0x04 PU 2.0  00171182 0x0000
*05103.0 0xCB        3333344444      4000C1024264 0x04 Disable Lab3174  0x0FF1

xvc5.2.2 Active      3333344444      4000C1024264 0x04 PU 2.0  (nil)    0x0001
*05102.0 0xCB        1111122222      40000000DEAD 0x04 Disable Host     0x0FF1


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 Power-up Diagnostic Option
- Secure Shell Commands
- Loadmap Command Privilege Levels

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>*]

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

AN and ANH Power-up Diagnostic Option

You can use the **set** command on AN and ANH routers to disable or reenable the power-up diagnostics.

set [*-P0* | *P1*]

set -P0	The router skips power-up diagnostics at subsequent restarts.
set -P1	The router executes all power-up diagnostics at subsequent restarts.

Pressing the Reset button on the back panel of the AN for more than 5 seconds initiates a cold boot; power-up 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 about these commands, refer to *Configuring Data Encryption Services*.

Loadmap Command Privilege Levels

The Technician Interface on AN and BN platforms now supports User as well as Manager level access to the **loadmap** command. (For information about the **loadmap** command, type **help loadmap** at the Technician Interface prompt, or refer to *Using Technician Interface Software*.)