Vanguard Managed Solutions

Vanguard Applications Ware
Multi-Service Feature Protocols

Data Encryption

Notice

©2005 Vanguard Managed Solutions, LLC
575 West Street
Mansfield, Massachusetts 02048
(508) 261-4000
All rights reserved
Printed in U.S.A.

Restricted Rights Notification for U.S. Government Users

The software (including firmware) addressed in this manual is provided to the U.S. Government under agreement which grants the government the minimum “restricted rights” in the software, as defined in the Federal Acquisition Regulation (FAR) or the Defense Federal Acquisition Regulation Supplement (DFARS), whichever is applicable.

If the software is procured for use by the Department of Defense, the following legend applies:

Restricted Rights Legend

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

If the software is procured for use by any U.S. Government entity other than the Department of Defense, the following notice applies:

Notice

Notwithstanding any other lease or license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction, and disclosure are as set forth in FAR 52.227-19(C).

Unpublished - rights reserved under the copyright laws of the United States.

Notice (continued)

Proprietary Material

This document is for information purposes only and is subject to change without notice.

Part No. T0103-09, Rev L
Publication Code DS
First Printing November 1998

Manual is current for Release 6.5 of Vanguard Applications Ware.

To comment on this manual, please send e-mail to LGEN031@vanguardms.com

Contents

Data Encryption

Overview

Introduction

This manual describes the Data Encryption technology employed in Vanguard Managed Solutions products.

The Data Encryption feature is a combination of discrete hardware, in the form of a dedicated Encryption SIMM (which includes Vanguard Managed Solutions hardware data compression capability), and Vanguard Applications Ware.

What Is In This Manual?

This manual includes a general description and history of encryption techniques and technology. In addition, a thorough description of Vanguard Managed Solutions implementation of data encryption, and explanations of how to configure Vanguard products to accept encrypted data.

Ordering Data Encryption

Vanguard data encryption is a combined hardware and software implementation. When ordering the Vanguard Encryption option, four choices are available:

- DES Encryption
- DES and Triple-DES Encryption
- ECC DIMM (Triple-DES & AES)
- Advanced Encryption Card (AEC) - Vanguard 7300 Series

Release 6.3 and greater supports Triple-DES and AES encryption on the Vanguard 342. Release 6.4 and greater supports Triple-DES and AES encryption on the Vanguard 340 Enhanced. Release 6.4 and greater supports the Advanced Encryption Card on the Vanguard 7300 Series (refer to the Vanguard 7300 Installation Manual for AEC information, Part Number T0185). Please refer to “Encryption” section on page 5 for Encryption information.

■ **Note**

DES and Triple-DES SIMMs include Vanguard Managed Solutions hardware data compression capability. Data Compression is not supported on the ECC DIMM or the Advanced Encryption Card (AEC).

What Products Support Encryption?

Only those Vanguard products capable of using these SIMMs and software combination supports data encryption. Contact Vanguard Managed Solutions Customer Service if you have any questions regarding product support.

- The Data Encryption feature does not work on access ports that have the Data Connection Protection feature enabled.
- Encryption is not supported on PPP/MLPPP links.
- Data Compression is not supported on the ECC DIMM and the Advanced Encryption Card (AEC).
- The DCC SIMM and ECC DIMM cannot be used together on the same node.

■**Note**

The ECC DIMM (Triple-DES & AES) is available for the Vanguard 342, 340 Enhanced and 7300 Series. The AEC module provides Triple-DES and AES for the 7300 Series.

Feature Table

The following table provides an overall summary of the encryption and compression features supported by the various Vanguard platforms.

Vanguard Platform	***Hardware SAM***	***IPSEC***	***Software Encryption***	***Hardware Compression***	***Software Compression***
320					**X**
340	**X**	**X**	**X(IPSEC)**	**X**	**X**
340 Enhanced	**X**	**X**	**X(IPSEC)**		**X**
342	**X**	**X**	**X(IPSEC)**	**X(DCCSIMM)**	**X**
6435 and 6455	**X**	**X**	**X(IPSEC)**	**X**	
7300		**X**	**X(SAM)***		**X**

* Release 6.5 and above.

The “X” indicates that the specified feature is supported by the Vanguard Platform.

Terminology

Please refer to the Vanguard Technical Glossary for the definition of terms specific to the Encryption feature.

In This Notice

Topic **See Page**

In This Notice *(continued)*

Topic	See Page

Network Security and Privacy

Introduction

Network security and privacy of communication on that network is of paramount concern to many system administrators, corporate security departments, and governments. Network security and privacy can be ensured by employing three major functions:

- Encryption
- Authentication
- Integrity Control

Encryption

Encryption involves preventing sensitive data from falling into the wrong hands. Encryption effectively scrambles data such that the original content can not be determined without knowing the encryption algorithm and the Encryption Key.

Authentication

Authentication refers to the ability to know, with absolute confidence, whom or what you are connected to.

Integrity Control

Integrity control ensures that transmitted data is not modified during transmission. Modification of encrypted data is referred to as an Attack. An Attack occurs whenever an unauthorized individual intrudes on your data communication without your knowledge. There are two types of attacks:

- Passive Attack - This type attack takes place when someone “breaks into your system” and does nothing but observe what is happening in that system. During a passive attack, data is not changed or inserted into the normal data stream.
- Active Attack - An active attack is said to have occurred whenever data being transmitted between nodes is changed, inserted, or deleted before being received.

  Changing, or modifying data could, for example, involve taking a banking transaction and changing the amount of a withdrawal before resending it as a new transaction. An encrypted checksum is used to verify the integrity of each encrypted message.

  Inserted data can be in the form of either a new message or a previously sent message that is replayed (resent) at a later date. For example, assume that an employees weekly paycheck is electronically deposited into their bank account. If they were to make an electronic record of that transaction, they could (at a later time or date) replay that transaction and continually redeposit the same amount of money into their account. In other words, that person could repeatedly withdraw the same amount of money, many different times, from your companies bank account. This person could also take the recorded data and create a new transaction, for an even larger amount of money, before sending it through the encrypted network.

Encryption

Introduction

Modern encryption is based on two factors: a well known algorithm and the use of secret keys. These are used to both encrypt and decrypt messages. Figure 1 illustrates the basic Encryption model.

■**Note**

In this manual, we use the term ‘plaintext’ when referring to information before it is encrypted.

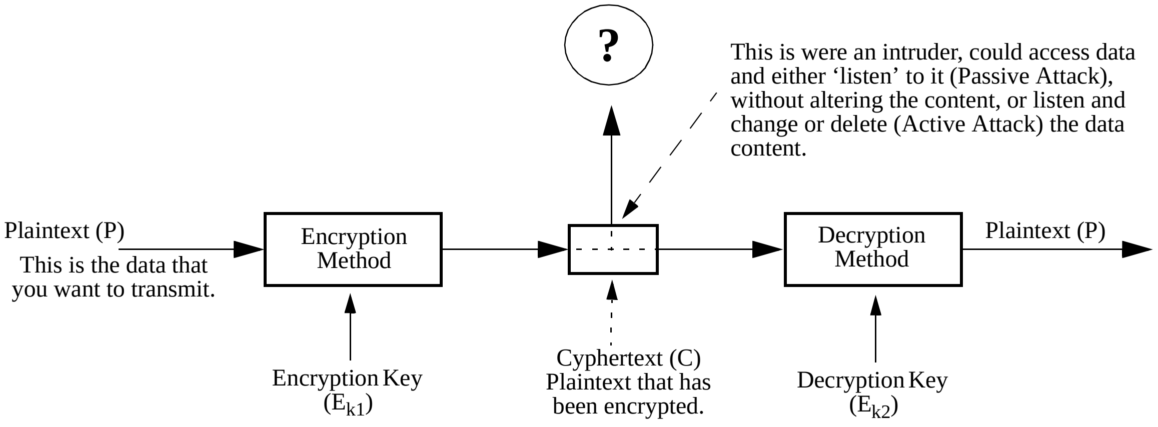

?
This is were an intruder, could access data and either ‘listen’ to it (Passive Attack), without altering the content, or listen and change or delete (Active Attack) the data content.
Plaintext (P)
This is the data that you want to transmit.
Encryption Method
Decryption Method
Plaintext (P)
Encryption Key (E_{k1})
Cyphertext (C) Plaintext that has been encrypted.
Decryption Key (E_{k2})

Figure 1. Fundamentals of the Encryption Process

Simplified Encryption Example

Assume that the process illustrated in Figure 1 includes the expression “ENCRYPT”. When the encryption key is applied to this expression, Cyphertext results. For example, the expression may appear somewhat like the hexadecimal string shown in Figure 2.

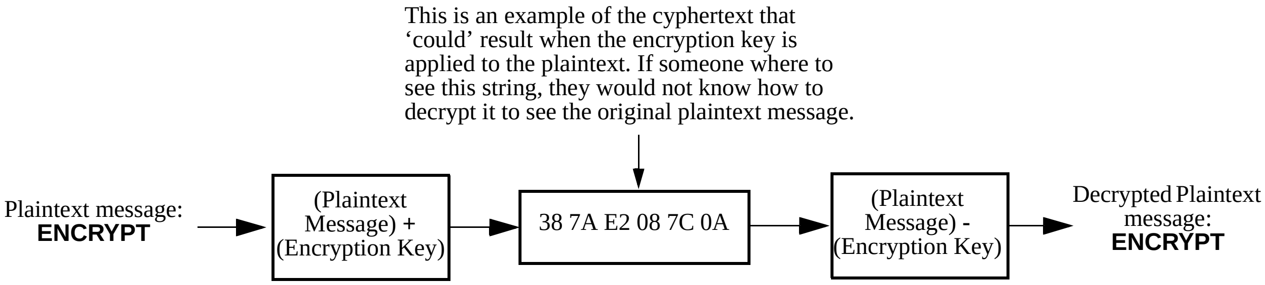

This is an example of the cyphertext that ‘could’ result when the encryption key is applied to the plaintext. If someone where to see this string, they would not know how to decrypt it to see the original plaintext message.
Plaintext message: ENCRYPT
(Plaintext Message) + (Encryption Key)
38 7A E2 08 7C 0A
(Plaintext Message) - (Encryption Key)
Decrypted Plaintext message: ENCRYPT

Figure 2. Basic Example of Encrypting Data

Data Encryption Standard (DES)

Introduction

The purpose of the data encryption is to create unidentifiable streams of bits out of a plaintext message that must be protected. To achieve this, a well defined encryption algorithm is needed. The major requirements for the encryption algorithm are:

- A transformation that is reversible. A person who has the key, must be able to decypher encrypted messages (cyphertext).
- The encryption/decryption process has to produce a unique result; the same original plaintext message. The same cyphertext cannot produce two different results using the same key that encrypted the message.
- Every output bit must depend on as many as possible bits of the input text and of the key used. Any change, even a single bit, in input text (or the key) has to produce a significant change in the resulting cyphertext.

There are two major principles of transforming plaintext to produce cyphertext:

- Substitution
- Transposition

Substitution

Substitution takes one piece of a message and replaces it with another, totally different pattern, of the same size. The basic rule on substituting one elementary pattern with another, is that the encryption algorithm has to be predictable and repeatable to ensure that it is reversible and unique. The mapping between input and output patterns, however, depends on the key used in each particular case.

Transposition

Transposition, on the other hand, takes a piece of a message and changes the order of the message bits in a predefined way. As with substitution, the basic rule of altering the arrangement of bits has to be predictable and repeatable. Although predictable, the actual mapping between input and output in each particular case depends on the key that is used. The person who has the key is the only one who can decrypt encrypted messages.

Data Encryption Standard (DES)

The Data Encryption Standard (referred to as the DES standard) encryption algorithm is the most commonly used algorithm in data encryption. The National Institute of Standards and Technology (formerly the National Bureau of Standards) adopted the DES standard in 1977, see Federal Information Processing Standard 46 (FIPS PUB 46). This document can be obtained from any US Government bookstore.

DES takes 64 bit long blocks of data and produces 64 bit long blocks of cyphertext. Encryption is achieved using 16 cycles of both substitution and transposition. The key used in each cycle is derived from the original key. Derivation of the key involves using circular shift and transformation of bits; decryption is done using exactly the same procedure.

Triple-DES

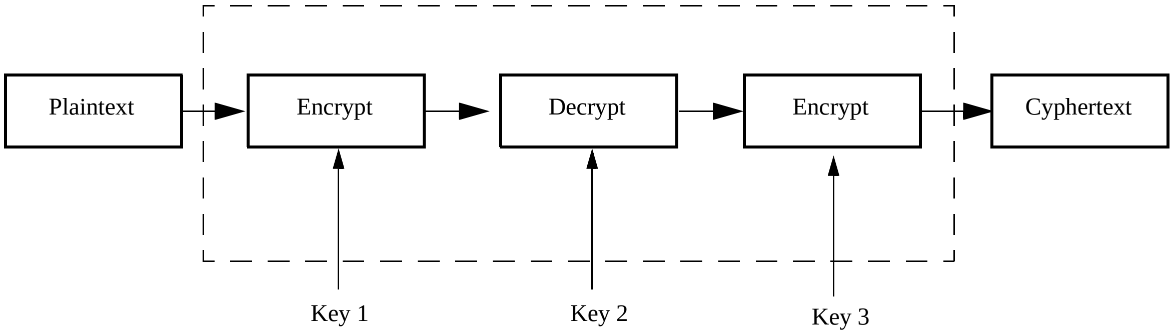
Triple-DES

A variation of DES, known as Triple-DES, has a key size that is larger than the key used for DES encryption.

Three keys used in Triple-DES encryption/decryption, and each 8 byte block of plaintext is operated on three times, which involves:

Operation...	*Performs this function...*
1	Encrypt using the first key
2	Decrypt using the second key
3	Encrypt again, using the third key

As illustrated in Figure 3, each key is a subset of the original 128 bits.



In the VanguardMS implementation, only two keys are used, although key number 1 is used in place of key number 3.

Figure 3. Triple-DES Key Construction of the Base Key

Advanced Encryption Standard (AES)

Introduction

AES is a Federal Information Processing Standard (FIPS), which specifies a cryptographic algorithm for use by organizations to protect sensitive, classified information. AES provides a better combination of security and speed than DES or Triple-DES. AES has more elegant mathematical formulas behind it, and only requires one pass to encrypt data. AES was designed from the ground up to be fast, unbreakable and able to support the smallest computing devices imaginable. The big differentiators between AES and Triple-DES are the strength of security, superior performance and better use of resources. AES provides faster encryption and compatibility with the widest range of devices. Without AES, it would be necessary to have different encryption technologies for application-specific purposes, such as wireless e-mail, financial transactions or quality-of-service-specific applications.

AES is defined for 128, 192 and 256 bit key lengths.

■ **Note**

Release 6.3 and greater supports Triple-DES and Advanced Encryption Standard (AES) on the Vanguard 342, release 6.4 on the 340 Enhanced. Release 6.4 and greater also supports the Advanced Encryption Card (AEC) for the Vanguard 7300 Series.
Please refer to the *Virtual Private Network (VPN) Manual's* Security Chapter for more information. (Part Number T0103-10).

Encryption Modes

Introduction

As a result of the tremendous progress in computer technology, encryption algorithms require additional features that make them even stronger. One such feature is known as the mode of the encryption algorithm called Cipher Block Chaining (CBC).

Cypher Block Chaining (CBC) DES

During data transfer, a Cypher Block Chaining (CBC) mode is used. With CBC, an Initialization Vector (IV) prevents repeated patterns in plaintext from appearing as repeated patterns in the cyphertext.

Initialization Vectors

An Initialization Vector (IV) is used to prepare each 8 byte plaintext block for encryption.

The network transport protocols, and volume of encrypted data being transmitted, dictates whether IV should be included in each packet. If you are using encryption on a connectionless network, you should configure the use of IVs. The same applies if you are transmitting large volumes of encrypted traffic, or are transmitting encrypted data in very small packets.

CBC Without Initialization Vectors Configured

Figure 4 illustrates how the IVs required to successfully encrypt data are generated. You do not have to configure this type of operation. If you keep Initialization Vectors turned off during configuration of your node, this example applies.

In this example, a randomly generated number is used as the first IV (IV_1)and, after IV_1 is Exclusive OR'd with the data in Block #1, it is encrypted using the encryption key.

The resulting encrypted data (in this case Q R S) is used by the next IV. This is Exclusive OR'd with the data in Block #2 and encrypted to create another packet of encrypted data (Encrypted Block #2).

Encrypted Block #2 creates IV_3 which is Exclusive OR'd with the data in Block #3 and encrypted to create another packet of encrypted data (Encrypted Block #3).

From this example, you can see that by encrypting the same data (Block 1 and 3 contain the same data), you create encrypted text that is totally different.

■**Note**

The encryption example shown in Figure 4 is for illustration purposes only; it is not intended to show exact results of CBC, or any other form of data encryption.

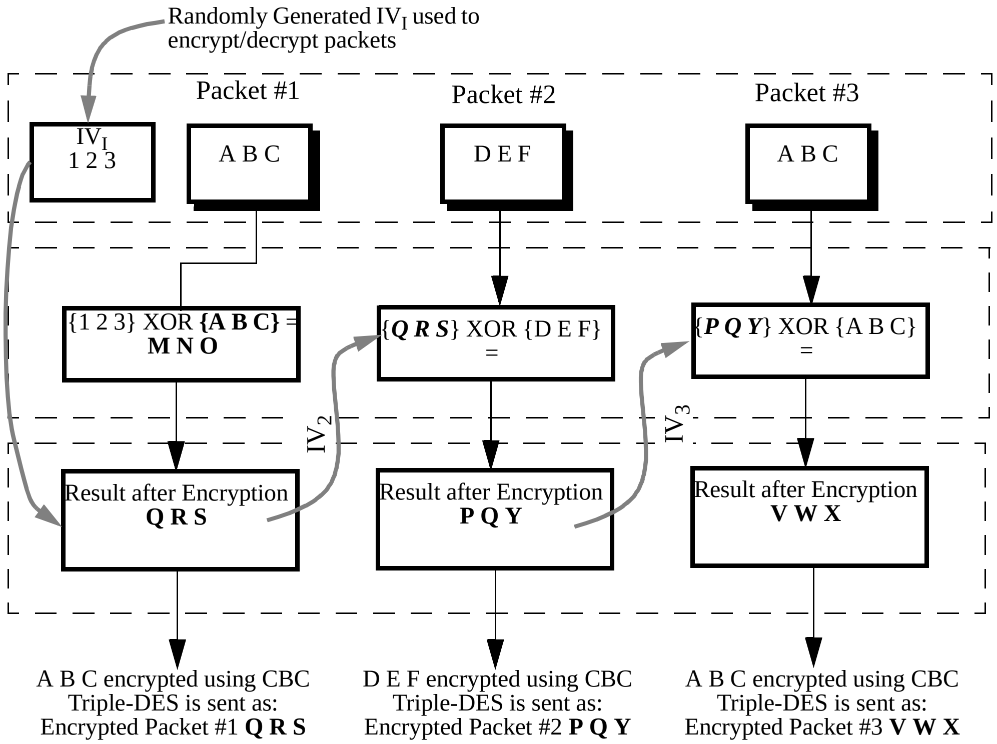

Randomly Generated IV_I used to encrypt/decrypt packets
Packet #1
Packet #2
Packet #3
IV_I
1 2 3
A B C
D E F
A B C
{1 2 3} XOR {A B C} =
M N O
{Q R S} XOR {D E F}
=
{P Q Y} XOR {A B C}
=
IV_2
IV_3
Result after Encryption
Q R S
Result after Encryption
P Q Y
Result after Encryption
V W X
A B C encrypted using CBC Triple-DES is sent as: Encrypted Packet #1 Q R S
D E F encrypted using CBC Triple-DES is sent as: Encrypted Packet #2 P Q Y
A B C encrypted using CBC Triple-DES is sent as: Encrypted Packet #3 V W X

Figure 4. Example Initialization Vector Creation and Use

Lost CBC Packets

Figure 4 illustrates how Initialization Vectors are created and used. It also identifies one significant potential difficulty with this mode of encryption. What happens when encrypted packets are lost or corrupted.

From Figure 4, assume that encrypted packet #2 is lost for one reason or another. Should this happen IV$_3$ is not created and the receiving node cannot decrypt the data stream.

The solution to this problem is to use the last 8 bytes of the proceeding encrypted packet, as the Initialization Vector for the next packet to be encrypted. Therefore, if one packet is missing or has been corrupted, only that packet and the next one in the data stream, is lost. Depending on the communication protocol being used, a Resend command may be used to request the missing packets. Figure 5, and the following description, illustrates this solution.

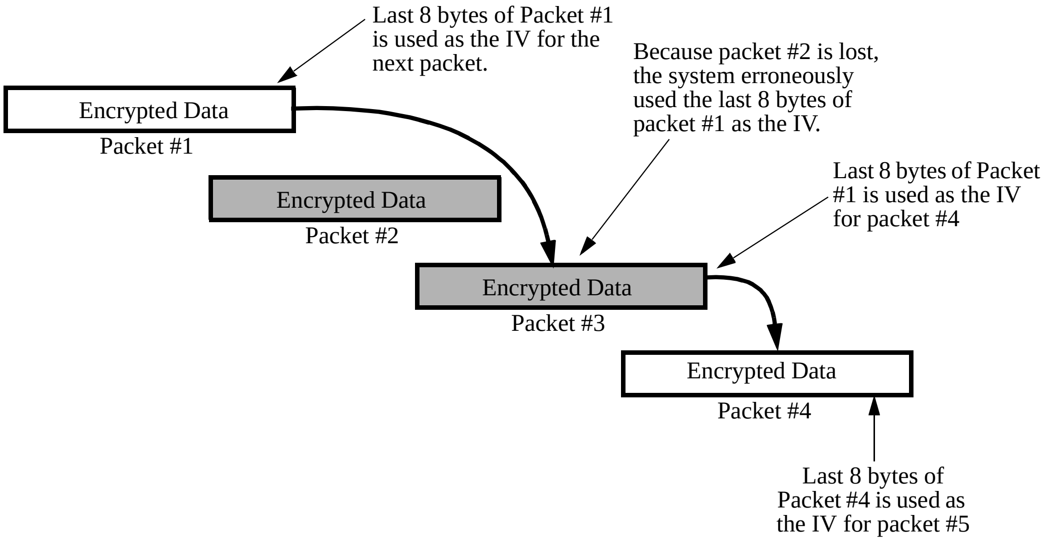

Last 8 bytes of Packet #1 is used as the IV for the next packet.
Because packet #2 is lost, the system erroneously used the last 8 bytes of packet #1 as the IV.
Last 8 bytes of Packet #1 is used as the IV for packet #4
Encrypted Data
Packet #1
Encrypted Data
Packet #2
Encrypted Data
Packet #3
Encrypted Data
Packet #4
Last 8 bytes of Packet #4 is used as the IV for packet #5

Figure 5. Correction for Missing/Corrupt Packets

Assuming that Packet #2 (in Figure 5) is missing or corrupted:

- Packet #1 is decrypted properly since its IV is correct.
- packet #2 is lost during transit.
- The last 8 bytes of packet #1 are erroneously applied as the IV for Packet #3, the resulting decrypted packet fails the integrity check and the packet is dropped by the system.
- Packet #4 is decrypted properly because it has the IV found in Packet #3 to work with.

■Note

To see the parameter you need to set to use the Initialization Vector, refer to the Data Encapsulation Type parameter description, found in the “Configure Encryption Profile Table” section on page 48. The example shown in Figure 5 occurs when you select NO_IV.

CBC With Initialization Vectors Configured

If you configure IVs into your node, a randomly generated IV is inserted as the first 8 bytes in the first Packet. After encryption of the first packet, the last 8 bytes in the encrypted packet are used as the second IV. This is then used to encrypt the second packet; the last 8 bytes of which are used as the IV for the third packet. Figure 6 illustrates this approach.

It is obvious, from Figure 6, that configuring IVs could result in additional packet overhead. Because of this, you would usually want to avoid using this approach when you are:

- Transmitting a substantial amount of encrypted traffic in small packets.
- Using a connection oriented communications protocol such as X.25 or Frame Relay Annex_G, where the protocol detects frames lost and retransmitted automatically.

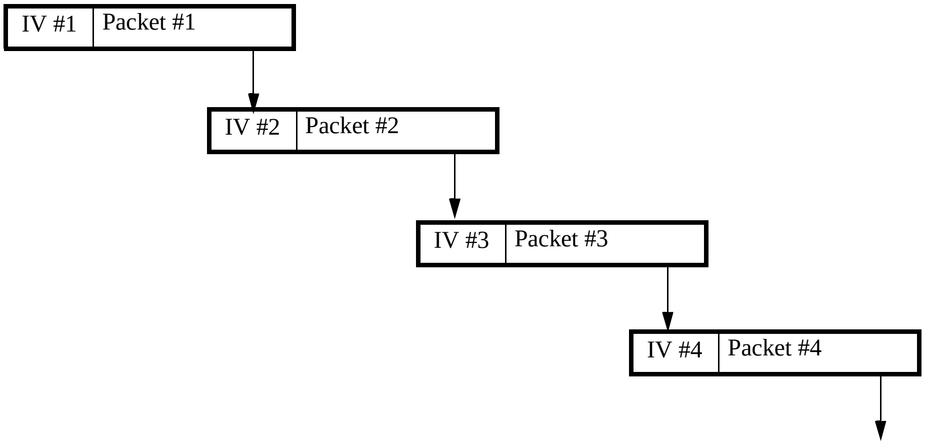


Figure 6. Packets with Initialization Vectors Configured

Keys

Introduction

In Data Encryption systems, the encryption key is the password to system security. If the key is large enough and it is changed frequently, it becomes almost impossible or prohibitively expensive (in time and money) for someone to discover which key is being used, and apply that key to the cyphertext in order to decrypt it back to plaintext.

Using Keys

Encryption and Decryption keys are binary codes essential to the concept of data encryption. If an unauthorized individual knows how a block of cyphertext was encrypted, that person may be able to decrypt it just as easily as you encrypted it. When considering encryption, you must always assume that someone somewhere may discover how you did it and, therefore, be able to intercept your data.

Consider this...

If a key is three digits long (like a combination lock) there is one thousand possible combinations of those digits. A six digit key would yield one million possible combinations. Obviously, therefore, if a longer key used to encrypt data it becomes much more difficult for someone to intercept, or steal that data.

Key Size

Various key sizes are used for different methods of encryption. The encryption scheme used in Vanguard products, is DES and Triple-DES, which use 64 and 128 bit keys respectively. The larger the key is, the more combinations the key can have. This makes it more difficult to break the keys used.

Key Exchange Authentication

Introduction

Authentication is critical for the security of an encryption network. Without being able to authenticate who it is you are going to pass encrypted data, you may unwittingly open your secure network to those who intend to cause network disruption or engage in illegal activity.

How Is Authentication Performed?

Authentication between two encrypting peers, is performed using the Base Key, to Triple-DES encrypt data. Figure 7 illustrates an example of how authentication is performed.

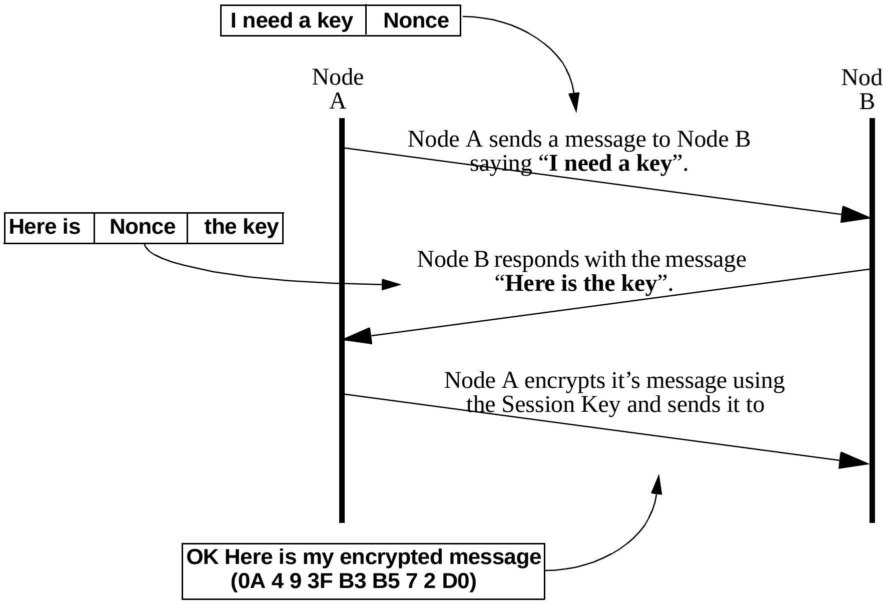

I need a key | Nonce
Node A
Node B
Node A sends a message to Node B saying "**I need a key**".
Here is | Nonce | the key
Node B responds with the message "**Here is the key**".
Node A encrypts it's message using the Session Key and sends it to
OK Here is my encrypted message (0A 4 9 3F B3 B5 7 2 D0)

Figure 7. Authentication Example

In Figure 7, the message "I need a key" is sent to node B. Along with the request for a key, the random number generator adds a random 32-bit number known as a Nonce. When node B receives the request it generates a Session Key and encapsulates the same Nonce within the key. This is returned to node A.

Authentication occurs when node A receives the response and extracts the Nonce value. After comparing the received Nonce to the transmitted Nonce, node A verifies that node B has responded using the correct 'authentication'. Node A then uses the Session Key it received from Node B to encrypt it's message and send it to node B. The fact that node A is able to send data encrypted with the Session Key that node B sent to it, authenticates node A to node B.

Use of a Nonce that is created by a random number generator guarantees the time freshness of the Session Key. This introduces a high level of security to the Session Key because it is practically impossible to generate the same random number twice and, without this random number, authentication can not take place.

■**Note**

Both the key request and key response are Triple-DES protected using the Base Key that nodes A and B share for that particular connection. However, data is encrypted, and passed between nodes, using the Session Key and DES protection. Refer to the “Data Encryption Standard (DES)” section on page 6 for additional information.

The Vanguard Managed Solution Implementation

Introduction

This section describes, in detail, how VanguardMS has implemented data encryption in its products, and includes:

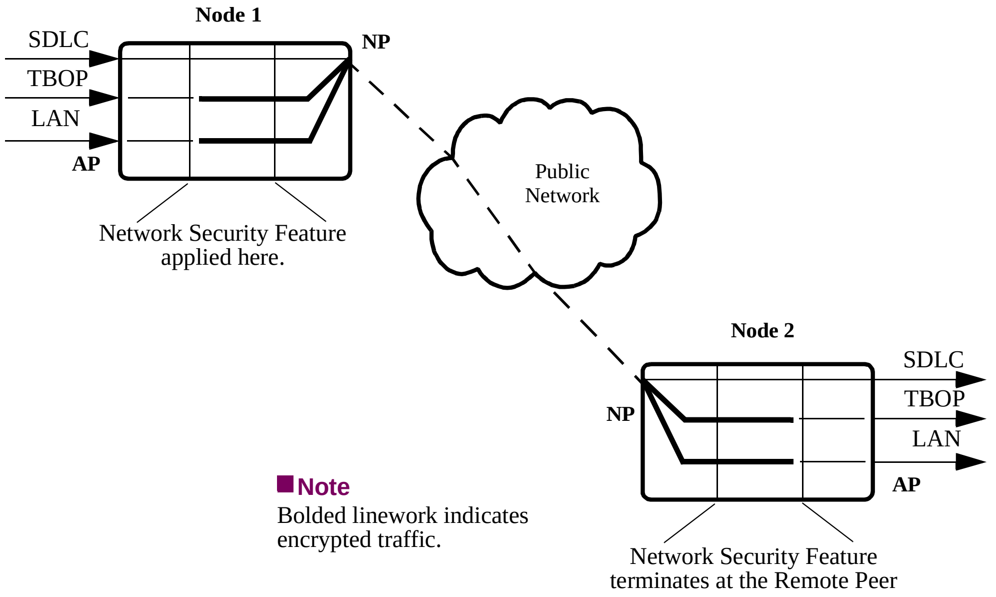
- “Default Base Key Table and Node Key” section on page 23
- “Encrypted Connections” section on page 30
- “Protocol Support for Data Encryption” section on page 33
- “CTP Access to an Encrypted Node” section on page 35

Data encryption has been implemented in Vanguard products, with flexibility in mind. Encryption can be implemented on individual Access Port connections going over Frame Relay and X.25 links. The ability to enable or disable encryption on individual end-to-end connections allows a network administrator to conserve the nodal encryption resources by only enabling encryption where it is needed.

Depending on the application, it is possible that only a few connections within some network ports may carry encrypted traffic while the remaining connections stay un-encrypted.

Where is Encryption Applied?

Data encryption is a Network Security feature in Vanguard products and Applications Ware software. This type of feature can be applied to any Vanguard Access Port (AP) at an AP/NP (Network Port) interface and terminates at the corresponding AP peer in a remote network. See Figure 8.


Node 1
SDLC
TBOP
LAN
AP
NP
Network Security Feature applied here.
Public Network
Node 2
NP
SDLC
TBOP
LAN
AP
Network Security Feature terminates at the Remote Peer

Note
Bolded linework indicates encrypted traffic.

Figure 8. Encryption in a Vanguard Network

Protocol Support

The VanguardMS implementation of data encryption can support these AP protocols over Frame Relay (Annex_G or Bypass), X.25, and LCON traffic can be sent over and PPP/MLPPP networking ports:

Access Port	***Network Ports FR-X.25-Annex_G***
TBOP	X
SDLC	X
SNA	X
LAN/LCON (router and Bridge)	X
LSC-TR	X
LSC-ET	X
LSC-FR	X
FRA	X

Encryption Keys

Introduction

VanguardMS uses a DES algorithm to encrypt data in an encryption session. This algorithm is considered to be satisfactory for confidentiality for user data transfer. The session keys are transferred using Triple-DES.

Vanguard encryption uses three keys:

- Node Key - This is two 64-bit keys for a total of 128 bits.
- Base Keys and CTP Keys - Each of these keys consist of two 64-bit keys for a total of 128 bits.
- Session Keys - These automatically generated keys consist of 64 bits.

Node Keys

Each node can be assigned one Node Key to allow access to the node and a list of Base Keys. One Base Key is assigned for each Closed Secure Group (Figure 9).

There may be up to 64 Base Keys which create separate closed secure groups of nodes that communicate, that is, exchange data using encryption, within each group but not to other groups.

The Node Key encrypts all Base Keys, before they are stored in CMEM, to provide confidentiality of the information. On the Vanguard 7300 Series platform the node key is encrypted and stored in FLASH on the CPU card. For all other platforms, the node key is encrypted and stored in non-volatile RAM on the encryption module.

For platforms running software encryption the node key is encrypted and stored in a special area of CMEM. This special area of CMEM is non transferable (unlike conventional CMEM which can be transferred through the CTP ports or via TFTP).

■**Note**

When entering node keys, you must enter both node key values at the same time. The node keys can not be the same value. If you would like to change only one of the node keys, you must also re-enter the other node key.

■**Note**

Refer to the *Vanguard Daughtercard Installation Guide* (T0020) for additional related SIMM information. Refer to the *Vanguard 7300 Installation Manual* (T0185) for additional information relating to the Advanced Encryption Card (AEC).

Keys also allow remote users to log onto the CTP port of an encryption enabled node. To do this, a remote user must originate a connection from a Vanguard node running the Security Applications Ware license and know the Node Key for the node being called. The Node Key is used to establish an encryption session and exchange Session Keys for the encrypted CTP session. This is similar to the Base Key being used for encryption.

The Node Key can be different for each node in the network. The administrator, however, may decide to use just one node-key for all the nodes that he or she manages. You should note that unrestricted access to all the node resources are available through a local dedicated CTP.

Closed Secure Groups

Introduction

Closed secure groups are an encrypted network arrangement that permits limited access to mutually agreed upon areas in networks serviced by data encryption. Figure 9 illustrates an example of possible multi-national Closed Secure Groups.

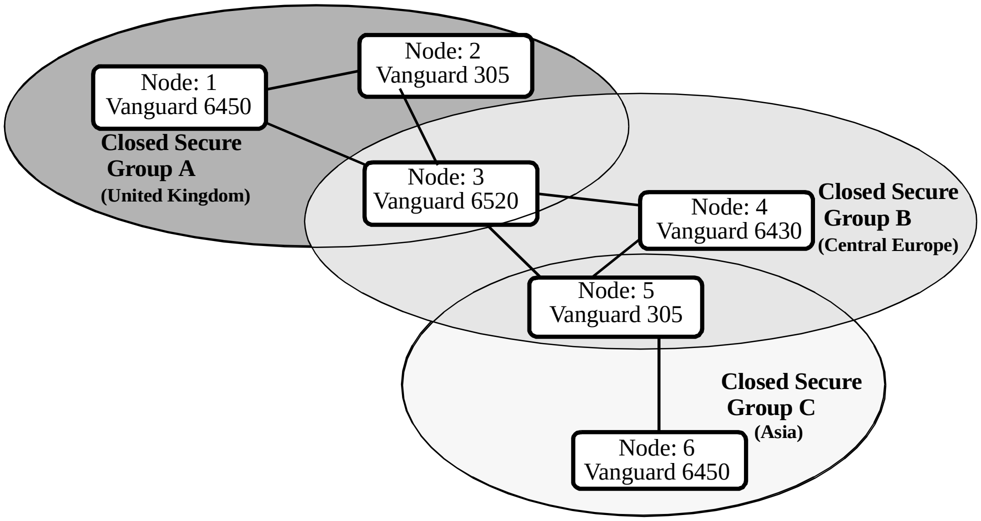


Figure 9. Closed Secure Group Example

In this example:

a) Nodes 1 and 2, in the United Kingdom, form Closed Secure Group A. This group uses encryption to communicate with Closed Secure Groups B and C.

b) Nodes 3, 4, and 5, in central Europe, form Closed Secure Group B. This group uses encryption to communicate with groups A and C.

c) Node 6 is located in Asia and, while connected to Node 5, is considered Closed Secure Group C. Node 6 uses encryption to communicate with Group B, but can not set up encrypted links directly to a node in Closed Secure Group A. The exception would be to allow Node 6 access to areas that have been mutually agreed upon by all Closed Secure Groups.

CTP Keys

Introduction

A CTP Key is a special key which allows any node in the network to communicate (have CTP access) with the node using encryption. Each node has a unique CTP Key.

■ **Note**

> The CTP Key is used for Network Management purposes including: node setup and management of all the keys. It does not allow access to security sensitive information.

Unlike the Node Key, which allows unlimited CTP access, the CTP Key does not allow unauthorized modifications to be made to the Base Key Table. The CTP Key allows encrypted remote access to standard CTP functions with the exception of: Node, CTP and Base Key setup or modification.

Possible Uses

The CTP Key can be used, for example, by VanguardMS Customer Service (for troubleshooting purposes) or other people responsible for managing non-security related functions of the network.

■ **Note**

> After the key has been used in this way, it should be changed by the Administrator.

It is possible to have one CTP Key for all nodes. For optimal security, change the CTP key for all nodes before sending them to VanguardMS Customer Service. After service work on those nodes is complete, the Administrator should return them to their original setting.

Any other node, outside that private network, can establish encrypted connection to a node within the private network provided that it has been configured with the proper Base Key for the particular Closed Secure Group.

■ **Note**

> Once the connection between two private networks is established, it is protected (encrypted) but the encryption only restricts CTP access. All other resources in the two networks are accessible. Some additional standard equipment, such as firewalls, are needed to restrict the access to the mutually agreed area.

Base and Session Keys

Introduction

Although not used extensively, a Base Key is critical to preserving the integrity and safety of encrypted data.

Base Keys

Authentication using Base Keys

Base Keys are used to authenticate the remote encryption peer and to protect Key exchange messages that establish Session Key.

A Base Key is user definable by either manually entering a key value or selecting the AUTO function during configuration. When the AUTO function is selected, a random number generator creates the Base Key value for use by the network. using AUTO eliminates the potential for network attacks because it does not rely on any predictable key value, such as a name, birthday, or similar key value that has an operators personal touch.

■ **Note**

The Base Key is exposed to the network whenever the Session Key is changed so it should be changed on a regular basis. The frequency of change should be dependent on the number of times the Session Key is changed. It may be acceptable to change the Base Key annually. Larger, busier networks may require Base Key changes more frequently; smaller networks may require less frequent Base Key changes.

■ **Note**

Base Keys are only supported on platforms which support the SAM protocol. The “X” indicates SAM protocol is supported.

Vanguard Platform	*SAM Protocol*
320	
34x Series	**X**
6435 and 6455	**X**
7300 Series	**X (software only)***

*Release 6.5 and greater.

Session Keys

Encrypting with Session Keys

The 64-bit Session Key is a randomly generated number that is used to actually encrypt data. It is exchanged between the encryption peers during authentication and key exchange phases. You can improve the security of your encryption system by changing the Session Keys frequently. You can configure a Vanguard node to change its Session Key as much as once every five minutes.

■ **Note**

Session Keys are only supported on platforms which support the SAM protocol.

Default Base Key Table and Node Key

Introduction

All Vanguard products shipped encryption-ready, from the factory, contain a default Node Key. This default key allows you to make an encrypted CTP connection to an un-initialized remote node.

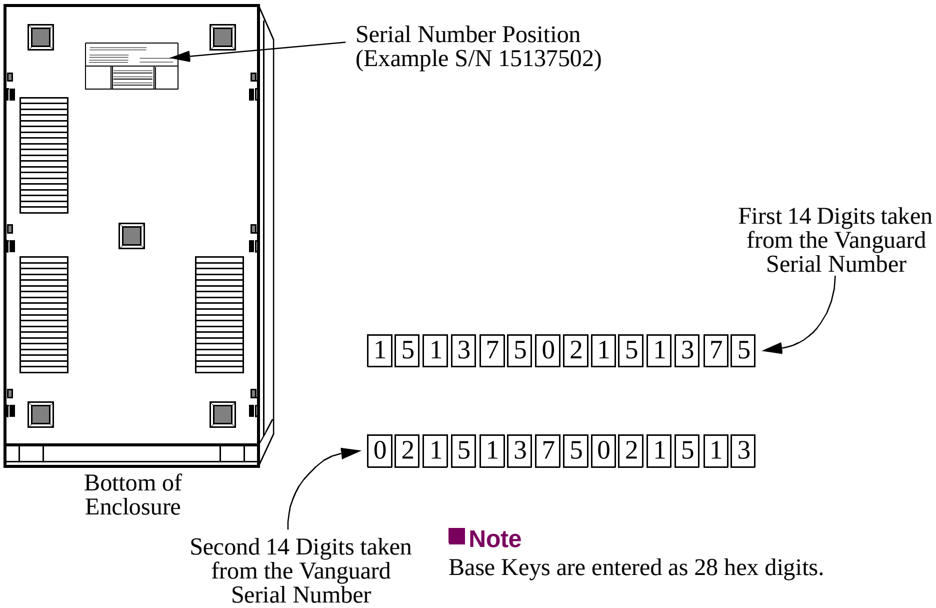
The default key is formed from the serial number of the device using the scheme described in this section.

Default Node Key

The default Node Key value is taken from the serial number of its Vanguard device. This is illustrated in Figure 10 where the first 14 hexadecimal digits of the key are formed using the serial number repeated as many times as needed. The next 14 hexadecimal digits are formed using the serial number in the reverse order.

■ **Note**

In situations were a Vanguard device has a serial number starting with one or more zeros (0), these are dropped from the default Node Key.



■ **Note**
Base Keys are entered as 28 hex digits.

Figure 10. Deriving the Default Node Key

In the example shown in Figure 10, a sample serial number (15137502) would result in a default Node Key of:

Key 1 = 1513 7502 1513 75

Key 2 = 0215 1375 0215 13

It is critical to note that the default key is a potential security hazard. Any unauthorized individual who knows a device serial number of the unit and, therefore, the value of the default key, can observe a supposedly secure encrypted CTP connection and decrypt the new setting for the Base Keys.

Caution

You should change the default Base Key ***BEFORE*** connecting the node to the network. If this is not possible, it must be changed immediately after installation, to prevent unauthorized intrusion.

Each time a Vanguard device powers up using the default Node Key, it generates an encryption alarm as a warning to change the key. Vanguard devices also generate an encryption alarm every time an encrypted connection is set up using the default node key.

Vanguard products and Applications Ware support up to 64 configurable Base Keys per node. While both ends of an encrypted session must be configured with the same Base Key, it is not necessary for one Base Key to be used only for a remote connection. In practice, you can partition a network into several Closed Secure Groups; each of which using the same Base Key to communicate with other nodes in the same CSG. Refer to the “Closed Secure Groups” section on page 19 for additional information.

■ **Note**

Even though the same Base Key can be used to establish sessions with multiple remote nodes, each encrypted session to the remote node negotiates its own Session Keys for encrypting data. Should a Session Key be ‘cracked’, the potential exposure is limited to that specific connection and does not effect other sessions.

Setting the Base Keys

You can set up a Base Key in one of three different ways:

- Local CTP connection is the most secure way to set Base Keys. They are write only parameters so that unauthorized access to a node can not result in the use of the CTP to read back the value of any Base Keys.
- Encrypted remote CTP connection using the Node Key for authentication. If the Base Key is configured across a remote CTP connection, it is only encrypted using DES during the transfer.
- Download the contents of a previously stored CMEM. Base Keys are encrypted by the Node Key, using Triple-DES, before being stored in CMEM.

■ **Note**

Due to a lack of security surrounding SNMP, you can not use this to set or read Base Keys. This may be supported in subsequent releases of the Data Encryption feature.

To simplify the process of selecting sound Base Key values, an embedded CTP feature ‘suggests’ Base Key values using a random number generator to create session keys. The value of each key must be recorded and stored in a secure location prior to entering it as a Base Key in the appropriate network nodes.

Changing the Base Keys

Generally speaking, it should not be necessary to change Base Keys because there is very little traffic sent across the network using the Base Keys. The exposure inherent in using a constant Base Key should not be sufficient to permit unauthorized intrusion. However, if a network operator suspects that the Base Keys have been compromised, change the Base Keys immediately.

Changing Base Keys is a two step procedure:

Step	Action	Result
1	Entering a new Base Key value for an existing key.	The Base Key is encrypted by the Node Key and stored in CMEM.
2	Boot the new key value.	The key (retrieved from CMEM) is decrypted and stored in dynamic RAM. During session key exchange, the Data Encryption feature takes the configured Base Key, for that session, from the dynamic RAM.

To simplify the process of selecting Base Key values, an embedded CTP feature (auto) ‘suggests’ Base Key values using a random number generator to create Session Keys. The value of each key must be recorded and stored in a secure location prior to entering it as a Base Key.

After a Base Key has been changed in CMEM record, the record must be booted before it takes effect in the system. Even then, an existing encryption session authenticated with the old base key continues to operate using its current session keys until the session time expires, at which time the new base keys are used to negotiate a new session key.

■ **Note**

Whenever a base key is changed, a high priority alarm is generated so that the network operator sees any unauthorized key changes and those that are expected.

Changing Node and CTP Keys

A CTP Key is a Base Key whose mnemonic name is “CTP”. Therefore, the procedure for changing the base key also applies to changing the CTP key.

The Node Key has a special function, as explained in the “Node Keys” section on page 18. It is used to protect (by encryption) all other keys stored in CMEM. On the Vanguard 7300 Series platform the node key is encrypted and stored in FLASH on the CPU card. For all other platforms, the node key is encrypted and stored in non-volatile RAM on the encryption module. A secondary function of the node key is to authenticate Session Key exchanges for unrestricted (encrypted) remote CTP access.

Whenever a Node Key is changed, the new value is immediately stored in the SIMM. The keys stored in CMEM are decrypted using the old Node Key and encrypted with the new key.

Protected remote CTP access uses the old Node Key value that is stored in DRAM while the new Node Key is used to decrypt base keys that are booted. After the Boot Node Key command is performed, the new node key is moved into DRAM.

Deleting Node and Base Keys via the CTP Port

All Base Keys can be deleted using either a local or encrypted remote CTP connection. A CTP connection can also be used to delete base keys. These can be deleted either one at a time or all keys at once.

When the Delete All Keys operation is selected, all Base Keys are deleted and the Node Key is set to the factory default value. Refer to the “Default Node Key” section on page 23 for specifics on how the default key is generated. After deleting a nodes Base Keys, you may notice some disruption of encrypted communication between that node and the remainder of the network. This is likely to occur whenever a periodic update occurs to the Session Key. This disruption generally only lasts until valid Base Key values are re-entered.

■ **Note**

Resetting the configuration memory to factory default, via the CTP, effects neither the Node or Base Keys. However, removing the CMEM battery effects both CMEM and the Base Keys.

Caution

You should delete all Base Keys and the Node Key on a node before turning control of that node over to a third party - including VanguardMS Customer Service. If you do not delete the keys, you may compromise the security of your own network.

Example Key Use

Introduction

Although Base Keys can not easily be compromised during file transfer, the most secure way of setting base keys is through a local CTP connection.

Example

Figure 11 illustrates how keys can be organized:

1) Nodes 1 through 6 are organized in Closed Secure Groups A, B and C.

- Nodes 1 to 3 belong to group A.
- Nodes 3 to 5 to group B.
- Nodes 5 and 6 belong to group C.

2) Nodes 1 to 5 belong to one private network and is managed by the System Administrator (SA).

3) Node 6 is managed by another System Administrator (SA).

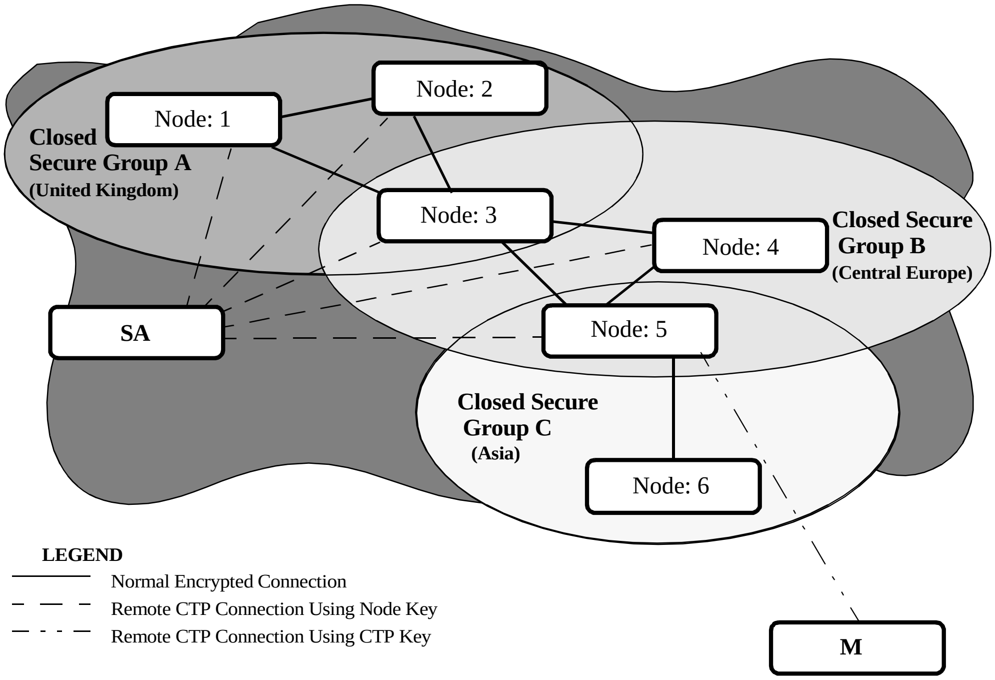


Figure 11. Key Usage Organization Example

In Figure 11, the System Administrator of the first network (nodes 1 to 6 and node SA) can not establish remote CTP connection to node 6 since that Administrator does not know the node-key or CTP key for node 6. It is possible however to establish an encrypted data exchange session between nodes 5 and 6, provided that System Administrators for both private networks agree on which Base Key is to be used. They must configure it independently at the both sides of the connection.

The private network administrator uses node SA to establish remote CTP connection to nodes 1 through 5 (these are nodes under his authority). The Administrator uses the Node Keys from these nodes to connect to the CTP and to set all encryption related records. The administrator can use any node in the private network to perform the same action provided that he has the correct Node Key.

Although node 6 belongs to another private network, an encrypted session can be established with node 5 as long as both nodes are configured with the same group C Base Key.

■Note

> Although node 6 is not able to decrypt messages sent between other groups in the private network (this node does not know the keys used), node 6 may be able to access resources in the network using connections between node 5 and nodes 3 and 4. The Data Encryption feature does not prevent this; although the system administrator of both networks may deploy some other mechanisms (filters, firewalls or routing tables) to block an area of unintended access.

In Figure 11, Node M represents a situation whereby VanguardMS Customer Service may have a ‘troubleshooting’ node connected to the network. The Administrator must set a CTP Key at node 5. The Administrator must give this key to the service technician who, using this key, accesses everything on the node 5 except any encryption related parameters.

Deleting Node Keys

When Do You Delete Node Keys

Node Keys should be deleted before swapping units out for service or repair. Alternatively, you can delete the key or physically remove the Data Encryption SIMM from the Vanguard device. Doing so causes the keys to remain in CMEM but, since they are encrypted, they are unreadable.

Vanguard products provide a CTP command to delete all encryption keys. When the Delete All Keys operation is performed, the Node Key is set to the factory default value and all base key CMEM records are deleted.

Resetting the configuration memory to factory default settings, via the CTP, effects neither the Node or Base Keys. However, removing the CMEM battery effects both CMEM and Base Keys.

You should delete all Base Keys and the Node Key on a node before turning control of that node over to a third party - including VanguardMS Customer Service. If you do not delete the keys, you may compromise the security of your own network.

Restoring Base Keys After Installing a new SIMM

Base Key records in a CMEM are encrypted by the Node Key stored in the encryption SIMM. These records are not decrypted properly when an existing SIMM is replaced by new SIMM. The system does generate an alarm at start up time to report the number of good or bad Base Keys found in CMEM. To restore the bad Base Keys, you can either re-enter all the Base Keys or re-configure the Node Key to the same value stored in the old SIMM.

Restore Node Key Vanguard 7300

The Node Key for the 7300 Series Platform is stored on the CPU card. Users do not have to restore the node key when changing encryption hardware in order to be able to read the encrypted keys in CMEM.

After Deleting a Node Key

When a Node Key is restored after being deleted, all Base Keys are available. If, for example, a different value from the original one is entered, the Node Key is not restored properly and you are warned that some Base Keys can not be decrypted. If this occurs, you have two options:

1) Accept the new Node Key and delete all unrecoverable keys.

2) Reject the new Node Key and exit. This allows you to enter the correct key without destroying the encrypted keys stored in CMEM.

Encrypted Connections

Introduction

This section describes encryption functionality for serial protocols and LAN bridging/routing across X.25 and Frame Relay WAN links.

Configuring Encryption for an Individual Connection

Encryption resources can be conserved in each node by only configuring encryption on those WAN links and channels that need it. In some networks, WAN links or channels requiring encryption may represent only a small subset of the total number of all WAN links and channels and, subsequently, a small portion of total data throughput.

Encryption Encapsulation and Control Protocol

VanguardMS has implemented a proprietary ‘encapsulation protocol’ that encapsulates encrypted frames, while differentiating between Control Messages and encrypted data. Control messages include:

- Encryption negotiation
- Authentication
- Periodic Session Key update messages

For encryption to work, data frames must be in multiples of 8 bytes. If they are not, encapsulation pads them until they are a multiple of eight bytes. When being decrypted, the padding is removed. Once decrypted, a data integrity check field ensures the quality of the decrypted data. A data integrity check field is incorporated into each data packet.

An optional initialization vector for CBC DES mode may be supplied with each packet. Otherwise, the last eight bytes of the previous data packet are used as initialization vector for the next packet decryption. See “Key Exchange Authentication” section on page 14 for additional information on authentication.

Encryption Negotiation and Authentication

After establishing a connection, encryption negotiation and mutual authentication must be completed before that connection is available for data transfer.

Encryption negotiation involves having the local and remote nodes agreeing on a encapsulation type. Either the initialization vector (IV) is passed along with each data packet or last eight bytes of the previous data packet are used as the IV.

Mutual authentication ensure that local and remote nodes have been configured with the same Base Keys, and is therefore a valid member of the same Closed Secure Group.

A VanguardMS proprietary protocol is used for encryption negotiation and key exchange. This protocol is based on three-way handshaking, and an authentication mechanism used in an authenticated version of the Diffie-Helman algorithm. The messages exchanged are authenticated and Triple-DES is encrypted by the configured Base Key.

If Authentication is Successful

The encryption channel is opened for passing data once the remote peer is authenticated, and a session key has been established. Data is then encrypted and decrypted using the negotiated Session Keys.

If Authentication Fails

If connection authentication fails, the Data Encryption feature attempts to re-establish an encrypted session two more times; a three second waiting period occurs between each consecutive retry.

If, after three attempts, the connection is unable to establish encryption session with the remote peer, the system identifies the encryption channel as being DOWN. The system continues trying to exchange the Session Key, and re-establish the connection, each time a new data packet has to be sent.

SCV Connections

If all attempts fail, the SVC connection is released. When each the local and remote nodes receive an acknowledgment message (ACK), user data is passed. This data is encrypted and decrypted using appropriate Session Keys.

PVC Connections

User data, on a PVC connection, is disabled after all attempts to re-establish an encrypted session have failed. If a PVC connection is disabled for user data passing because key exchange and authentication has failed, the system attempts to exchange a session key and re-establish the connection each time when a new data packet has to be sent.

Alarms are generated once the session is re-established and warns you that the connection is enabled.

Periodic Session Key Updates

Session keys are not stored in non-volatile memory. They are automatically cleared when power is turned off, so there is no need to delete them; new Session Keys are automatically generated and exchanged whenever required.

During the normal course of data transfer, the transmitting node counts the time between Session Key changes. Prior to this count exceeding a pre-configured interval, it sends a Session Key update message to the other end of the connection. When a key exchange is successfully completed, the transmitting end of the connection starts using the new key. The receiving end of the connection keeps both keys to allow decryption of delayed packets with the correct key.

Incomplete Session Key Update

If the Session Key update is not completed successfully, the current key continues to be used until the configured session time expires. Once expired, encryption ceases and the appropriate alarms are generated. Refer to the *Vanguard Applications Ware Alarms and Reports Manual* (T0005) for additional information on these reports.

Disabled Connection

If a connection is disabled because key exchange and authentication has failed, the system attempts to exchange a Session Key and re-establish the connection each time a new data packet has to be sent. The encryption module also accepts control messages from the remote end even though the connection is disabled.

Base Key Changes

If the base keys have been changed in the node on one end of a connection but have not yet been changed in the node on the other end, each transmitter continues to encrypt data with the current session key. Each receiver continues to decrypt data with the current session key but can not successfully decrypt a periodic session key update message.

Preserving Uninterrupted Data Flow

To preserve uninterrupted data flow between the exchange of two session keys, the length of the current session time must be configured long enough to ensure that the base key can be changed on both sides during the time of the exchange.

■ **Note**

> Before changing the base key, check the statistics for that particular connection and verify that there is sufficient time left before a new session key exchange starts.

Encryption Synchronization

When an encrypted frame is lost, depending on the type of encapsulation used, two scenarios (see Figure 4) occur.

1) If an initialization vector for CBC DES is not sent with each packet, the receiver detects an invalid data integrity check field in the next frame. This happens because decrypting the frame in CBC mode requires use of the last eight bytes of cypher text from the previous (lost) frame.

2) The system discards frames received with an invalid data integrity check field. However, without further lost frames, the next frame is decrypted correctly and decryption recovers synchronization without need for any reset protocol.

When the initialization vector is sent with each packet, after one packet is lost the next packet is decrypted correctly.

Vanguard Software Data Compression

The Vanguard 320, 340, 340E, 342 and 7300 nodes have data compression capability built into the operating software and require no additional hardware.

Concurrent Data Compression with Encryption

Data Encryption and Compression can be performed concurrently on the same connection by configuring the Network Security Feature Table.

Data compression encoding always occurs before encryption. Encryption removes redundancy from the data, so there is no gain from data compression if encryption is done first. Since data compression is performed in the network security layer, before data is placed on a network protocol stack that is enabled for encryption, compression is done before encryption and decompression is done after decryption.

Protocol Support for Data Encryption

Introduction

This section describes the current protocol support of the Vanguard Managed Solutions' implementation of data encryption. Refer to Figure 12 for additional information.

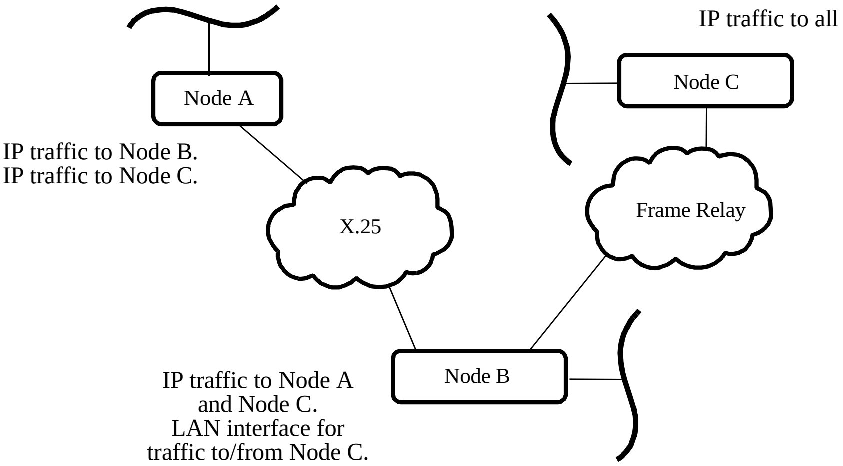


Figure 12. Protocol Support

X25 Access Port Traffic

All X.25 application port SVCs on Node A (Figure 12) are encrypted with a Base Key. Some of the virtual circuits are terminated at serial ports found in Node B, while other virtual circuits pass through Node B and terminate in Node C.

■ **Note**

Node B acts as either a Frame Relay or X.25 switch for these virtual circuits and passes the data transparently. All SVC calls from an X.25 port must use the same encryption profile.

IP & LAN Traffic

IP traffic from Node A (Figure 12) is encrypted and then decrypted in Node B before being passed on to the IP router of Node B. This router has another encrypted LAN interface to connect to the corresponding LAN interface in Node C.

Parallel SVCs are not be supported by the current version of Data Encryption; only single SVC support is available.

Serial Traffic

Encryption on each VC is intended to protect data from being attacked using different Base Keys and different encryption strengths. The use of different Base Keys, belonging to different encryption security groups, does not automatically segment users to different secure user groups, preventing access from one group to another. Once data is decrypted within a node, it can be routed to any other node; user group restriction can only be set up by applying filters and routing restricting on the node.

Caution

It is important to remember that overall data security is only as good as that found at the weakest link in the system.

CTP Access to an Encrypted Node

Introduction

The most vulnerable security component in and encrypted network, is the CTP port. VanguardMS has significantly reduced the possibility of compromised security, by incorporating encryption into remote CTP access by using either a Node Key or CTP Key for authentication.

Secure CTP Connections

You must configure Data Encryption CMEM records via the CTP. In order to ensure security of configuration and key configuration, all CTP access to an encryption enabled node is encrypted. This prevents unauthorized observation, of the CTP session, when access is over an un-secured public network. A node is considered encryption enabled, and encrypted CTP access is enforced, if the “Enable Encryption” parameter in the “Encryption Parameters” CMEM record is set to “Enable.”

Connecting to an Encryption Enabled Node

When connected to the CTP on an encryption enabled node, you must provide a valid secret key (Node Key or CTP Key) for the node. If access is being made from a remote node (via X25 or FR/Annex-G) the key you enter is used to setup an encryption channel between the remote calling node and local node. After the encrypted channel is established, normal CTP operation continues (with the exception of X25 or Annex-G link when traffic is encrypted). This requires that the call originate from a PAD/ATPAD port on an encryption enabled Vanguard node.

PAD or ATPAD Port

If the access terminal is connected to a local PAD or ATPAD port, on the same node, the entered keys are checked against the Node Key, no encryption session is set up for this case, but entry to the CTP is granted only if the correct keys are provided.

As mentioned in previous sections, you can gain access to CTP of an encryption enabled node using either the Node Key or the CTP key. You must tell the system which key you plan to use by entering either “NODE” or “CTP” when prompted to enter the key type.

Full CTP Access

Full CTP access is granted if you log-in using the Node Key. Logging in within the CTP key allows you to perform every CTP function except Changing, Examining, or Listing encryption related CMEM records. These include the Node Key, the Base Key, the encryption profile and the encryption parameters records. You cannot Copy or Boot encryption records.

If the correct keys are entered, then the user is connected to the CTP, and the CTP session is protected by encryption.

If the wrong keys are entered, the system outputs the following message
(after approximately 9 seconds):

Secure Access Authentication Failure, Give Correct Key

At this time, the key information must be entered again.

Full Access From a Dedicated CTP Port

One way to gain access to CTP operation, without having to provide either the Node Key or CTP key, is by direct access via the dedicated CTP port of the node. This provides ‘last resort access’ to the node in case both keys have been forgotten.

Though still required to provide the correct CTP password in order to gain access to the dedicated CTP port, the dedicated CTP port is relatively insecure compared to normal access by providing the correct encryption keys and the CTP password. For this reason, physical access to the dedicated CTP port should be limited to the System Administrator.

Access via Telnet

Vanguard products support encrypted CTP operation, from a PAD or ATPAD port on another Vanguard. Although direct encrypted CTP operation from Telnet is not currently supported, it is possible for a PC or workstation connected to a LAN to telnet to an encryption enabled node, and then start an encrypted CTP operation to a remote node via ATPAD. Figure 13 illustrates this situation.

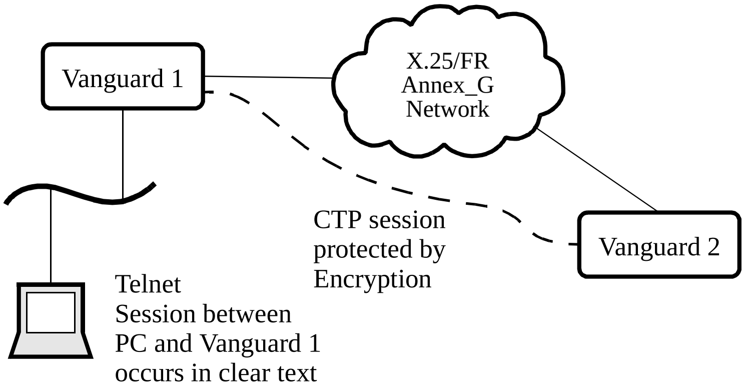


Figure 13. Access via Telnet

Since the Telnet session between the PC/workstation and the first Vanguard is not encrypted, the CTP message exchanges can be observed by illegal parties who simply monitor CTP traffic in clear text. The System Administrator should avoid using this configuration unless they are sure that the Telnet path is confined to a secure area.

Typical Data Encryption Configuration Example

Introduction

This section contains a typical example of a data encryption network and provides information necessary to configure the Vanguard products within it.

Typical Encrypted Network

Figure 14 illustrates a typical encrypted network. All Vanguard products shown in this figure are loaded with the appropriate Security Applications Ware license.

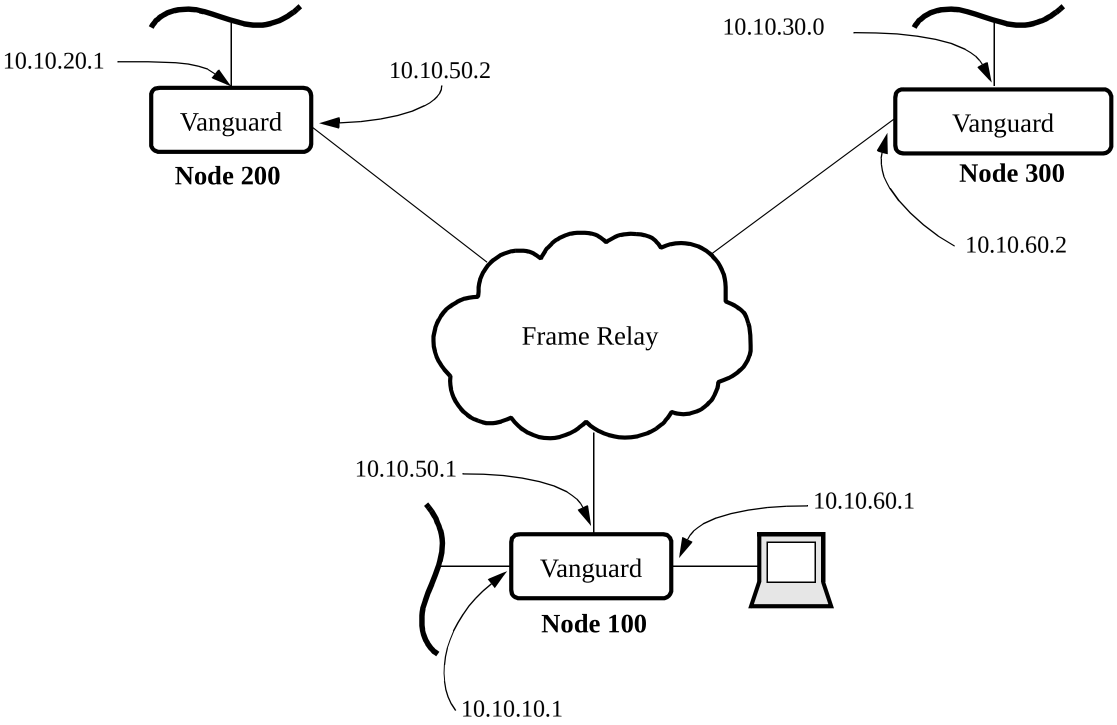


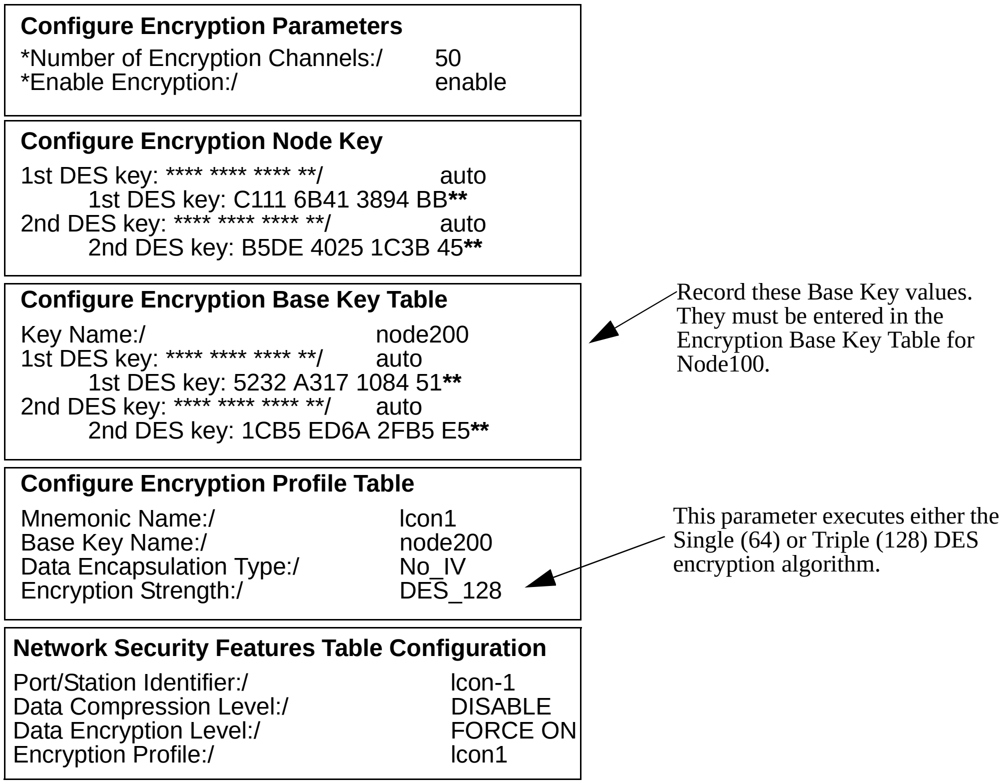
Figure 14. Example Configuration Network

■**Note**

The configuration of nodes in this example is done in this order: Node 200, Node 300, and Node 100.

Configuring Node200

Figure 15 illustrates the parameters that must be configured in Node 200, as shown in the configuration example:



```
Configure Encryption Parameters
*Number of Encryption Channels:/        50
*Enable Encryption:/                    enable

Configure Encryption Node Key
1st DES key: **** **** **** **/          auto
        1st DES key: C111 6B41 3894 BB**
2nd DES key: **** **** **** **/          auto
        2nd DES key: B5DE 4025 1C3B 45**

Configure Encryption Base Key Table
Key Name:/                         node200
1st DES key: **** **** **** **/    auto
        1st DES key: 5232 A317 1084 51**
2nd DES key: **** **** **** **/    auto
        2nd DES key: 1CB5 ED6A 2FB5 E5**

Configure Encryption Profile Table
Mnemonic Name:/                        lcon1
Base Key Name:/                        node200
Data Encapsulation Type:/              No_IV
Encryption Strength:/                  DES_128

Network Security Features Table Configuration
Port/Station Identifier:/                   lcon-1
Data Compression Level:/                    DISABLE
Data Encryption Level:/                     FORCE ON
Encryption Profile:/                        lcon1
```

Record these Base Key values. They must be entered in the Encryption Base Key Table for Node100.

This parameter executes either the Single (64) or Triple (128) DES encryption algorithm.

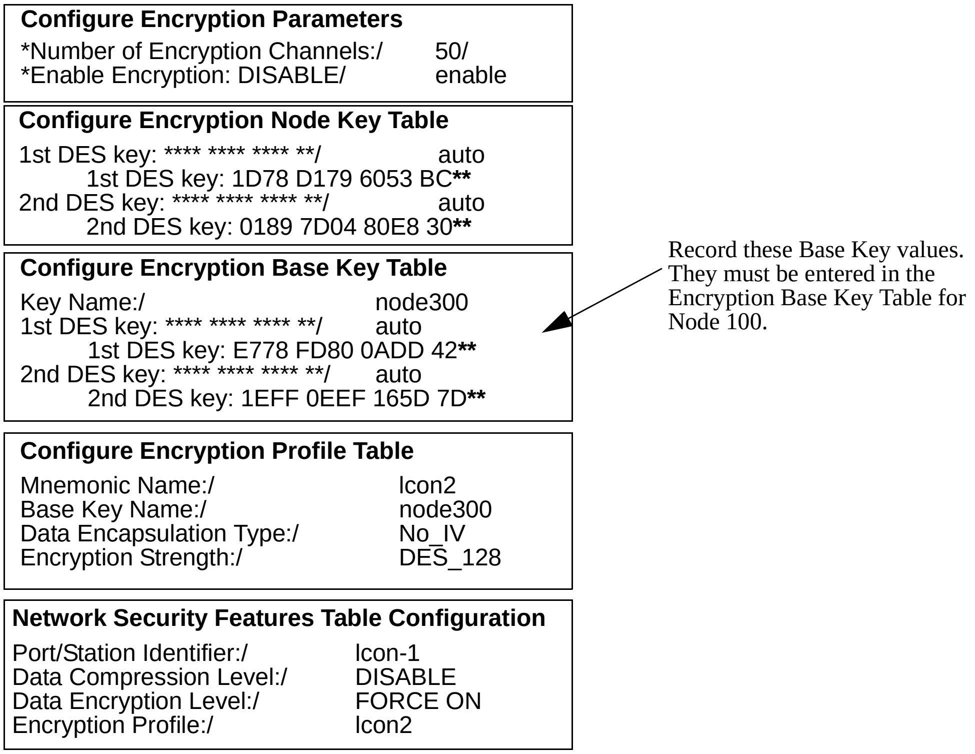
Figure 15. Node 200 Configuration

■Note

The Encryption Node and Base Key values (identified by **) are obtained from the random number generator. Refer to Encryption Keys on page 18 for additional information on randomly generated keys.

Configuring Node300

Figure 16 illustrates the parameters that must be configured in Node 300, as shown in the configuration example:



```
Configure Encryption Parameters
*Number of Encryption Channels:/       50/
*Enable Encryption: DISABLE/           enable

Configure Encryption Node Key Table
1st DES key: **** **** **** **/             auto
          1st DES key: 1D78 D179 6053 BC**
2nd DES key: **** **** **** **/             auto
          2nd DES key: 0189 7D04 80E8 30**

Configure Encryption Base Key Table
Key Name:/                            node300
1st DES key: **** **** **** **/       auto
          1st DES key: E778 FD80 0ADD 42**
2nd DES key: **** **** **** **/       auto
          2nd DES key: 1EFF 0EEF 165D 7D**

Configure Encryption Profile Table
Mnemonic Name:/                       lcon2
Base Key Name:/                       node300
Data Encapsulation Type:/             No_IV
Encryption Strength:/                 DES_128

Network Security Features Table Configuration
Port/Station Identifier:/             lcon-1
Data Compression Level:/              DISABLE
Data Encryption Level:/               FORCE ON
Encryption Profile:/                  lcon2
```

Record these Base Key values. They must be entered in the Encryption Base Key Table for Node 100.

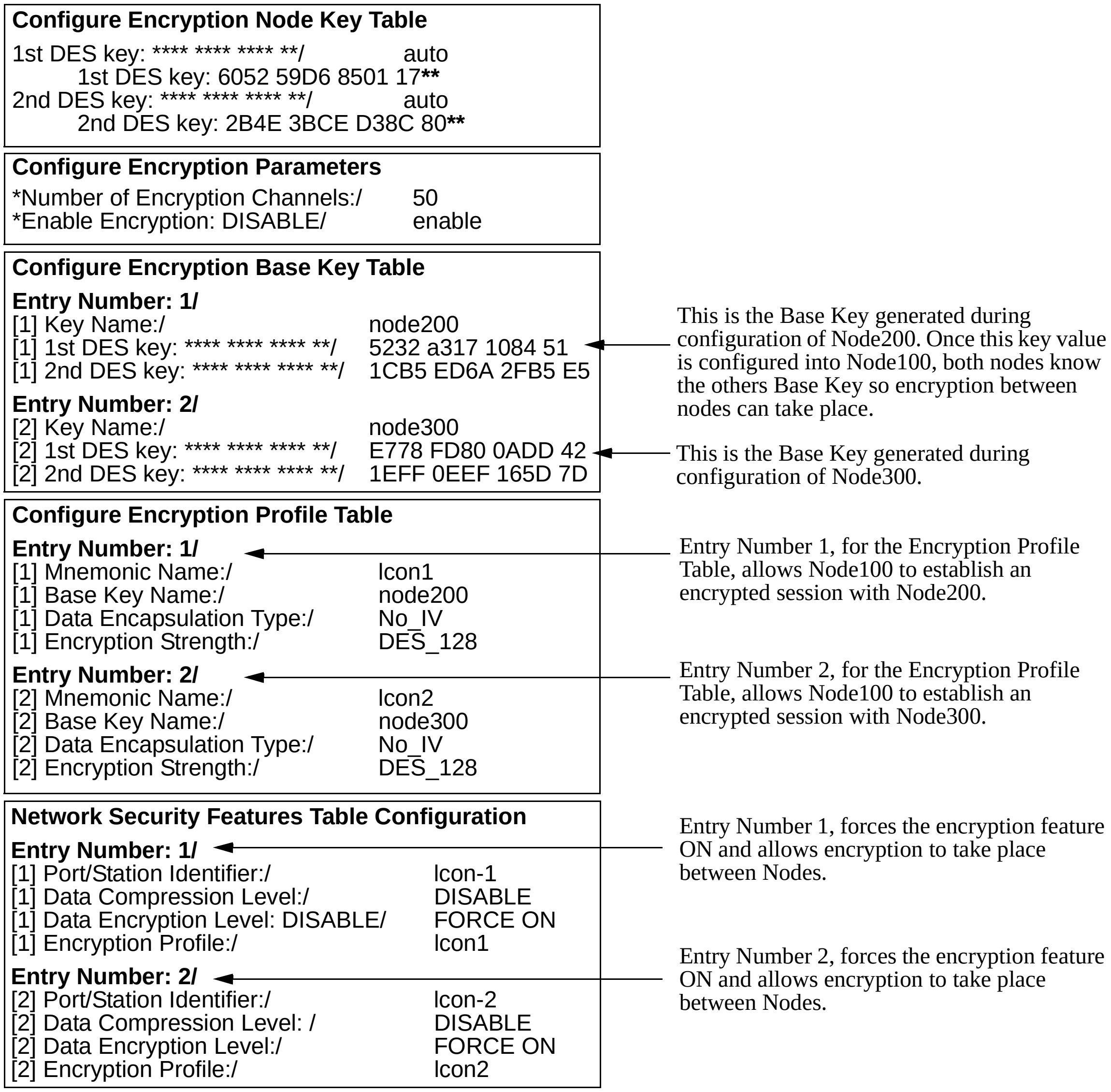
Figure 16. Node 300 Configuration

■Note

The Encryption Node and Base Key values (identified by **) are obtained from the random number generator. Refer to Encryption Keys on page 18 for additional information on randomly generated keys.

Configuring Node100

Figure 17 illustrates the parameters that must be configured in Node 100, as shown in the configuration example:



```
Configure Encryption Node Key Table
1st DES key: **** **** **** **/          auto
        1st DES key: 6052 59D6 8501 17**
2nd DES key: **** **** **** **/          auto
        2nd DES key: 2B4E 3BCE D38C 80**

Configure Encryption Parameters
*Number of Encryption Channels:/        50
*Enable Encryption: DISABLE/            enable

Configure Encryption Base Key Table
Entry Number: 1/
[1] Key Name:/                       node200
[1] 1st DES key: **** **** **** **/  5232 a317 1084 51
[1] 2nd DES key: **** **** **** **/  1CB5 ED6A 2FB5 E5
Entry Number: 2/
[2] Key Name:/                       node300
[2] 1st DES key: **** **** **** **/  E778 FD80 0ADD 42
[2] 2nd DES key: **** **** **** **/  1EFF 0EEF 165D 7D

Configure Encryption Profile Table
Entry Number: 1/
[1] Mnemonic Name:/                  Icon1
[1] Base Key Name:/                  node200
[1] Data Encapsulation Type:/        No_IV
[1] Encryption Strength:/            DES_128
Entry Number: 2/
[2] Mnemonic Name:/                  Icon2
[2] Base Key Name:/                  node300
[2] Data Encapsulation Type:/        No_IV
[2] Encryption Strength:/            DES_128

Network Security Features Table Configuration
Entry Number: 1/
[1] Port/Station Identifier:/                 Icon-1
[1] Data Compression Level:/                  DISABLE
[1] Data Encryption Level: DISABLE/           FORCE ON
[1] Encryption Profile:/                      Icon1
Entry Number: 2/
[2] Port/Station Identifier:/                 Icon-2
[2] Data Compression Level: /                 DISABLE
[2] Data Encryption Level:/                   FORCE ON
[2] Encryption Profile:/                      Icon2
```

This is the Base Key generated during configuration of Node200. Once this key value is configured into Node100, both nodes know the others Base Key so encryption between nodes can take place.

This is the Base Key generated during configuration of Node300.

Entry Number 1, for the Encryption Profile Table, allows Node100 to establish an encrypted session with Node200.

Entry Number 2, for the Encryption Profile Table, allows Node100 to establish an encrypted session with Node300.

Entry Number 1, forces the encryption feature ON and allows encryption to take place between Nodes.

Entry Number 2, forces the encryption feature ON and allows encryption to take place between Nodes.

Figure 17. Node 100 Configuration

■**Note**

The Encryption Node and Base Key values (identified by **) are obtained from the random number generator. Refer to Encryption Keys on page 18 for additional information on randomly generated keys.

Configuration Specifics

Introduction

You must access the Configure Network Security records menu and modify these Table records.

- Configuring Network Security Feature Tables on page 42
- Configure Network Security Menu on page 45
- Configure Encryption Parameters on page 46
- Configure Encryption Profile Table on page 48
- Configure Encryption Node Key Table on page 51
- Configuring the Encryption Base Key Table on page 53

■**Note**

Refer to the *Vanguard Basic Configuration Manual* (Part Number T0113) for additional information on configuring Vanguard products. When configuring for specific Applications Ware licenses, you should also refer to the Applications Ware Feature documentation for the protocols you are configuring.

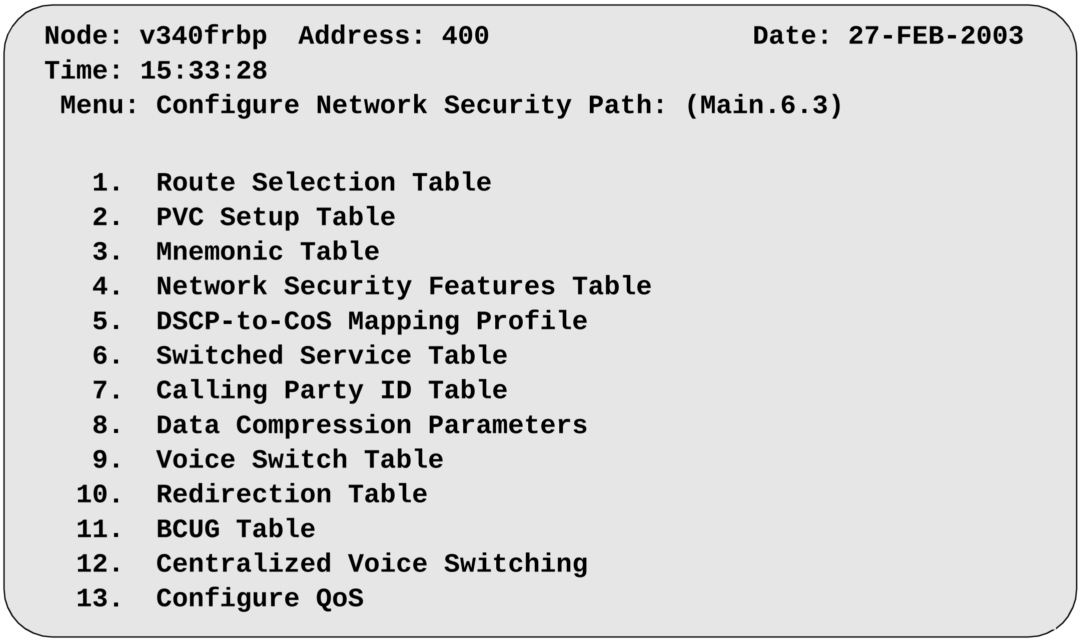
Configuring Network Security Feature Tables

Introduction

The Network Security Feature Table is used to configure the access port protocols to be encrypted when traffic is routed to the Network Port. If traffic from an LCON and SDLC are to be encrypted, the two access port end points must be configured in the corresponding entries in the Network Security Feature Table.

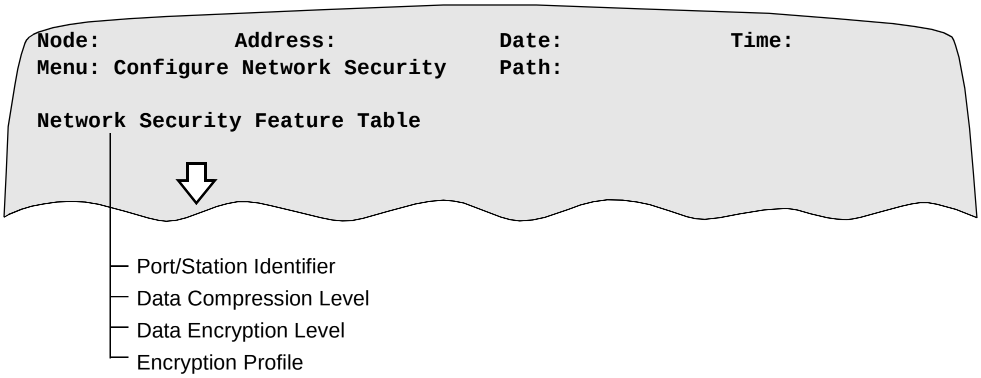
When you select Network Security Feature Table, from the Configure Network Security menu, you must configure the parameters shown in (Figure 19), and described below.

**Main Menu->Configure->Configure Network Security->
Network Security Features Table**



```
Node: v340frbp  Address: 400               Date: 27-FEB-2003
Time: 15:33:28
 Menu: Configure Network Security Path: (Main.6.3)

   1.  Route Selection Table
   2.  PVC Setup Table
   3.  Mnemonic Table
   4.  Network Security Features Table
   5.  DSCP-to-CoS Mapping Profile
   6.  Switched Service Table
   7.  Calling Party ID Table
   8.  Data Compression Parameters
   9.  Voice Switch Table
  10.  Redirection Table
  11.  BCUG Table
  12.  Centralized Voice Switching
  13.  Configure QoS
```

Figure 18. Configure Network Security



```
Node:           Address:            Date:              Time:
Menu: Configure Network Security    Path:

Network Security Feature Table
```

Figure 19. Configure Network Security Feature Table

Parameters

These are the parameters that must be configured:

Port/Station Identifier

Range:	0 to 31 alphanumeric characters
Default	blank
Description:	Identifies the port and station number that the Network Security feature(s) is enabled on. Enter an asterisk (*) as a wildcard character to match anything. These port types can be selected: • X25- (example: X25-1(16) or X25-1*) • FRA- (example: FRA-3S1 or FRA-3*) • LCON- (example: LCON-1 or LCON-*) • TCOP- (example: TCOP-1 or TCOP-*) • TBOP- (example: TBOP-1 or TBOP-*) • SDLC- (example: SDLC-2S1 or SDLC-3*) • LSC-TR (example: LSC-TR1 or LSC-TR*) • LSC-ETH- (example: LSC-ETH1 or LSC-ETH*) • LSC-FR (example LSC-FR1 or LSC-FR*) **■Note** You must use a hyphen, as indicated in these examples, and no leading spaces are required. The first Token Ring or Ethernet Port should use the format LSC-TRx or LSC-ETHx where “x” can be 1 to 256 and depicts the station number for that port. For example, correct entries for station 2 on Ethernet ports 5 and 10 should be as follows: **LSC-ETH2** (do not use LSC-ETH5s2) **LSC-ETH10s2** **■Note** If more than one token ring port is installed, a string of the following format should be used for the secondary Token Ring LLC to SDLC stations: **LSC-TR17sl** If more than one Ethernet Port is installed, a string of the following format should be used for the secondary Ethernet LLC to SDLC stations: **LSC-ETH151s1** **■Note** Use the space bar to blank this field.

■Note

To enable compression on a particular channel the Data Compression Level must be changed from Disable to another option (shown in the next parameter).

Data Compression Level

Range:	DISABLE, NEGOTIATE, REQUIRED, FORCE ON
Default	DISABLE
Description:	Specifies the Network Security features level. • DISABLE: Select this if the feature is not required. • NEGOTIATE: Select this if the feature is not available on both ends, and then bring the connection up without the feature. • REQUIRED: This is required for a call. Bring up the connection only if the feature is available on both ends. • FORCE ON: Select this if the feature is required for the circuit to come up. ■**Note** The use of 'feature' in the above descriptions represents the current feature you are configuring.

Data Encryption Level

Range:	DISABLE, FORCE ON
Default	DISABLE
Description:	Specifies the Encryption features level: • DISABLE: Data Encryption is not requested. • FORCE ON: Brings the connection up only if data encryption is available on both ends of the connection. ■**Note** To enable encryption, both ends of a connection must have this parameter set to FORCE ON.

Encryption Profile

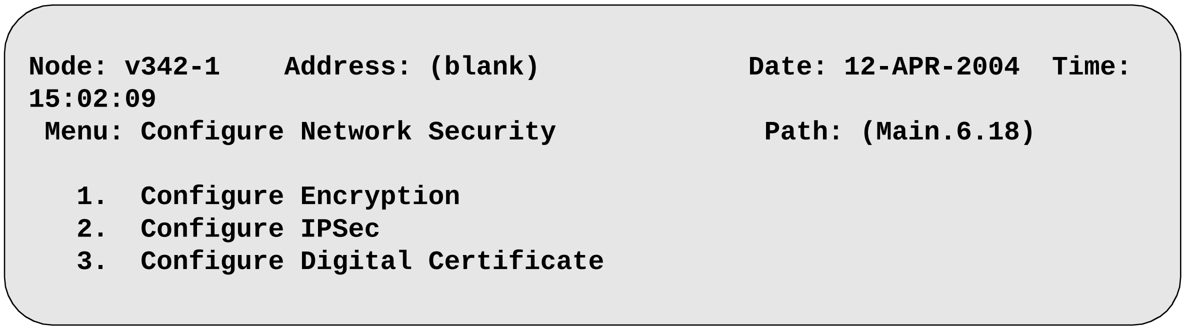
Range:	1 to 15 alphanumeric characters
Default	blank
Description:	Specifies the name of the encryption profile to be used when setting up the channel.

Configure Network Security Menu

Accessing The Configure Network Security Menu

To access the Network Security menu:

Main Menu->Configure->Configure Network Security



```
Node: v342-1    Address: (blank)            Date: 12-APR-2004  Time:
15:02:09
 Menu: Configure Network Security             Path: (Main.6.18)

   1.  Configure Encryption
   2.  Configure IPSec
   3.  Configure Digital Certificate
```

Figure 20. Configure Network Security

■**Note**

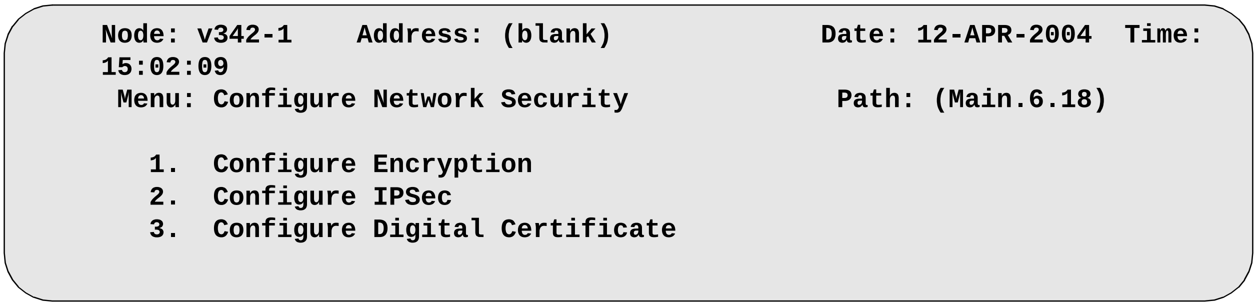
Vanguard 7300 Series platforms do not support the SAM encryption. The configuration options “Encryption Profile Tables” and “Base Key tables” are not shown for the 7300 Series.

Configure Encryption Parameters

Introduction

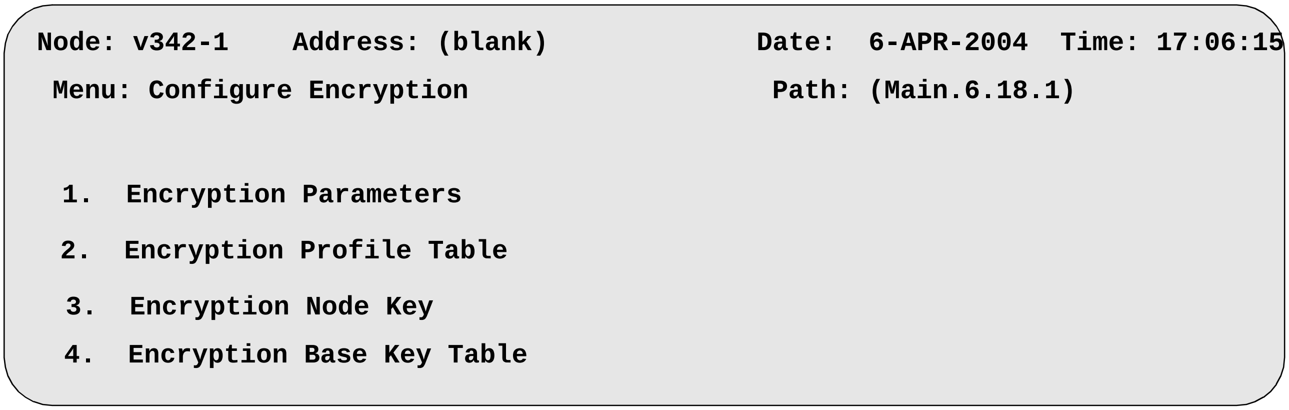
Follow these steps to access the Network Security Menu:

Step	*Action*	*Result*
1	Select **Configure**, from the CTP Main menu.	The Configure menu appears.
2	Select **Configure Network Security**.	The Configure Network Security Menu is shown.
3	Select **Configure Encryption**.	



```
      Node: v342-1    Address: (blank)            Date: 12-APR-2004  Time:
      15:02:09
       Menu: Configure Network Security            Path: (Main.6.18)

          1.  Configure Encryption
          2.  Configure IPSec
          3.  Configure Digital Certificate
```

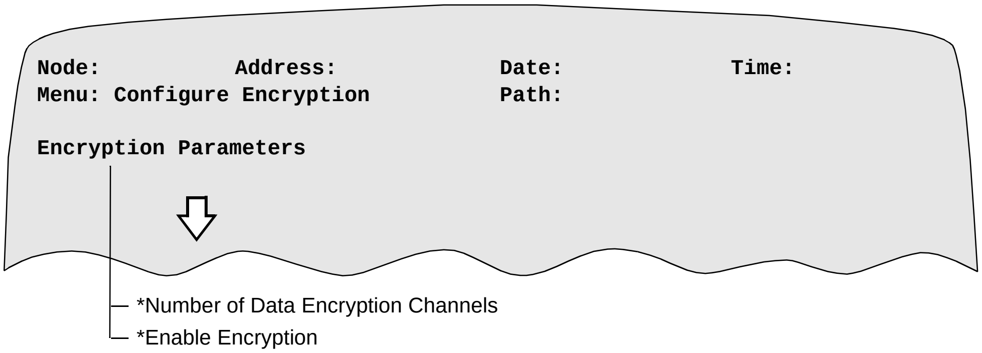
Figure 21. Configure Network Security



```
 Node: v342-1    Address: (blank)            Date:  6-APR-2004  Time: 17:06:15
  Menu: Configure Encryption                  Path: (Main.6.18.1)


   1.  Encryption Parameters

   2.  Encryption Profile Table

   3.  Encryption Node Key

   4.  Encryption Base Key Table
```

Figure 22. Configure Encryption

When you select Encryption Parameters, from the Configure Encryption menu, you must configure the parameters shown in Figure 23, and described below.



```
Node:          Address:            Date:            Time:
Menu: Configure Encryption         Path:

Encryption Parameters
```

Figure 23. Encryption Parameters

Parameters

These are the Data Encryption parameters:

Note

Unless otherwise indicated, perform a Node boot for changes to these parameters to take effect.

*Number of Encryption Channels

Range:	10 to 500
Default	50
Description:	Specifies the maximum number of data encryption channels to be created.

*Enable Encryption

Range:	ENABLE, DISABLE
Default	DISABLE
Description:	• ENABLE - Enables the data encryption feature on this node. • DISABLE - Disables the data encryption feature on this node.

Configure Encryption Profile Table

Introduction

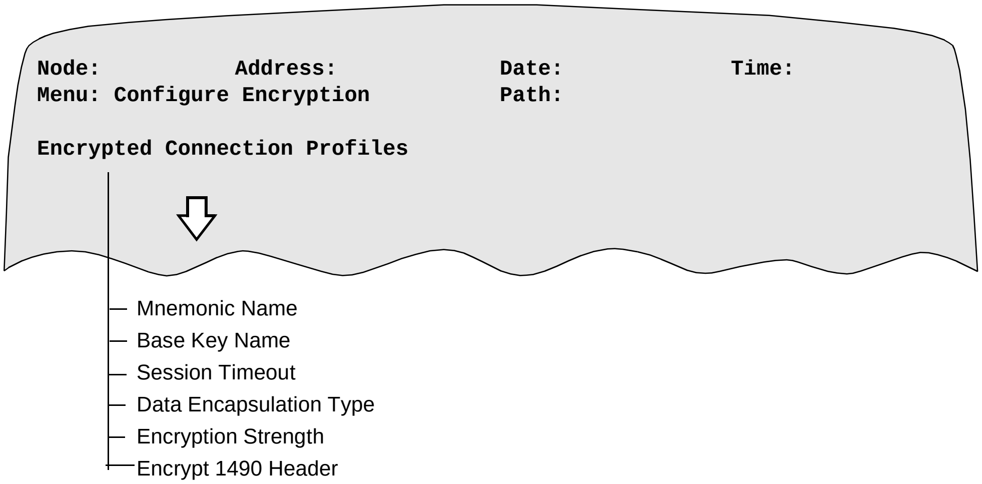
The encryption profile specifies the requirements for a specific encryption session. Once configured, an encryption profile can be referred to by several connections, thereby eliminating the need to configure the same information over, and over again. Each profile is associated with:

- a mnemonic name
- the name of the base key used for the connection
- allowed session duration time
- the type of the encapsulation and encryption algorithm used

The encapsulation type used specifies whether the encryption initialization vector and sequence number are sent with each data packet. It also specifies which data integrity check type is used.

■Note

Although any changes made to an encryption profile are immediately stored in memory, the data encryption feature does not make them available until the next session key exchange. The current session is not interrupted, or modified, by the changes.



```
Node:          Address:            Date:            Time:
Menu: Configure Encryption         Path:

Encrypted Connection Profiles
```

Figure 24. Encrypted Connection Profiles

Parameters

These are the Data Encryption parameters:

Mnemonic Name

Range:	1 to 15 alphanumeric characters
Default	blank
Description:	Specifies the name of the encrypted link profile and is referred to in the Network Service Tables.

Base Key Name

Range:	1 to 16 alphanumeric characters
Default	Blank
Description:	Specifies the mnemonic name of the Base Key to be used for the encryption session. The Base Key table must be configured with an entry that is identified by the same name. ■**Note** Use the space bar to blank this field.

Session Time (minutes)

Range:	5 to 65536
Default	1440
Description:	Specifies the length, in minutes, of the encryption session timer. ■**Note** A new Session Key is automatically generated when this timer expires.

Data Encapsulation Type

Range:	IV, NoIV
Default	NoIV
Description:	Specifies the initialization vector (IV) to be used: • IV - each data packet contains the 8 byte initialization vector. • NoIV - An IV, from the previous packet, is used by the next packet. Select this option if the session is conducted over a connection oriented protocol such as: X.25 or ANNEX-G.

Encryption Strength

Range:	DES_64, DES_128
Default	DES_64
Description:	Specifies the encryption algorithm to be used: • DES_64 - DES. • DES_128 - Triple-DES Encryption key strength (DES_64 for 64 bits, DES_128 for 128 bit)

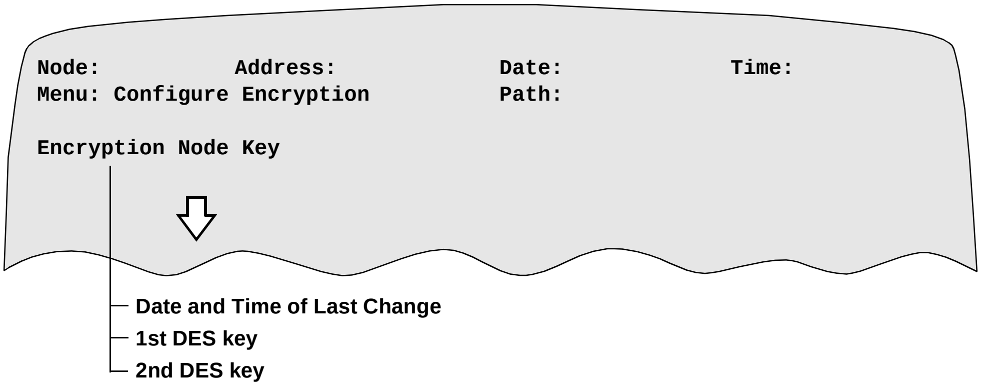
Encryption 1490 Header

Range:	NO, YES
Default	NO
Description:	N/A

Configure Encryption Node Key Table

Introduction

When you select Encryption Node Key, from the Configure Encryption menu, you must configure the parameters shown in Figure 25, and described below.



```
Node:           Address:            Date:            Time:
Menu: Configure Encryption          Path:

Encryption Node Key
```

Figure 25. Encryption Node Key Table

Parameters

These are the Encryption Node Key parameters that must be configured:

Date and Time of Last Change

Range:	real time
Default	(blank)
Description:	Specifies the date and time that the Node Key was last changed. The system automatically enters this information, if the Node Key has never been changed, this field may be blank. ■ **Note** Do not attempt to modify this parameter. Any changes that you make to the Date and Time of Last Change parameter is ignored by the system.

1st DES key

Range:	AUTO, 14 hexadecimal digits
Default	**** **** **** **
Description:	Specifies a new Base Key value. • AUTO: Enter this to allow the random number generator to automatically create a new Base Key value. • ****_****_****_**: Enter 14 hexadecimal numbers to represent the Base Key. You must enter the spaces (as indicated in this table by underscores) in the locations shown here. ■**Note** This is a write only field that is displayed only once. You must record this value. ■**Note** An all zero default value (0000...0) is used to prevent accidental overwriting of the key value. This all zero value is a known weak DES key and it is therefore rejected by the system.

2nd DES key

Range:	AUTO, 14 hexadecimal digits
Default	**** **** **** **
Description:	Specifies a new Base Key value. • AUTO: Enter this to allow the random number generator to automatically create a new Base Key value. • ****_****_****_**: Enter 14 hexadecimal numbers to represent the Base Key. You must enter the spaces (as indicated in this table by underscores) in the locations shown here. ■**Note** This is a write-only field that is displayed only once. You must record this value. ■**Note** An all zero default value (0000...0) is used to prevent accidental overwriting of the key value. This all zero value is a known weak DES key and it is therefore rejected by the system.

Configuring the Encryption Base Key Table

Introduction

Each Base Key Table entry is associated with:

- a mnemonic key name
- a base key (hexadecimal) value
- the date and time of the last change

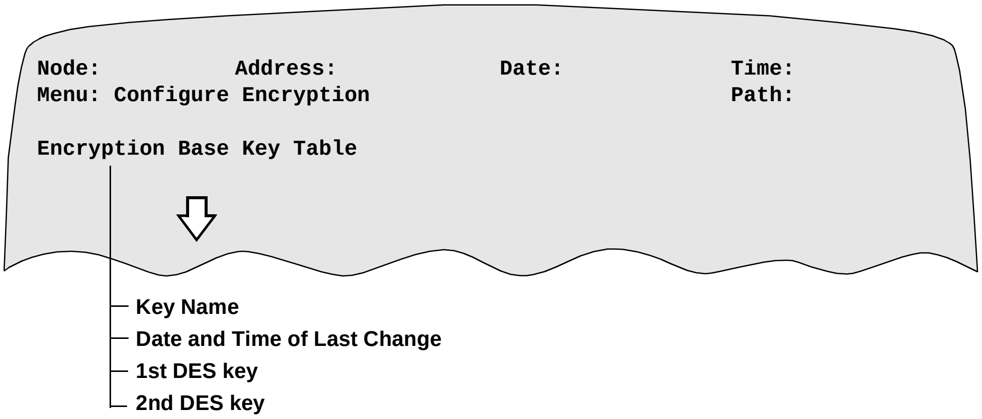
If "auto" is typed in and return is pressed for the key value, The Encryption option automatically generates a key whenever a Base Key value of "auto" is entered. The Base Key value is only displayed once, to allow you to record it. Whenever this key is displayed after that, it appears as fourteen X's.

The system automatically enters the date and time whenever the key is changed or a new key is entered. You can use this read-only field to verify that no unauthorized changes have been made.

■Note

You must keep a record of the time and date all changes are made. If you enter the same base Key value, the date and time of the last modification is not changed.

It should be noted that any changes made in the base key table, even after booting the new keys, are not used by the system until the next session key exchange. The current session is not effected by the changes.



```
Node:          Address:            Date:              Time:
Menu: Configure Encryption                            Path:

Encryption Base Key Table
```

Figure 26. Encryption Base Key Table

Parameters

These are the Encryption Base Key Table parameters:

Base Key Name

Range:	1 to 15 alphanumeric characters
Default	Blank
Description:	Specifies the mnemonic name of the Base Key to be used for the encryption session. ■**Note** Use the space bar to blank this field.

Date and Time of Last Change

Range:	real time
Default	(blank)
Description:	Specifies the date and time that the Node Key was last changed. The system automatically enters this information, if the Node Key has never been changed, this field may be blank. ■**Note** Do not attempt to modify this parameter. Any changes that you make to the Date and Time of Last Change parameter is ignored by the system.

1st DES key

Range:	AUTO, 14 hexadecimal characters
Default	**** **** **** **
Description:	Specifies a new Base Key value. • AUTO: Enter this to allow the random number generator to automatic create a key value. • ****_****_****_**: Enter 14 hexadecimal numbers to represent the Base Key. You must enter the spaces (as indicated in this table by underscores) in the locations shown here. ■**Note** This is a write only field that is displayed only once. You must record this value. ■**Note** An all zero default value (0000...0) is used to prevent accidental overwriting of the key value. This all zero value is a known weak DES key and it is therefore rejected by the system.

2nd DES key

Range:	AUTO, 14 hexadecimal characters
Default	**** **** **** **
Description:	Specifies a new Base Key value. • AUTO: Enter this to allow the random number generator to automatic create a key value. • ****_****_****_**: Enter 14 hexadecimal numbers to represent the Base Key. You must enter the spaces (as indicated in this table by underscores) in the locations shown here. ■ **Note** This is a write only field that is displayed only once. You must record this value. ■ **Note** An all zero default value (0000...0) is used to prevent accidental overwriting of the key value. This all zero value is a known weak DES key and it is therefore rejected by the system.

Examine, List, Copy and Boot Record

Introduction

The Examine, List, Copy and Boot functions are standard commands which have been extended to support Data Encryption. However, security restriction makes it necessary to implement some functional modifications for Data Encryption.

Functional Modifications for Data Encryption

This table identifies the restrictions introduced to the Examine, List, Copy, Boot and Delete functions to support Data Encryption. In the table below a “Yes” indicates that the Vanguard router supports the operation, and a “No” indicates the Vanguard Router does not support the operation. Some restrictions do apply, and are referenced by number 1 or 2 in the table.

Operation	*Encryption Parameters*	*Encryption Profile*	*Node Key*	*Base Key*
Examine	Yes	Yes	No	[1]Yes
List	Yes	Yes	No	[1]Yes
Copy	No	Yes	No	Yes
Boot	No	Yes	No	Yes
Delete	No	Yes	[2]No	Yes

■ **Note**

[1] The Base Key Table may be seen, but the actual keys are not displayed for security reasons.

[2] The node key may not be deleted on its own. However, selecting “Delete All Encryption Keys” would delete the node key also.

Statistics

Introduction

These statistics are available:

- Data Encryption General Statistics
- Data Encryption Channel Statistics
- Data Encryption All Channel Statistics
- Data Encryption Summary Statistics
- Reset Data Encryption Channel Statistics
- Reset All Data Encryption Statistics

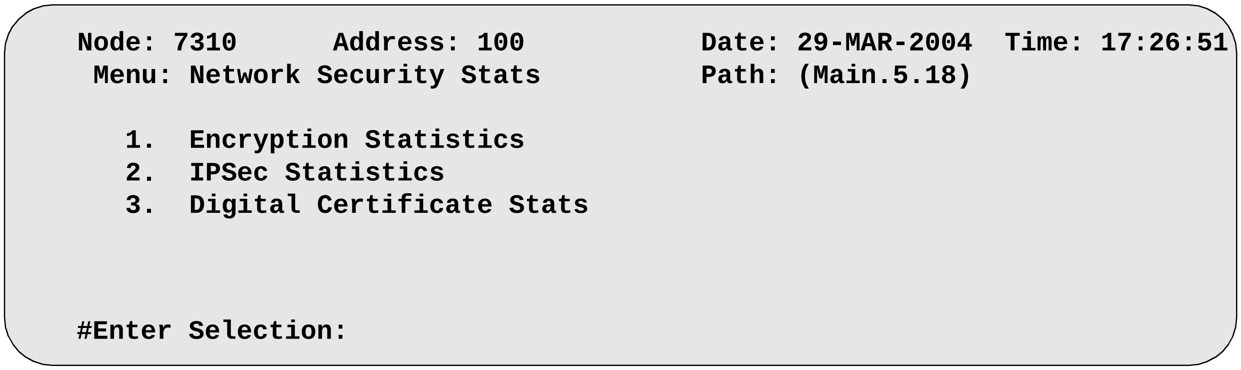
■**Note**

Vanguard 7300 Series platforms do not support SAM encryption. Certain SAM specific menu items in Examine, List, Copy, Delete, Stats and Configuration menus are not shown on the Vanguard 7300.

Examining Encryption Statistics

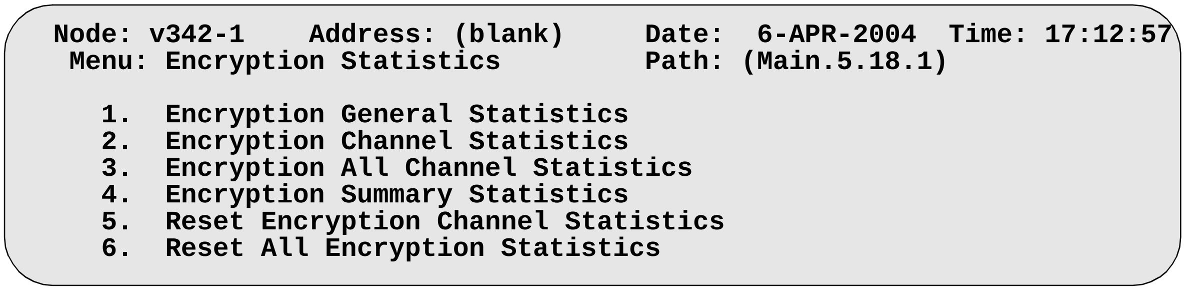
Follow the steps below to view the Data Encryption statistics:

Step	***Action***	***Result***
1	Select **Status/Statistics**, from the CTP Main menu.	The Status/Statistics menu appears.
2	Select **Network Security Stats**.	The Network Security Stats menu, similar to that shown in Figure 27 is displayed.
3	Select **Encryption Statistics**.	



```
Node: 7310      Address: 100          Date: 29-MAR-2004  Time: 17:26:51
 Menu: Network Security Stats         Path: (Main.5.18)

   1.  Encryption Statistics
   2.  IPSec Statistics
   3.  Digital Certificate Stats



#Enter Selection:
```

Figure 27. Network Security Statistics



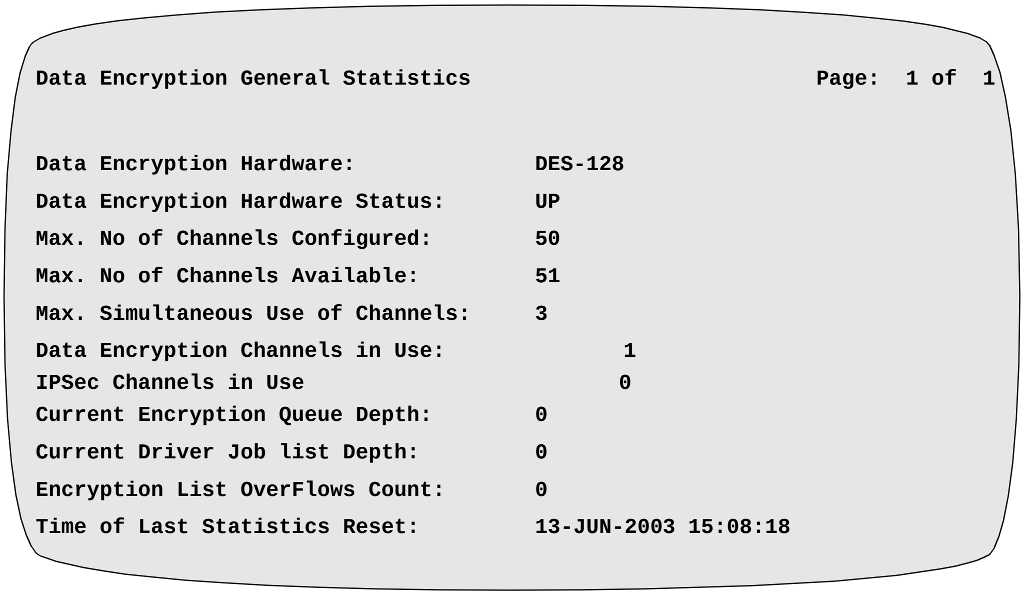
```
Node: v342-1    Address: (blank)     Date:  6-APR-2004  Time: 17:12:57
 Menu: Encryption Statistics         Path: (Main.5.18.1)

   1.  Encryption General Statistics
   2.  Encryption Channel Statistics
   3.  Encryption All Channel Statistics
   4.  Encryption Summary Statistics
   5.  Reset Encryption Channel Statistics
   6.  Reset All Encryption Statistics
```

Figure 28. Encryption Statistics

Encryption General Statistics

Introduction

The Encryption General Statistics screen (Figure 29) is displayed for all statistics that pertain to the Data Encryption feature.



```
Data Encryption General Statistics                           Page:  1 of  1


Data Encryption Hardware:              DES-128
Data Encryption Hardware Status:       UP
Max. No of Channels Configured:        50
Max. No of Channels Available:         51
Max. Simultaneous Use of Channels:     3
Data Encryption Channels in Use:              1
IPSec Channels in Use                         0
Current Encryption Queue Depth:        0
Current Driver Job list Depth:         0
Encryption List OverFlows Count:       0
Time of Last Statistics Reset:         13-JUN-2003 15:08:18
```

Figure 29. Data Encryption General Statistics Screen

Encryption General Statistics Screen Terms

All statistics are computed since the last statistics reset or node boot. This table describes the terms found in Figure 29.

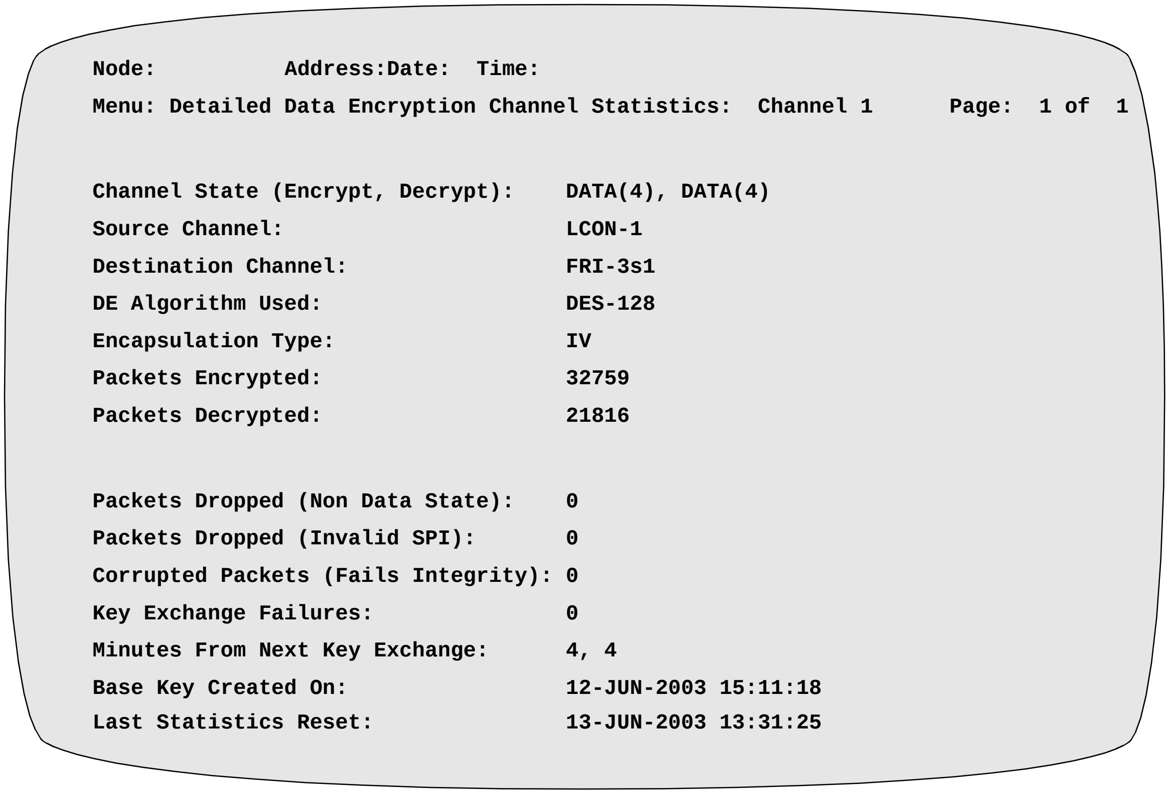
Term	*Indicates...*
Data Encryption Hardware	Data Encryption algorithm supported by hardware: • DES-64 - DES • DES-128 - 2 key Triple-DES • AES, 3DES, DES
Data Encryption Hardware Status	Identifies the current status/existence of Data Encryption hardware. • UP: Data encryption hardware is installed and operational. • DOWN: Data encryption hardware is non-functional.
DE algorithm supported by H/W	Default Encryption algorithm supported by hardware: • DES-64 - DES • DES-128 - Triple-DES

Term	***Indicates...*** *(continued)*
Data Encryption Software Status	Identifies the current status of the data encryption software. • Enabled: DE module is present and running • Disabled: DE module is present but not used
Max No.of Channels Available	Identifies the number of DE Channels (15 to 500) supported by the Data encryption hardware installed on the node.
Max No. of Channels Configured	Identifies the maximum number of DE Channels (0 to 500) configured for use. This parameter is used to control the amount of RAM that gets allocated for Data Encryption during node initialization.
Data Encryption Channels in Use	Identifies the number of Data Encryption Channels (0 to 500) that are assigned and are currently in use by the calls.
IPSec Channels in Use	Identifies the number of IPSec Channels (0 to 500) that are currently in use by the calls.
Max. Simultaneous use of Channels	Identifies the maximum number of data encryption channels (0 to 500) in use simultaneously since the last stats reset.
Encryption List OverFlows Count	The number of times (0 to 65535) that an overflow condition occurred in the queue.
Current Encryption Queue Depth	Current number of frames (0 to 65535) in the queue, waiting to be encrypted or decrypted.
Current Driver Job list Depth	The number of packets waiting to be encrypted/ decrypted by the Data Encryption SIMM.
Time of the Last Statistics Reset	Identifies the time when the node restarted or the stats reset by CTP/SNMP Manager command.

Encryption Channel Statistics

Introduction

The Encryption Channel Statistics screen is displayed for each encrypted channel (Figure 30).



```
Node:          Address:Date:  Time:
Menu: Detailed Data Encryption Channel Statistics:  Channel 1      Page:  1 of  1


Channel State (Encrypt, Decrypt):    DATA(4), DATA(4)
Source Channel:                      LCON-1
Destination Channel:                 FRI-3s1
DE Algorithm Used:                   DES-128
Encapsulation Type:                  IV
Packets Encrypted:                   32759
Packets Decrypted:                   21816


Packets Dropped (Non Data State):    0
Packets Dropped (Invalid SPI):       0
Corrupted Packets (Fails Integrity): 0
Key Exchange Failures:               0
Minutes From Next Key Exchange:      4, 4
Base Key Created On:                 12-JUN-2003 15:11:18
Last Statistics Reset:               13-JUN-2003 13:31:25
```

Figure 30. Encryption Channel Statistics Screen

Encryption Channel Statistics Screen Terms

All statistics are computed since the last statistics reset or node boot. This table describes the terms found in Figure 30.

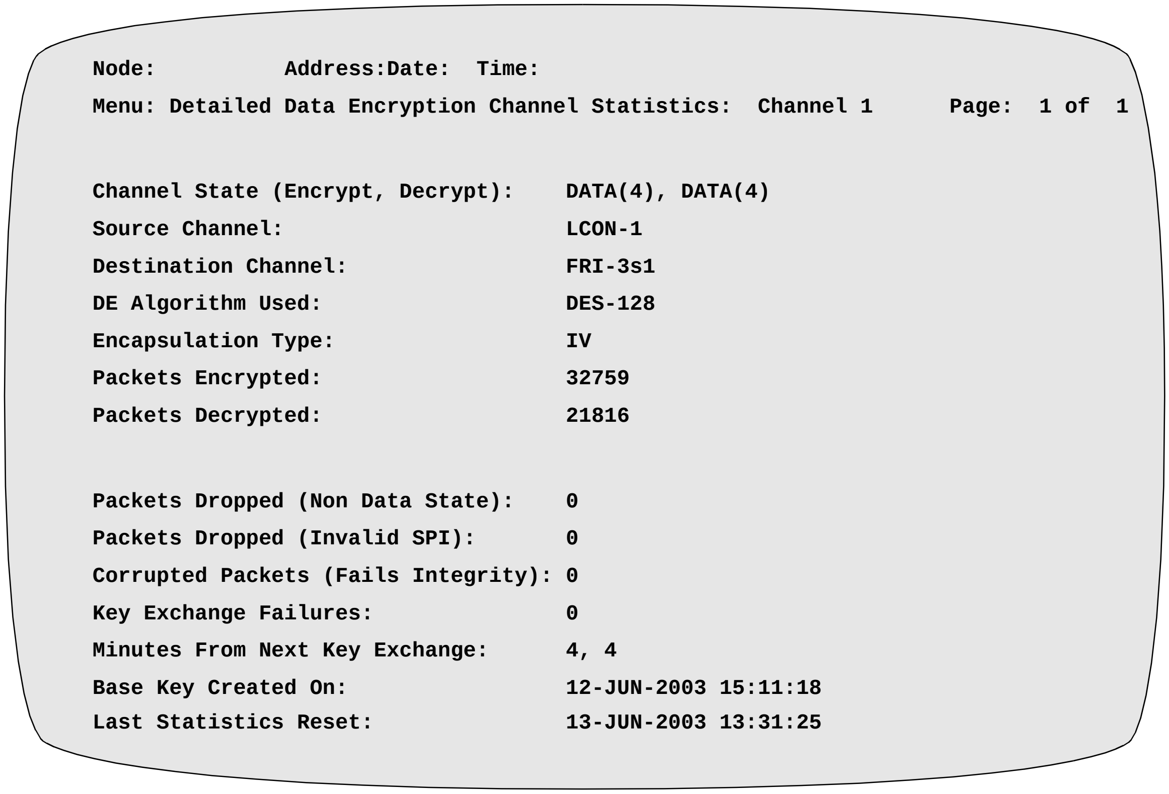
Term	*Indicates...*
Channel State (Encrypt, Decrypt)	Identifies the activity state of the channel for each direction. • Data: Indicates that normal data is passing through the channel. • No Data: Indicates that a channel is blocked for data traffic.
Source Channel	Identifies the access protocol’s identity string.
Destination Channel	Identifies the network protocol’s identity string.
DE Algorithm used	Identifies the encryption algorithm used. • DES-64 - DES • DES-128 - Triple-DES

Term	**Indicates...** *(continued)*
Encapsulation Type	Identifies the type of encapsulation used: • IV - DES initialization vector sent with each packet • No-IV - Last 8 bytes of the previous packet used for DES algorithm initialization
Packets Encrypted	The number of packets encrypted since the last statistics reset.
Packets Decrypted	The number of packets decrypted since the last statistics reset.
Corrupted Packets (Bad CRC)	Identifies the number of decrypted packets encountered with false data integrity check fields.
Packets Dropped (Non Data State)	The number of packets dropped before the encryption session was established.
Packets Dropped (Invalid SPI)	The number of packets dropped because they do not belong to the current session.
Key Exchange Failures	Identifies the number of key exchange attempts (0 to 232-1) that have not been completed successfully since the last stats reset.
Minutes from next key exchange	The maximum number of minutes allowed for this session. The actual key exchange however, may happen before this time expires if the other end of the connection requires it.
Base Key Created On:	Identifies the last time a base key was used for this connection (since booted).
Last Statistics Reset	Identifies the time that the channel stats were reset by a CTP or SNMP Manager command.

Encryption All Channel Statistics

Introduction

The Encryption All Channel Statistics screen is displayed for each encrypted channel (Figure 31).



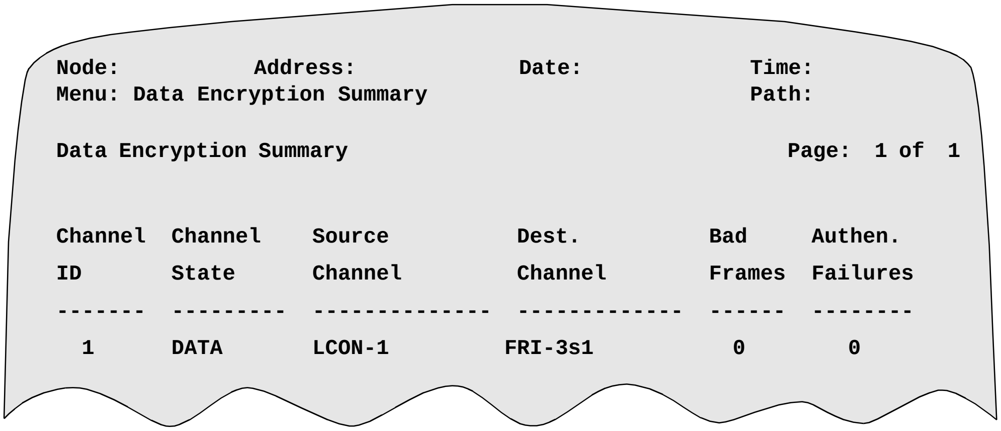
```
Node:          Address:Date:  Time:
Menu: Detailed Data Encryption Channel Statistics:  Channel 1      Page:  1 of  1


Channel State (Encrypt, Decrypt):    DATA(4), DATA(4)
Source Channel:                      LCON-1
Destination Channel:                 FRI-3s1
DE Algorithm Used:                   DES-128
Encapsulation Type:                  IV
Packets Encrypted:                   32759
Packets Decrypted:                   21816


Packets Dropped (Non Data State):    0
Packets Dropped (Invalid SPI):       0
Corrupted Packets (Fails Integrity): 0
Key Exchange Failures:               0
Minutes From Next Key Exchange:      4, 4
Base Key Created On:                 12-JUN-2003 15:11:18
Last Statistics Reset:               13-JUN-2003 13:31:25
```

Figure 31. Encryption All Channel Statistics Screen

Data Encryption Summary Statistics

Introduction

The Data Encryption Summary Statistics screen (Figure 32) contains statistics for all channels that are currently in use.



```
Node:           Address:            Date:             Time:
Menu: Data Encryption Summary                         Path:

Data Encryption Summary                                  Page:  1 of  1


Channel  Channel    Source          Dest.          Bad     Authen.
ID       State      Channel         Channel        Frames  Failures
-------  ---------  --------------  -------------  ------  --------
  1      DATA       LCON-1         FRI-3s1          0        0
```

Figure 32. Data Encryption Summary Statistics

Encryption Summary Statistics Screen Terms

All statistics are computed since the last statistics reset or node boot. This table describes the summary statistics terms:

Term	*Indicates*
Channel ID	A number that uniquely identifies the encryption channel.
Channel State	Identifies the activity state of the channel for each direction. • Data: Indicates that normal data is passing through the channel. • No Data: Indicates that a channel is blocked for data traffic.
Source Channel	Identifies the access protocol’s identity string.
Destination Channel	Identifies the network protocol’s identity string.
Bad Frames	Number of packets that are dropped during the encryption process.
Authentication Failures	Number of key exchange failures.

Diagnostics

Introduction

This section describes the diagnostics that support the ECC DIMM and the Advanced Encryption Card. Power up diagnostics are available.

Start-up Diagnostics

The startup diagnostics screen for a Vanguard 340 Enhanced Series router is shown below with an ECC DIMM inserted in the node:

```
Executing V340 STARTUP Diagnostics (Rev. 4.0)...

DRAM Test (00200000--01000000): <<-PASSED->>
Flash Motherboard Test:      INTEL-MICRON Flash
Flash SIMM 1-0 Test:        Flash SIMM Not Installed
Ethernet Test (100 Mbps, Full_duplex, FPGA loopback): <<-PASSED->>
LAN2 Eth Test (100 Mbps, Full_duplex, PHY loopback): <<-PASSED->>
VRDC Port 01 (None): <<---NA--->>
VRDC Port 02 (None): <<---NA--->>
UART Port 01 (None): <<-PASSED->>
UART Port 02 (None): <<-PASSED->>
UART Port 03 (UDIM): <<-PASSED->>
HDLC Port 01 (None): <<-PASSED->>
HDLC Port 02 (None): <<-PASSED->>
HDLC Port 03 (UDIM): <<-PASSED->>
Clock Measurement:   <<-PASSED->>
Timers:              <<-PASSED->>
IDPROM Test:         <<-PASSED->>
DCC/DCE SIMM:        <<---NA--->>
ECC DIMM:            <<-PASSED->>
Exiting V340 STARTUP Diagnostics...
```

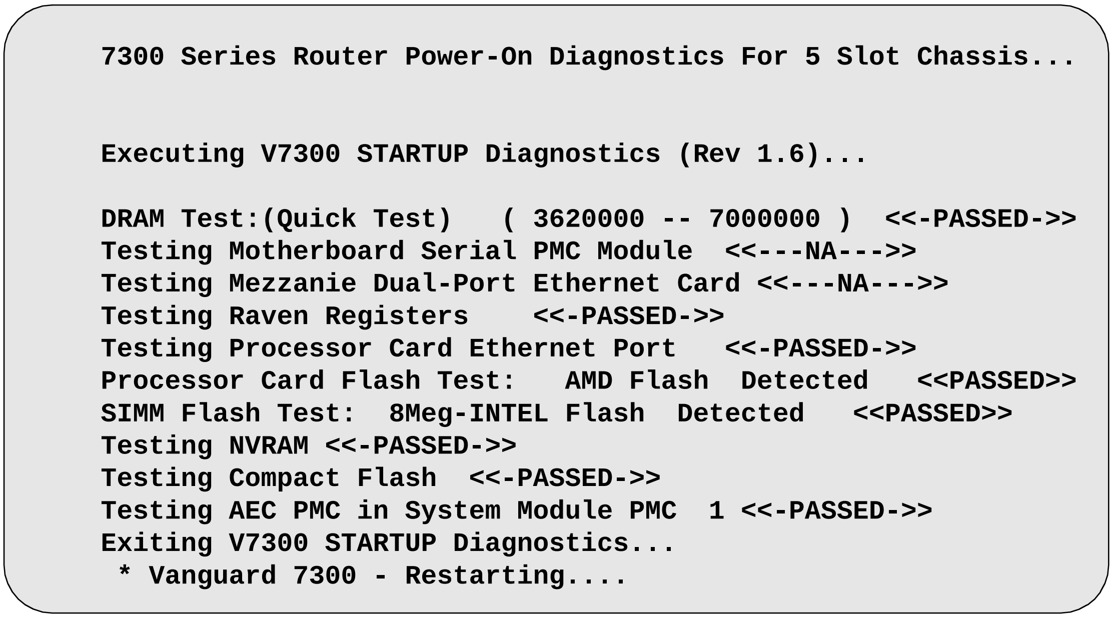
Figure 33. Vanguard 340 Enhanced Diagnostics Screen

■**Note**

A DCC/DCE SIMM and an ECC DIMM cannot be installed at the same time. If the ECC DIMM is not installed in the node, a result identical to the DCC/DCE SIMM of NA as shown in Figure 33 is displayed.

73xx Startup Diagnostics

The startup diagnostics for the Vanguard 73xx series routers is shown below with an Advanced Encryption Card (AEC) inserted in the node.



```
7300 Series Router Power-On Diagnostics For 5 Slot Chassis...


Executing V7300 STARTUP Diagnostics (Rev 1.6)...

DRAM Test:(Quick Test)   ( 3620000 -- 7000000 )  <<-PASSED->>
Testing Motherboard Serial PMC Module  <<---NA--->>
Testing Mezzanie Dual-Port Ethernet Card <<---NA--->>
Testing Raven Registers    <<-PASSED->>
Testing Processor Card Ethernet Port   <<-PASSED->>
Processor Card Flash Test:   AMD Flash  Detected   <<PASSED>>
SIMM Flash Test:  8Meg-INTEL Flash  Detected   <<PASSED>>
Testing NVRAM <<-PASSED->>
Testing Compact Flash  <<-PASSED->>
Testing AEC PMC in System Module PMC  1 <<-PASSED->>
Exiting V7300 STARTUP Diagnostics...
 * Vanguard 7300 - Restarting....
```

Figure 34. Vanguard 7300 Diagnostics Screen

Troubleshooting

Power Up and Recovery

A failure during power up diagnostics, or the absence of the data encryption hardware, is detected during the initialization of data encryption module. Should either of these events take place all data encryption services are disabled.

Software Configuration	***Hardware Status***		
	Missing	***Failed***	***OK***
Encryption Enabled	Disable / disconnect all the connections configured for encryption. Generate Report.	Disable / disconnect all the connections configured for encryption. Generate Report.	Normal operation
Encryption Disabled	No Action	Generate Report.	Generate Report.

Data Encryption Diagnostics

Data Encryption hardware performs all diagnostics during a power-up, a reset, and a cold boot.

Index