Configuring Data Encryption Services

BayRS Version 12.00
Site Manager Software Version 6.00

Part No. 117386-A Rev. A
September 1997

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Bay Networks, Inc. Software License Agreement

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

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

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

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

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

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

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

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

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

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

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

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

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

Contents

Figure

About This Guide

If you are responsible for configuring and managing Bay Networks® routers, read this guide to learn how to configure data encryption.

If you want to	Go to
Learn about data encryption services	Chapter 1
Read implementation notes	Chapter 2
Start encryption services	Chapter 3
Obtain information about Site Manager parameters (this is the same information you obtain using Site Manager online Help)	Appendix A
Learn about k commands	Appendix B

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (refer to the installation manual that came with your router).
- Connect the router to the network and create a pilot configuration file (refer to *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Bay Networks Site Manager and router software. For instructions, refer to *Upgrading Routers from Version 7–11.xx to Version 12.00.*

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.
ellipsis points	Horizontal (. . .) and vertical (⋮) ellipsis points indicate omitted information.
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.

Acronyms

ANSI	American National Standards Institute
BRI	Basic Rate Interface
DES	Data Encryption Standard
DLCI	data link connection identifier
DTR	data terminal ready
ISDN	Integrated Services Digital Network
LTSS	long-term shared secret
MD5	Message Digest 5
MEK	Master Encryption Key
MIB	management information base
NPK	Node Protection Key
NTP	Network Time Protocol
pcfs	personal computer file system
PPP	Point-to-Point Protocol
PVC	permanent virtual circuit
PRI	Primary Rate Interface
RNG	random number generator
SEO	strong encryption option
TEK	Traffic Encryption Key
WAN	wide area network
WEP	WAN Encryption Protocol

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

The Bay Networks Press catalog is available on the World Wide Web at *support.baynetworks.com/Library/GenMisc*. Bay Networks publications are available on the World Wide Web at *support.baynetworks.com/Library/tpubs*.

Bay Networks Customer Service

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

Region	Telephone number	Fax number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 508-916-8880 (direct)	508-916-3514
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

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

How to Get Help

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

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

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	800-2LANWAN	508-916-3514
Santa Clara, CA	800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

Chapter 1
Data Encryption Overview

Bay Networks data encryption services enable you to protect sensitive traffic on your network. Encryption prevents unauthorized persons from reading, changing, or replaying data that travels between Bay Networks routers.

Data encryption services include

- Software-based encryption for PPP dedicated links for the BN®, AN®, ARN™, ASN™, System 5000 router modules, and all serial interfaces. This includes encryption on multiline and multilink.
- Software-based encryption for Frame Relay circuits that have one permanent virtual circuit (PVC) per service record. This include encryption on multiline.
- Encryption configurable on a line or circuit basis.
- Encryption independent or combined with data compression.

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.

Data Encryption Architecture

Bay Networks uses the following standards and protocols to provide encryption services:

- Data Encryption Standard (DES)
- Message Digest 5 (MD5)
- WAN Encryption Protocol (WEP), proprietary to Bay Networks

Data Encryption Standard (DES)

Bay Networks bases encryption services on DES, which the United States government has adopted to protect sensitive but nonclassified data. The American National Standards Institute (ANSI), the IETF, and various banking and financial standards groups have also incorporated DES into security standards.

DES describes the process that transforms 64-bit blocks of data from readable *plaintext* to scrambled *ciphertext*. A 40-bit or 56-bit number that you generate, known as a *key,* controls the scrambling and unscrambling. Both ends of a link must use the same key value for one end to be able to decrypt the data that the other end sends.

DES is designed so that even if someone knows some of the plaintext data and the corresponding ciphertext, there is no way to determine the key without trying all possible keys. The strength of encryption-based security rests on the size of the key, and on properly protecting the key.

Because DES is a public standard, the encryption is secure only if the communicating routers and the management station keep the DES key secret and protected from unauthorized change.

40-Bit and 56-Bit Encryption Strengths

Bay Networks offers two encryption strengths:

- The standard router software includes encryption that uses 40-bit keys. This version provides reasonably strong security.
- We also offer a strong encryption option (SEO) that uses 56-bit DES keys.

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

Message Digest 5 (MD5)

MD5 is a secure hash algorithm, and is a component in a number of IETF standard protocols. MD5 operates on data of varying lengths, and produces from it a single 128-bit output called the *digest*. It is very difficult, given one message and its digest, to fabricate another message that has the same digest. This property enables MD5 to function like a checksum to detect errors in the integrity of a message. When a message that contains a secret key is hashed, the resulting digest also authenticates the origin of the message: only a source that possesses the secret key could have calculated the digest. This technique is called keyed MD5.

Bay Networks encryption uses MD5 to

- Authenticate the originator of the message, that is, to verify that the source possesses the secret key
- Verify the integrity of the DES keying material
- Create new keys as part of a process that changes key values

WAN Encryption Protocol (WEP)

WEP employs the DES algorithm, combined with MD5 and the appropriate key, to encrypt data and add protocol information the receiver requires to identify the data as encrypted.

WEP begins by establishing the security of the link and verifying that both ends have the same key. The two sides of the link issue connection request and acknowledgment messages. They use keyed MD5 to exchange and authenticate these messages. If the negotiation fails, data communication does not occur on that circuit.

Security and Data Encryption

To use data encryption effectively, you must take precautions to protect the security of your network equipment and the configuration process.

Site Security

Carefully restrict access to routers that encrypt data and the workstations you use to configure encryption. Because DES is a public standard, data is secure only if you properly protect the encryption keys. The configuration files that contain these keys include safeguards to prevent unauthorized access. However, the best strategy is to physically protect your equipment.

Configuration Security

Bay Networks recommends that you store the key management files that our encryption services use on removable media, such as floppy disks, and that you store this media in a secure place. This is the easiest way to prevent unauthorized persons from gaining access to these files.

You should always configure the NPKs locally, not over a network. When you connect a computer to a router's console port to configure encryption, use a computer that is not connected to any other equipment.

You can configure LTSSs remotely because LTSSs are encrypted.

Note further recommendations about network security in the following sections of this guide.

Encryption Keys

Figure 1-1 illustrates the hierarchy of secret keys that Bay Networks encryption uses to protect and transmit data.

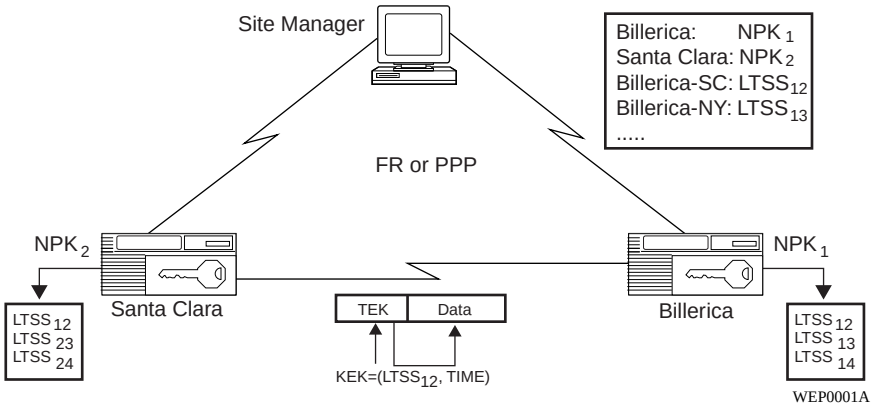

Figure 1-1. Hierarchy of Encryption Keys

The keys are the

- Node Protection Key (NPK). It encrypts the LTSS.
- Long-Term Shared Secret (LTSS). It is the sourcefor the Master Encryption Key.
- Master Encryption Key (MEK). It encrypts the Traffic Encryption Key.
- Traffic Encryption Key (TEK). The TEK encrypts the data that travels across the network.

Random Number Generators (RNGs)

RNGs generate values for the keys. These values are statistically random. An RNG uses as its source a *seed* that you supply. Refer to “Creating Seeds” in Chapter 3 for instructions.

Site Manager uses two of the RNGs to generate NPKs and LTSSs. The router uses the third RNG to generate TEKs.

Node Protection Key (NPK)

The NPK encrypts and decrypts LTSSs.

Caution: The NPK is the most critical key in the hierarchy. If the NPK is compromised, all encrypted data on the router could be compromised. Protect the files that store the NPKs, preferably by using removable media that you store securely. Also protect the routers on which the NPKs reside.

The NPK is stored in the router's nonvolatile memory and its *fingerprint* is in the MIB. The NPK and its fingerprint must match for encryption to occur.

The process of generating and using NPKs is as follows:

1. The key management software uses an RNG in Site Manager to generate as many NPKs as your network requires, and you specify a name for each NPK.
2. You use the Technician Interface to enter an NPK in the router's nonvolatile RAM. You do this for each secure router.
3. You enter the same NPK in the Site Manager Frame Relay or PPP Node Protection Key parameter for that router.

Bay Networks recommends that you create and use a different NPK for each secure router on your network.

Generating an NPK

To generate an NPK you must

1. Use the WEP software to create a seed that initializes the random number generator for the NPKs.
2. Use the WEP Key Manager on Site Manager to generate NPKs.

Entering the NPK on the Router

You enter the NPK into a router locally via the console port and the secure shell section of the Technician Interface. A password protects access to the secure shell. Both the NPK and the secure shell password are stored in the router's nonvolatile memory. You cannot access the NPK or the password via the MIB or by using normal Technician Interface debug commands. You cannot invoke the secure shell in a Telnet session.

The easiest way to enter the NPK is to use a text editor in read-only mode to display the contents of the file that contains your NPKs. Examples of editors include vi or emacs on a UNIX platform and EDIT on a PC. Copy the value of the appropriate NPK, and paste it into the Technician Interface command line.

Note: We recommend that you enter the NPK in each router using a laptop computer that you attach directly to the router. You should not use a terminal server to enter the NPK because of security risks.

Choosing a Secure Shell Password

The Secure Shell password protects all of the secret data in the router that WEP uses. Select a password of at least 10 to 12 characters. Do not use anything obvious, like your nickname, family birthdates, or your social security number. Change this password often and randomly.

Entering the NPK into Site Manager

You also enter the NPK into Site Manager using the Frame Relay or PPP Node Protection Key parameter. When you enter an NPK, it is visible only until you exit the Configuration Manager. You must reenter the NPK each time you modify the security configuration for a router. If you do not enter the NPK exactly as you entered it when you configured encryption initially, you cannot make changes.

Long-Term Shared Secret (LTSS)

The Long-Term Shared Secret is the source for the Master Encryption Key (MEK). It consists of 128 to 248 bits of secret data that each end of a secure link shares. The LTSS resides in the MIB, encrypted by the NPK, which you must have previously entered into Site Manager. You need a different LTSS for each circuit that you configure to use encryption.

The key manager uses an RNG to generate LTSSs, and you specify a name for each of these values. You thereby create a file of LTSS keys and then assign the same key to each end of a secure circuit.

Note: Store the files of NPKs and LTSSs on removable media, such as floppy disks, and store that media in a safe place.

Master Encryption Key (MEK)

The MEK encrypts the Traffic Encryption Key (TEK). The LTSS for a circuit, combined with the current time, is the source of its MEK. You do not actually generate, enter, or view the MEK. The WEP software automatically calculates this value. Like the LTSS, the MEK must be the same on each end of a link.

An MEK periodically changes according to the value of the MEK Change parameter.

For the encryption software to generate identical MEKs, and for the MEKs to remain identical on both sides of a link as their values change, they must change at approximately the same time. That can only happen if

- The MEK Change parameter is set to the same value on each end of a link. For more information on configuring this key change attribute, refer to Appendix A, “Encryption Parameters.”
- The clocks on both routers are synchronized. For further information about router clocks in relation to encryption, see the section “Synchronizing Router Clocks” in Chapter 2.

Traffic Encryption Key (TEK)

The TEK encrypts the data that travels across the network. The RNG on a transmitting router creates the TEK. WEP then encrypts the TEK, using the MEK. At the receiving router, WEP decrypts the TEK, and uses it to decrypt the data.

The TEK that the standard encryption software generates is 40 bits long. The Strong Encryption Option (SEO) can generate both 40-bit and 56-bit TEKs.

The TEK automatically changes according to the values in the TEK Change Time and TEK Change Bytes parameters. A sending router generates a new TEK, and WEP encrypts it. The receiving router notes the change, decrypts it, replaces the old TEK with the new one, and uses the new one to decrypt current and future data until the TEK changes again.

Each router has its own TEK and TEK Change attributes that it uses to protect data that it sends. A link therefore has two TEKs which are different, and which change independently of each other. For more information on configuring key change attributes, refer to Appendix A, “Encryption Parameters.”

Chapter 2
Implementation Notes

This chapter describes special issues that you may encounter in configuring and running encryption.

Requirements for Enabling Encryption

To configure encryption, you must configure WEP parameters and either Frame Relay or PPP encryption parameters. You must enable encryption for both the line and circuit WEP parameters, and for either Frame Relay or PPP.

If you enable encryption for the line and circuit, but not for a protocol, data does not travel over the network.

If you enable encryption for the line, circuit, and protocol, and some other attribute for encryption is misconfigured, WEP drops data rather than sending it unencrypted.

Selecting Encryption Strength

Both sides of a link must use the same encryption strength. Note that you can select both encryption strengths, enabling a router that has 56-bit encryption strength to use 40-bit encryption with a router that has only 40-bit encryption.

Synchronizing Router Clocks

The Master Encryption Key must be the same at both ends of a link. Therefore, the MEK Change parameter value, which sets the amount of time between changes in the value of the MEK, must also be the same. For these values to be the same routinely, the MEK changes must occur at approximately the same time, which requires that the routers use the same date and time. If the routers' clocks differ by more than the MEK Change value, WEP drops all packets.

You can use the Network Time Protocol (NTP) to synchronize the routers. You can also set the MEK Change parameter to a value large enough to accommodate differences between the routers' clocks.

Using Encryption with AN Routers

AN router models earlier than Version 8.12/2.12 lose both date and time if they are powered off. Newer models have a battery that maintains the router clock. If your AN has a model number in the format AE *xxxxxxx*, it is a new, BayStack™ AN, and it has the battery.

To use encryption with older ANs, you must synchronize the router clocks before you configure encryption.

Caution: You should disable Telnet access of any kind between secure routers. If anyone changes the date on either of the routers, traffic stops.

Encryption and Performance

Using encryption requires substantial resources, and reduces router throughput. Carefully select the interfaces on which you use encryption. You can partially lower the cost of using encryption by using data compression with encryption.

Using Data Compression with Encryption

You can configure both hardware- and software-based data compression over Frame Relay and PPP networks running encryption.

Enabling compression improves bandwidth efficiency by eliminating redundant strings in data streams. This, in turn, improves network response times and reduces line costs. Hardware compression is particularly effective in improving a router's throughput when you use encryption.

When you use encryption with compression, the software compresses the data before it encrypts it.

To use data compression, refer to *Configuring Data Compression Services.*

Using an NPK

Your configuration file includes a fingerprint of the NPK. The NPK in the MIB must match the NPK in the router's nonvolatile memory, or encryption cannot occur. This means that if you want to change anything in your encryption configuration after you have exited from the original configuration session, you must reenter the NPK exactly as you entered it initially.

If you install a new CPU board on a router, or swap boards between routers, you must reenter the NPK on the affected routers.

The NPK remains on a board that you remove from a router using data encryption. For security reasons, you need to plan ahead to make sure that an NPK you are using resides only on a router that carries encrypted traffic.

Using Floppy Disks to Store Key Files

For security reasons, Bay Networks recommends that you use removable media such as floppy disks to store key files. You can use the same floppy disks on both PCs and UNIX platforms if you have UNIX *personal computer file system* (pcfs) compatibility, which allows UNIX platforms to access data on floppy disks formatted for PCs. Issue the following series of commands:

1. **Log on as superuser.**

   % **su**

2. **Enter the superuser password.**

   password **<password>**

3. **Move to the root file system.**

   $ **cd /**

4. **Make a mount point directory.**

   $ **mkdir <*directory_name*>**

5. **Mount the floppy disk.**

   $ **mount -t pcfs /dev/fd0 <*directory_name*>**

Configuring Encryption with Dial Backup

You can configure a Frame Relay PVC that uses encryption with a PPP dial backup circuit. If the primary line fails, traffic travels unencrypted over the PPP backup circuit.

PPP dial backup does not work with PPP circuits that you configure for encryption. Further, if a PPP primary circuit includes values in any PPP encryption parameters, whether or not the circuit uses encryption, PPP dial backup does not work.

Frame Relay dial backup does not work with Frame Relay circuits that you configure for encryption.

Chapter 3
Enabling Encryption

This chapter describes how to configure data encryption.

Before You Begin

Before you can start data encryption, you must

1. Create and save a configuration file that has at least one PPP or Frame Relay interface.
2. Retrieve the configuration file in local, remote, or dynamic mode.
3. Specify router hardware if this is a local mode configuration file.
4. Reboot the router.

Using the MIB Object ID

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify parameter values you enter. Entering an invalid value can corrupt your configuration.

Starting Encryption

To use Bay Networks data encryption on your network, you must

1. Create the seeds that the RNG uses as source values for the NPKs and LTSSs.
2. Create an NPK for each secure router.
3. Create an LTSS for each secure line or interface.
4. Enter an NPK on each secure router via the console interface.
5. Create the seeds that are source values for TEKs.
6. Enter the NPK in the Frame Relay or PPP Node Protection Key parameter.
7. Enter the LTSS in the Frame Relay or PPP LTSS Name and LTSS Value parameters.

You can also customize encryption by editing the Frame Relay or PPP encryption parameters, as well as the WEP line and interface parameters.

Creating Seeds

You create seeds to initialize the RNGs that generate keys, using a PC or UNIX platform on which you have installed Site Manager.

Site Manager 6.00 includes software that enables you to create these seeds. The software includes a default length of 128 bits for the LTSS key generator. Site Manager for the PC also includes an environment variable that defines the location where the files that will contain the NPKs and LTSSs reside. On a UNIX platform, you must set this path.

You must create three seeds to use encryption on your network. The RNGs on Site Manager use two of these seeds to generate random numbers for the NPKs and LTSSs. The RNG on a secure router uses the third seed to generate a TEK.

The following sections provide information about creating seeds for the NPKs and LTSSs. The section “Creating TEKs,” later in this chapter, describes how to create the seed for a TEK.

Creating Seeds on a PC

To use a PC to create seeds that the WEP software uses to generate NPKs and LTSSs, issue the **wfkseed** command at the DOS prompt. Default values exist for the key file path and the length of the LTSS key. If you want to change these values, do so before you create the seeds.

Changing the Path to the Key Files

WF_KEY_FILE_PATH is an environment variable that resides in the *\windows\siteman.ini file*. It defines the location, or directory path, for WEP to write the seeds, and from which Site Manager can both retrieve the seeds, and write the generated keys to LTSS and NPK files. The default value of the path is *n:*, where *n* is removable media.

If you want to change the storage place for your key files, use an editor such as Notepad to edit the *WF_KEY_FILE_PATH* line.

Note: Store the files containing NPKs and LTSSs on removable media, such as floppy disks, and store that media in a safe place.

Changing the Length of the LTSS Key Generator

You can set the length of the LTSSs to a value other than the default of 128 bits by editing the *WF_LTSS_KEY_GEN_LEN* line in the *\windows\siteman.ini* file. Use an editor such as Notepad. You can enter a value from 128 to 248.

Running the wfkseed Command

The **wfkseed** command creates the seed that enables WEP to generate random numbers. You run this command twice to create seeds for both the NPKs and the LTSSs.

1. **At the DOS prompt, enter**

   wfkseed

   WEP asks

   ```
   Do you wish to create the LTSS or NPK Key File? [LTSS]:
   ```

2. **Press Return to create the LTSS key file.**

   WEP displays this message:

   ```
   Enter the path of the key path:
   ```

3. **Enter**

   <n>:

   n is the removable disk you are using to store the key files.

   WEP then displays this message:

   ```
   To initialize the seed for the cryptographic random number generator,
   please now enter a series of characters which you would consider to
   be 'random.'  As you enter them, dots '.' will be displayed to
   indicate progress.  If your string is not 'random' enough, questions
   '?' will be displayed.  In that case, modify the pattern you are
   entering.  When enough data is input, you will be prompted to stop
   (near 3 lines of input)...
   ```

4. **Type a series of random characters.**

   The screen displays a dot for each 5 keystrokes that WEP accepts.

   ```
   .... .... .... .... ....

   .... .... .... .... ....

   .... .... .... ..
   ```

   If your keystrokes are not random enough, the screen displays ???

   After you enter a sufficient number of random keystrokes, WEP displays a completion message, and returns you to the prompt.

   ```
   All done, thank you!
   ```

5. **Enter the wfkseed command again to generate the NPK key file.**

   WEP asks

   ```
   Do you wish to create the LTSS or NPK Key File? [LTSS]:
   ```

6. **Type NPK, and press Return**.

7. **Repeat Steps 3 and 4 above to generate the NPK key file.**

Creating Seeds on a UNIX Platform

To create a seed on a UNIX platform:

1. Set the environment variable for the path to the key files.
2. If you want to set a length other than the default value (128 bits) for the LTSSs, change the value before you generate the seeds.
3. Enter the WEP **wfkseed** command.

Setting a Path to the Key Files

You must set an environment variable to establish a location for the key files.

Note: Store the files containing NPKs and LTSSs on removable media, such as floppy disks, and store that media in a safe place.

At the C shell prompt, enter

setenv WF_KEY_FILE_PATH <*n*>

n is a removable disk that you are using to store the key files.

Changing the Length of the LTSS Key Generator

You can set the length of the RNGs for the LTSSs to a value other than the default of 128 bits.

At the C shell prompt, enter

setenv WF_LTSS_KEY_GEN_LEN <*number of bits, from 128 to 248*>

Running the WEP wfkseed Command

The **wfkseed** command creates the seed that enables you to generate random numbers. You run this command twice to create seeds for the NPK and the LTSSs.

To create the LTSS seed:

1. **At the C shell prompt, enter**

   wfkseed

   WEP asks

   ```
   Do you wish to create the LTSS or NPK Key File? [LTSS]:
   ```

2. **Press Return to create the LTSS key file.**

   WEP displays this message:

   ```
   To initialize the seed for the cryptographic random number generator,
   please now enter a series of characters which you would consider to
   be 'random.'  As you enter them, dots '.' will be displayed to
   indicate progress.  If your string is not 'random' enough, questions
   '?' will be displayed.  In that case, modify the pattern you are
   entering.  When enough data is input, you will be prompted to stop
   (near 3 lines of input)...
   ```

3. **Type a series of random characters.**

   The screen displays a dot for each 5 keystrokes that WEP accepts.

   ```
   .... .... .... .... ....

   .... .... .... .... ....

   .... .... .... ..
   ```

   If your keystrokes are not random enough, the screen displays ???

   After you enter a sufficient number of random keystrokes, WEP displays a completion message, and returns you to the prompt.

   ```
   All done, thank you!
   ```

4. **Enter the wfkseed command again to generate the NPK key file.**

   WEP asks

   ```
   Do you wish to create the LTSS or NPK Key File? [LTSS]:
   ```

5. **Type NPK and press Return**.
6. **Repeat Step 3 to generate the NPK key file.**

Creating NPKs and LTSSs

After you generate the NPK and LTSS seeds, you open Site Manager and use the WEP Key Manager tool to generate NPKs and LTSSs. You enter an NPK on each router, and in the Site Manager NPK parameter. You enter the LTSSs in the MIBs of each router on a link.

Creating NPKs

To generate an NPK:

1. **Start Site Manager.**

   Note that you open Site Manager *after* you set the path to the key files.

2. **Select Tools > WEP Key Manager > NPK Manager.**

3. **In the NPK name box, type a name for the NPK.**

   Specify a name that identifies this router, perhaps by location, for example, *Boston*.

4. **Click on Add.**

   The NPK name and value appear in the NPK list box.

5. **Repeat Steps 3 and 4 to generate as many NPKs as you need.**

6. **After you finish, click on OK.**

   Site Manager stores these values on the removable media you selected when you set the key file path. Site Manager does not save the NPKs until you click on OK.

   The file name that stores NPKs on both PC and UNIX platforms is *wep_npk.dat*

Caution: Do not attempt to edit this file. If you do, the NPKs may become invalid.

Creating LTSSs

To generate an LTSS:

1. **Start Site Manager.**

   Note that you open Site Manager *after* you have set the path to the key files.

2. **Select Tools > WEP Key Manager > LTSS Manager.**

3. **In the LTSS name box, type a name for the LTSS.**

   Remember that the routers on both ends of a link share the LTSS. Choose a name that identifies the link, perhaps by locations, for example, *Boston_Sacramento*.

4. **Click on Add.**

   The LTSS name and value appear in the LTSS list box.

5. **Repeat Steps 3 and 4 to generate as many LTSSs as you need.**

6. **After you finish, click on OK.**

Site Manager stores these values on the removable media you selected when you set the key file path. Site Manager does not save the LTSSs until you click on OK.

The file name that stores LTSSs on a PC or UNIX platform is *wep_ltss.dat*.

Caution: Do not attempt to edit this file. If you do, the NPKs may become invalid.

Entering an NPK on a Router

The router stores its NPK in nonvolatile RAM. To enter the NPK, you work in the secure shell of the router. Follow these instructions to copy the NPK to the router from the file you created using the Site Manager WEP tool. You enter an NPK on each secure router.

These instructions assume that you have connected a PC or UNIX computer directly to the console port of the router. For instructions on connecting a computer to the router console port, refer to the installation manual that came with your router.

To enter an NPK on a router:

1. **At any shell prompt on a UNIX platform, or at the DOS prompt on a PC, enter**

   ksession

   You enter the secure shell, which prompts you for the password.

2. **Enter the password.**

   Your password should be at least 10 to 12 characters long. It should not be anything obvious. Change it often.

   The prompt changes to SSHELL.

3. **To view NPKs, display the** *wep_npk_file***.**

   On a Unix platform, use an editor such as vi or emacs in read-only mode. For example:

   vi -R a:/wep_npk_file

   On a PC, use an editor such as EDIT or Notepad.

4. **Using a text editor, copy the NPK for this router.**

5. **At the SSHELL prompt, enter the kset command followed by a space, and paste in the NPK.**

   kset NPK 0x <*NPK_value*>

   You must enter the NPK value in hexadecimal form, and you must include the *0x* notation.

6. **Save the configuration file.**
7. **Exit the secure shell by entering**

   kexit

   You return to the regular prompt.

Changing NPKs

You should change NPKs on a router periodically. For many applications, a period of three to six months is appropriate. To change an NPK, issue the **kset NPK** command as described in the previous section. The new NPK overwrites its predecessor, and WEP now uses the new NPK value. Remember that you must enter the new NPK in the Frame Relay or PPP Node Protection key parameter the next time you want to change your encryption configuration.

Monitoring NPKs

If the NPK on a router does not match the NPK in the MIB, encryption does not work. This situation occurs most frequently when you change a CPU board on one slot of a router, and that slot therefore lacks the current NPK.

You can view the log notes to make sure that the NPK for each slot matches the value of the NPK in the MIB. If they do not match, you can change either the router NPK value or the MIB NPK value by working in the secure shell of the router.

To view the log notes, in the Technician Interface enter

log -ffwidt -eKEYMGR

Changing an NPK on a Router

To change the router NPK value, follow the procedure in the previous section, “Entering an NPK on a Router.”

Changing an NPK in the MIB

To change the MIB NPK value:

1. **At any shell prompt on a UNIX platform, or at the DOS prompt on a PC, enter**

   ksession

   You enter the secure shell, which prompts you for the password.

2. **Enter the password.**

   The prompt changes to SSHELL.

3. **Enter**

   ktranslate *<old_NPK_value>*

   The MIB now has the same NPK as the router.

4. **Save the configuration file.**

Changing LTSSs

You should change LTSSs periodically as well. To change LTSSs, create new ones using the WEP Key Manager tool as described in the previous sections.

Creating TEKs

The router stores its TEK seed in nonvolatile RAM. WEP uses and manages the TEK to encrypt data. Your only task is to create a seed for the RNG that generates TEKs.

These instructions assume that you have connected a PC or UNIX computer directly to the console port of the router. For instructions on connecting a computer to the router console port, refer to the installation manual that came with your router.

The **kseed** command creates the seed that enables WEP to generate random numbers. To create a TEK seed, you work in the secure shell of the router.

1. **At the C shell prompt on a UNIX platform, or at the DOS prompt on a PC, enter**

   ksession

   You enter the secure shell, which prompts you for the password.

2. **Enter the password.**

   Your password should be at least 10 to 12 characters long. It should not be anything obvious. Change it often.

   The prompt changes to SSHELL.

3. **Enter the kseed command and press Return.**

   WEP asks

   ```
   Do you wish to create the TEK Key File?
   ```

4. **Press Return to create the TEK Key File.**

   WEP displays

   ```
   To initialize the seed for the cryptographic random number generator,
   please now enter a series of characters which you would consider to
   be 'random.'  As you enter them, dots '.' will be displayed to
   indicate progress.  If your string is not 'random' enough, questions
   '?' will be displayed.  In that case, modify the pattern you are
   entering.  When enough data is input, you will be prompted to stop
   (near 3 lines of input)...
   ```

   As you type, the screen displays a dot for each keystroke the WEP accepts:

   ```
   .... .... .... .... ....

   .... .... .... .... ....

   .... .... .... ..
   ```

   If your keystrokes are not random enough, the screen displays ???

   When you have entered a sufficient number of random keystrokes, WEP displays a message telling you you're done, and returns you to the prompt.

   ```
   All done, thank you!
   ```

5. **Exit the Secure Shell by entering**

   kexit

   You return to the regular prompt.

Starting Encryption for PPP

To configure encryption for PPP:

1. **Insert the floppy disk or other removable media that contains your NPK and LTSS files.**

Note: Take the following precaution to make sure that your NPK and LTSS source files are the ones you generated: When you enter values for the NPK, the LTSS Value, and LTSS Name parameters following the directions in the steps below, make sure that the path that appears in the top bar of the Configuration Manager window, the WEP NPK window, and the WEP LTSS window is the path that you set for your NPK and LTSS files.

2. **Select the WEP protocol.**

Site Manager Path	
You do this	**System responds**
1. Select a port to configure for PPP.	The Add Circuit window opens.
2. Click on **OK**.	The WAN Protocols window opens.
3. Choose **PPP** and click on **OK**.	The Select Protocols window opens.
4. Scroll down to choose **WEP**. You can also select other protocols. Click on **OK.**	You return to the Configuration Manager.

3. **Enter the NPK.**

   You need to do this once for each router or configuration file.

Site Manager Path	
You do this	**System responds**
1. In the Configuration Manager window, select Protocols > **PPP** > Interfaces.	The PPP Interface Lists window opens.
2. Select the Node Protection Key parameter. Click on **Values**.	The NPK Values that you generated previously appear in the WEP NPK window.
3. Highlight the NPK that you want to assign to this router. Click on **Confirm**.	The value appears in the Node Protection Key parameter box.
4. Click on **Apply**.	You have entered an NPK. The PPP Interface Lists window remains open.

   After you enter the NPK, the remaining parameters become available. If you are editing a configuration file that you created during a previous session, you must enter exactly the same NPK that you used before.

4. **Enter the LTSS Value and LTSS Name.**

Site Manager Path	
You do this	**System response**
1. Select the LTSS Value parameter. Click on **Values**.	The LTSS Names and LTSS Values that you generated previously appear in the WEP LTSS window.
2. Highlight the LTSS that you want to assign to this router. Click on **Confirm**.	The value appears in the LTSS Name and LTSS Value parameter boxes.
3. Click on **Apply**.	You have entered an LTSS Name and Value. The PPP Interface Lists window remains open.

5. **Set the Encrypt Enable parameter to Enable.**

The Encrypt Enable parameter defaults to Disable. Both the PPP Encrypt Enable parameter and the WEP Enable parameter must be set to Enable for WEP to function.

Site Manager: Encrypt Enable parameter: page A-2

6. **Set a Change Time for the MEK.**

   The MEK Change parameter sets the amount of time, in minutes, between changes in the MEK. The value for this attribute must be the same on both sides of a link.

Site Manager: MEK Change parameter: page A-3

7. **Click on Apply to save your changes.**
8. **Click on Done to exit the window.**
9. **Configure the WEP parameters.**

   Refer to “Configuring WEP Parameters,” later in this chapter.

Starting Encryption for Frame Relay

To configure encryption for Frame Relay:

1. **Insert the floppy disk or other removable media that contains your NPK and LTSS files.**

Note: Take the following precaution to make sure that your NPK and LTSS source files are the ones you generated: When you enter values for the NPK, the LTSS Value, and the LTSS Name parameters following the directions in the steps below, make sure that the path that appears in the top bar of the Configuration Manager window, the WEP NPK window, and the WEP LTSS window is the path that you set for your NPK and LTSS files.

2. Select the WEP protocol.

Site Manager Path	
You do this	**System responds**
1. Select a port to configure for Frame Relay.	The Add Circuit window opens.
2. Click on **OK**.	The WAN Protocols window opens.
3. Select **Frame Relay** and click on **OK**.	The Select Protocols window opens.
4. Scroll down to select **WEP**. You can also select other protocols. Click on **OK.**	You return to the Configuration Manager.

3. Enter the NPK.

You need to do this once for each router or configuration file.

Site Manager Path	
You do this	**System responds**
1. In the Configuration Manager window, select Protocols > **Frame Relay** > Services.	The Frame Relay Service List window opens.
2. Click on **PVCs**.	The FR PVC List window opens.
3.Click on **Add**.	The FR PVC Add window opens.
4. Enter a DLCI number. Refer to *Configuring Frame Relay Services* for instructions. Click on **OK**.	You return to the FR PVC List window.
5. Select the Node Protection Key parameter. Click on **Values**.	The NPK Values that you generated previously appear in the WEP NPK window.
6. Highlight the NPK that you want to assign to this router. Click on **Confirm**.	The value appears in the Node Protection Key parameter box.
7. Click on **Apply**.	You have entered an NPK. The Frame Relay PVC List window remains open.

After you enter the NPK, the remaining parameters become available. If you are editing a configuration file that you created during a previous session, you must enter exactly the same NPK that you used before.

4. **Enter the LTSS Value and LTSS Name.**

Site Manager Path	
You do this	**System response**
1. Select the LTSS Value parameter. Click on **Values**.	The LTSS Names and LTSS Values that you generated previously appear in the WEP LTSS window.
2. Highlight the LTSS that you want to assign to this router. Click on **Confirm**.	The value appears in the LTSS Name and LTSS Value parameter boxes.
3. Click on **Apply**.	You have entered an LTSS Name and Value. The PPP Interface Lists window remains open.

5. **Enable Encryption.**

   The Encrypt Enable parameter defaults to Disable. Both the Frame Relay Encrypt Enable parameter and the WEP Enable parameter must be set to Enable for WEP to function.

Site Manager: Encrypt Enable parameter: page A-2

6. **Set a Change Time for the MEK.**

   The MEK Change parameter sets the amount of time, in minutes, between changes in the MEK. The value for this attribute must be the same on both sides of a link.

Site Manager: MEK Change parameter: page A-3

7. **Click on Apply to save your changes.**
8. **Click on Done to exit the window.**
9. **Configure the WEP parameters.**

   Refer to the following section, “Configuring WEP Parameters.”

Configuring WEP Parameters

WEP has both line and circuit interface parameters. WEP parameters have default values. You can edit those values to customize WEP for your network.

Enabling Encryption

The WEP Enable parameter defaults to Enable when you select WEP from the Protocols menu. Both the WEP Enable parameter and the Frame Relay or PPP Enable parameter must be set to Enable for WEP to function.

Site Manager: Enable parameter: page A-4, lines; page A-5, interface

Selecting Encryption Strength

Encryption is available in two versions, regular and strong. The standard router software includes encryption that uses regular encryption, that is, 40-bit keys. We also offer a strong encryption option that uses 56-bit keys. Strong encryption is generally available only in the United States and Canada.

Select the encryption strength that is appropriate for your network. Note that you can select both encryption strengths. This option enables a system that has 56-bit encryption strength to support secure links with either 40-bit and 56-bit strength encryption sites. If you select both, WEP uses 56-bit encryption if both sides of the link can support it.

Site Manager: Cipher Mode Mask parameter: page A-4, lines; page A-6, interface

Setting Change Rates for the TEK

The TEK changes depending on the values of the TEK Change Time and TEK Change Bytes parameters.

TEK Change Bytes

The TEK Change Bytes parameter sets the number of bytes between changes in the value of the TEK.

Site Manager: TEK Change (Bytes) parameter: page A-5, lines; page A-6, interface

TEK Change Time

The TEK Change Time parameter sets the number of seconds between changes in the value of the TEK.

Site Manager: TEK Change (Seconds) parameter: page A-5, lines; page A-7, interface

Disabling Encryption

Remember that the Frame Relay or PPP Encrypt Enable parameter and the WEP line and circuit interface parameters must all be set to Enable for encryption to work. This does not mean that you can temporarily disable encryption on a line or interface by setting any of these parameters to Disable.

If you enable encryption for the line and circuit, but not for a protocol, and an LTSS exists, data does not travel over the network.

Deleting Encryption from an Interface

To delete encryption from an interface on which it is currently configured:

1. **In the Configuration Manager window, select Circuits > Edit Circuits.**

   The Circuit List window opens.

2. **Click on Edit.**

   The Circuit Definition window opens.

3. **Select Protocols > Add | Delete.**

   The Select Protocols window opens.

4. **Deselect WEP and click on OK.**

   Encryption is no longer operating on the interface.

Deleting Encryption from a Router

To delete encryption from all circuits on which it is currently configured:

1. **In the Configuration Manager window, select Protocols > WEP > Delete WEP.**

   A window opens and prompts:

   Do you REALLY want to delete WEP?

2. **Click on OK.**

   You return to the Configuration Manager. Encryption is no longer operating on the router.

Appendix A
Encryption Parameters

This appendix contains parameter descriptions for Frame Relay and PPP encryption parameters, and for WEP line and circuit interface parameters.

PPP and Frame Relay Encryption Parameters

Encryption parameters for PPP and Frame Relay are the same, but Site Manager paths and MIB object IDs differ.

Parameter: **Node Protection Key**

Path: **PPP:** Configuration Manager > Protocols > PPP > PPP Interface Lists window

Frame Relay: Configuration Manager > Protocols > Frame Relay > Services > Frame Relay Service List Window > **PVCs** > **Add**

Default: None

Options: 16 hexadecimal digits

Function: 1) Protects LTSSs on Site Manager.

2) Encrypts and decrypts LTSSs stored in the router's MIB.

3) Works as a password. The router compares the NPK from RAM to the NPK entered in Site Manager; this ensures that the MIB values are encrypted under the same NPK.

Each router or configuration file requires an NPK.

Instructions: Select the NPK from the list in the Site Manager WEP NPK window. Refer to instructions in Chapter 3.

Parameter:	**Encrypt Enable**
Path:	**PPP:** Configuration Manager > Protocols > PPP > PPP Interface Lists window
	Frame Relay: Configuration Manager > Protocols > Frame Relay > Services > Frame Relay Service List Window > **PVCs** > **Add**
Default:	Disable
Options:	Enable | Disable
Function:	Enables or disables encryption services on this port.
Instructions:	Set to Enable if you want to use encryption on this interface. Encryption will not work unless both this parameter and the WEP Enable parameter are set to Enable.
	If you select WEP in the Protocols menu, but set this parameter to Disable, data does not travel over this circuit.
MIB Object ID:	**PPP:** 1.3.6.1.4.1.18.3.4.28.5.1.2
	Frame Relay: 1.3.6.1.4.1.18.3.4.28.4.1.2

Parameter:	**LTSS Name**
Path:	**PPP:** Configuration Manager > Protocols > PPP > PPP Interface Lists window
	Frame Relay: Configuration Manager > Protocols > Frame Relay > Services > Frame Relay Service List Window > **PVCs** > **Add**
Default:	None
Options:	A string of up to 29 characters
Function:	Distinguishes this LTSS from others.
Instructions:	Select the LTSS from the list in the Site Manager WEP LTSS window. Refer to instructions in Chapter 3. When you enter the LTSS Value, you automatically enter the LTSS Name it represents.

Parameter: **LTSS Value**

Path: **PPP:** Configuration Manager > Protocols > PPP > PPP Interface Lists window

Frame Relay: Configuration Manager > Protocols > Frame Relay > Services > Frame Relay Service List Window > **PVCs** > **Add**

Default: None

Options: 32 through 62 hexadecimal characters.

Function: Creates the Master Encryption Key (MEK). The LTSS must be the same on both sides of the link.

Instructions: Select the LTSS from the list in the Site Manager WEP LTSS window. Refer to instructions in Chapter 3. When you enter the LTSS Value, you automatically enter the LTSS Name.

MIB Object ID: **PPP:** 1.3.6.1.4.1.18.3.4.28.5.1.5

Frame Relay: 1.3.6.1.4.1.18.3.4.28.4.1.8

Parameter: **MEK Change**

Path: **PPP:** Configuration Manager > Protocols > PPP > PPP Interface Lists window

Frame Relay: Configuration Manager > Protocols > Frame Relay > Services > Frame Relay Service List Window > **PVCs** > **Add**

Default: 60 minutes

Options: 1 through 65,535 minutes

Function: Sets the amount of time, in minutes, between changes in the value of the Master Encryption Key.

Instructions: Accept the default, or select another value within the specified range. The value for this parameter must be the same on both sides of a link.

If the router clocks are not synchronized and you want to use encryption, set this parameter to a value large enough to compensate for the time difference between the routers. This ensures that the MEKs are the same on both sides of a link.

MIB Object ID: **PPP:** 1.3.6.1.4.1.18.3.4.28.5.1.6

Frame Relay: 1.3.6.1.4.1.18.3.4.28.4.1.9

WEP Line Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > WEP > Lines

Default: Enable

Options: Enable | Disable

Function: Enables or disables encryption on this line. Defaults to Enable only if you select WEP in the Protocols menu.

Instructions: Accept the default, Enable, to use encryption on this line. Remember to enable either the PPP or Frame Relay Encrypt Enable parameter also.

MIB Object ID: 1.3.6.1.4.1.18.3.4.28.1.1.2

Parameter: Cipher Mode Mask

Path: Configuration Manager > Protocols > WEP > Lines

Default: DES (40 bit keys)

Options: DES (40 bit keys) | DES (56 bit keys) | Both

Function: Determines whether this line uses 40-bit or 56-bit encryption.

Instructions: Accept the default, 40, unless you have the strong encryption option that enables you to use 56-bit encryption. Select both values if you have 56-bit encryption and don't know the value on the other side of the link. If you select both, the link uses 56-bit encryption if both sides support it; if not, it uses 40-bit encryption.

The Site Manager screen displays the value of this parameter in hexadecimal notation:

0x 10000000 = 56-bit encryption

0x 20000000 = 40-bit encryption

0x 30000000 = Both

MIB Object ID: 1.3.6.1.4.1.18.3.4.28.1.1.5

Parameter: **TEK Change (Bytes)**

Path: Configuration Manager > Protocols > WEP > Lines
Default: 65,535 bytes
Options: 256 through 2,147,483,647 bytes
Function: Sets the number of data bytes between changes in the value of the TEK.
Instructions: Accept the default or select another value within the specified range.
MIB Object ID: 1.3.6.1.4.1.18.3.4.28.1.1.6

Parameter: **TEK Change (Seconds)**

Path: Configuration Manager > Protocols > WEP > Lines
Default: 10 seconds
Options: 1 through 65,535 seconds
Function: Sets the number of seconds between changes in the value of the TEK.
Instructions: Accept the default or select another value within the specified range.
MIB Object ID: 1.3.6.1.4.1.18.3.4.28.1.1.7

WEP Circuit Interface Parameters

Parameter: **Enable**

Path: Configuration Manager > Protocols > WEP > Circuit Interface
Default: Enable
Options: Enable | Disable
Function: Enables or disables encryption on this interface. Defaults to Enable only if you select WEP in the Protocols menu.
Instructions: Accept the default, Enable, to use encryption on this interface. Remember to enable either the PPP or Frame Relay Encrypt Enable parameter also.
MIB Object ID: 1.3.6.1.4.1.18.3.4.28.2.1.2

Parameter: **Cipher Mode Mask**

Path: Configuration Manager > Protocols > WEP > Circuit Interface

Default: Inherit from Line

Options: Inherit from Line | 40 | 56 | Both

Function: Determines whether this line uses 40-bit or 56-bit encryption.

Instructions: Accept the default, Inherit from Line, or select another option. To select another option, first deselect Inherit from Line, and then select either 40-bit or 56-bit encryption or both.

Accept the default, 40, unless you have the strong encryption option that enables you to use 56-bit encryption. Select both values if you have 56-bit encryption and don't know the value on the other side of the link. If you select both, the link uses 56-bit encryption if both sides support it; if not, it uses 40-bit encryption.

The Site Manager screen displays the value of this parameter in hexadecimal notation:

0x 10000000 = 56-bit encryption

0x 20000000 = 40-bit encryption

0x 30000000 = Both

0x 40000000 = Inherit from Line

MIB Object ID: 1.3.6.1.4.1.18.3.4.28.2.1.4

Parameter: **TEK Change (Bytes)**

Path: Configuration Manager > Protocols > WEP > Lines

Default: 65,535 bytes

Options: 256 through 2,147,483,647 bytes

Function: Sets the number of data bytes between changes in the value of the TEK.

Instructions: Accept the default, or select another value within the specified range.

MIB Object ID: 1.3.6.1.4.1.18.3.4.28.1.1.6

Parameter:	**TEK Change (Seconds)**
Path:	Configuration Manager > Protocols > WEP > Lines
Default:	10 seconds
Options:	1 through 65,535 seconds
Function:	Sets the number of seconds between changes in the value of the TEK.
Instructions:	Accept the default, or select another value within the specified range.
MIB Object ID:	1.3.6.1.4.1.18.3.4.28.1.1.7

Appendix B
Definitions of k Commands

This appendix contains definitions of the k 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>*

Index

F

G

K

L

M

N

O

P

R