Vanguard Managed Solutions

Vanguard Applications Ware

Software Installation and Coldloading Manual

Notice

Restricted Rights Notification for U.S. Government Users

Proprietary Material

Information and software in this document are proprietary to Vanguard Managed Solutions (or its Suppliers) and without the express prior permission of an officer, may not be copied, reproduced, disclosed to others, published, or used, in whole or in part, for any purpose other than that for which it is being made available. Use of software described in this document is subject to the terms and conditions of the Software License Agreement.

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

Contents

Software Installation and Coldloading Manual

About This Manual

Special Notices and Translations

Customer Information

Customer Response Card

i

Overview

What is in This Document?

This document describes the methods of installing and crossloading software in Vanguard Products. This table lists and describes each chapter:

Chapter	Description
Chapter 1, Before You Begin	Describes Vanguard Product software images, how to find them, and how to load them.
Chapter 2, Downloading Software From a PC	Describes all procedures necessary to download software into Vanguard products from a PC, using data communication packages.
Chapter 3, Downloading From A LAN via TFTP	Describes how to TFTP download software to Vanguard Products.
Chapter 4, Crossloading Nodes FLASH-to-FLASH	Describes crossloading new software into Vanguard Products (except the 6500^{PLUS}) where FLASH memory has not been corrupted.
Chapter 5, Installing/Crossloading 6500PLUS Nodes	Describes the software installation process using NSO disks and the crossloading process using RAM-to-RAM transfer.
Chapter 6, Saving And Restoring Configurations	Describes the processes involved in saving a copy of your configurations and restoring the configurations using Kermit and TFTP.

About This Manual (continued)

Before You Operate Vanguard Products

Before you can operate any of the devices in a network, you must load operating software images into the node's FLASH-based memory.

■ Note

Download instructions in this notice supersede information described in the remainder of the Vanguard products documentation set.

Audience

This manual is intended for use by system administrators or anyone responsible for loading operating software into a network node containing Vanguard products.

Special Notices

The following notices emphasize certain information in this manual. Each serves a special purpose and is displayed in the format shown:

Related Documentation

Refer to these documents to obtain additional information on Vanguard products. On-line versions of these documents can also be accessed over the World Wide Web or on the Vanguide CD-ROM.

- *Vanguard Configuration Basics Manual* - This manual (Part Number T0113) provides details on how to configure and maintain Vanguard products.
- *Vanguard Applications Ware Software Release Notice* - This notice describes new features available with the software.
- Feature Protocols documentation - This series of binders contain manuals that describe features, options, and protocols designed for Vanguard products and found in various Vanguard Applications Ware.

iv

Special Notices

The following notices emphasize certain information in the guide. Each serves a special purpose and is displayed in the format shown:

■Note
Note is used to emphasize any significant information.

⚠ Caution

Caution provides you with information that, if not followed, can result in damage to software, hardware, or data.

✋ Warning

Warning is the most serious notice, indicating that you can be physically hurt.

Simplified Chinese

特别通告

以下通告强调指南中的某些信息。
每条信息均有一个特殊的目的并以如下格式显示：

■注解
注解用于强调任何重要的信息。

⚠ 切记

切记提供您这类信息，如果不遵照信息的要求，可能导致软件、硬件或数据的损坏。

✋ 警告

警告是最严重的通告，表明您的身体可能被伤害。

Danish

S¾rlige overskrifter

F¿lgende overskrifter fremh¾ver nogle af oplysningerne i vejledningen. De tjener hvert et specifikt formŒl og vises i f¿lgende format:

■Bem¾rk
Bem¾rk anvendes til at fremh¾ve vigtig information.

⚠ Forsigtig

Forsigtig understreger oplysninger, som, hvis de ikke bliver fulgt, kan f¿re til beskadigelse af software, hardware eller data.

✋ Advarsel

Advarsel er den mest alvorlige overskrift, og tilkendegiver mulig personskade.

Dutch

Bijzondere vermeldingen

De volgende vermeldingen besteden extra aandacht aan bepaalde informatie in de handleiding. Elke vermelding heeft een eigen nut en wordt in de volgende opmaak weergegeven:

■Opmerking
Een opmerking wordt gebruikt om belangrijke informatie te benadrukken.

⚠ Let op
Dit kopje geeft aan dat u de beschreven instructies moet volgen om schade aan de software, hardware of gegevens te vermijden.

🛑 Waarschuwing
Een waarschuwing is de belangrijkste vermelding. Indien u deze niet volgt, kan dit tot lichamelijke verwondingen leiden.

Finnish

Erityisilmoitukset

Seuraavat ilmoitukset korostavat tiettyjŠ oppaan tietoja. Kullakin on oma erikoistarkoituksensa ja ne esitetŠŠn seuraavassa muodossa:

■Huomaa
Huomautusta kŠytetŠŠn korostamaan tŠrkeŠtŠ tietoa.

⚠ Vaara
Vaarailmoitus antaa tietoa, jonka huomiotta jŠttŠminen voi johtaa ohjelmiston, laitteiston tai tietojen vahingoittumiseen.

🛑 Varoitus
Varoitus on kaikkein vakavin ilmoitus ja se kertoo mahdollisesta loukkaantumisriskistŠ.

French

Messages spŽciaux

Les messages suivants mettent en valeur certaines informations dans le guide. Chacun dÕeux remplit une fonction spŽciale et est affichŽ dans le format indiquŽ :

■Important
Important est utilisŽ pour souligner des informations critiques au sujet dÕune procŽdure.

⚠ Mise en Garde
Une mise en garde vous fournit des informations qui, si elles ne sont pas observŽes, peuvent se traduire par des dommages pour le logiciel, le matŽriel ou les donnŽes.

Avertissement

Un avertissement constitue le message le plus sŽrieux, indiquant que vous pouvez subir des blessures corporelles.

German

Besondere Hinweise

Durch die folgenden Hinweise werden bestimmte Informationen in diesem Handbuch hervorgehoben. Jeder Hinweis dient einem bestimmten Zweck und wird im dargestellten Format angezeigt:

■Wichtig

WICHTIG wird zur Betonung signifikanter Angaben zu Vorgehensweisen verwendet.

Vorsicht

Ein Vorsichtshinweis macht Sie darauf aufmerksam, da§ Nichtbefolgung zu Software-, Hardware- oder DatenschŠden fŸhren kann.

Warnung

Eine Warnung weist Sie darauf hin, da§ ernsthafte Kšrperverletzungsgefahr besteht.

Italian

Simboli speciali

I seguenti simboli, ciascuno con una speciale funzione, evidenziano determinate informazioni allÕinterno del manuale. Il formato   quello riportato qui di seguito.

■Nota

Questo tipo di avvertimento viene utilizzato per evidenziare tutte le informazioni significative relative ad una procedura.

Attenzione

Questo tipo di avvertimento fornisce informazioni che, se non vengono seguite, possono provocare danni al software, allÕhardware o ai dati.

Avvertenza

Questo tipo di avvertimento indica la presenza di condizioni di rischio che possono causare lesioni fisiche. Si tratta del simbolo pi   importante al quale prestare attenzione.

Japanese

特別表記　　　ガイド内では、以下の表記を使って特に注意する必要のある情報が提供されます。各表記にはそれぞれ目的があり、次の形式で表示されます。

■ 重要
重要な情報が記述されています。

⚠ 注意
記述されている内容に従わない場合、ソフトウェア、ハードウェア、またはデータが壊れる可能性があります。

警告
最も重要な情報が記述されています。身体的な障害を被る可能性があります。

Korean

일러두기　　　이 설명서에는 사용자에게 특정한 내용을 강조하기 위해서 다음 내용이 포함되어 있습니다.

■참고
중요한 정보를 강조하는데 사용합니다.

⚠ 주의
소프트웨어나 하드웨어, 또는 데이터를 손상시킬 수 있으므로 주의가 필요한 상황을 알립니다.

🛑 경고
사용자의 안전에 위험을 알리는 가장 심각한 수준의 경고입니다.

Norwegian

Spesielle merknader

Merknadstypene nedenfor representerer en bestemt type informasjon i hŒndboken. Hver merknadstype har en spesiell hensikt og vises pŒ f¿lgende format:

■**Merk**
Merk brukes for Œ fremheve viktig informasjon.

⚠ **Forsiktig**

Forsiktig gir deg informasjon om situasjoner som kan f¿re til skade pŒ programvare, datamaskin eller data dersom den blir fulgt.

🛑 **Advarsel**

Advarsel er den mest alvorlige merknaden og indikerer at du kan bli fysisk skadet.

**Portuguese/
Portugal**

Avisos Especiais

Os avisos que se seguem real am certas informa ›es neste guia. Cada um deles serve um objectivo especial e Ž visualizado no formato apresentado:

■**Nota**

    Nota Ž utilizado para real ar qualquer informa ‹o importante.

⚠ **Aten ‹o**

Aten ‹o faculta-lhe informa ›es que, se n‹o forem cumpridas, poder‹o provocar danos no software, hardware ou nos dados.

✋ **Cuidado**

Cuidado constitui o aviso mais grave, o qual indica que poder‡ ficar fisicamente ferido.

Spanish/Spain

**Notificaciones
especiales**

Las siguientes notificaciones ponen Žnfasis sobre determinada informaci—n de la gu'a. Todas tienen un prop—sito especial y se muestran con el formato siguiente:

■**Nota**

    Las notas se utilizan para destacar determinada informaci—n de importancia.

⚠ **Advertencia**

Las advertencias le proporcionan informaci—n que debe seguirse, si no desea que el software, el hardware o los datos puedan verse da–ados.

✋ **Aviso**

Los avisos son las notificaciones de car‡cter m‡s importante e indican la posibilidad de da–os f'sicos para el usuario.

Swedish

**Speciella
beteckningar**

Fšljande beteckningar betonar viss information i handboken. Var och en har ett speciellt syfte och visas i formatet nedan:

■**OBS!**

    OBS! anvŠnds fšr att betona viktig information.

⚠ **Viktigt**

Viktigt ger dig information som, om den inte fšljs, kan resultera i skada i programvara, maskinvara eller data.

Varning

Varning Šr den mest allvarliga beteckningen och den indikerar att du kan
skadas fysiskt.

Customer Information

Customer Questions	Customers who have questions about Vanguard Managed Solutions products or services should contact your Vanguard Managed Solutions representative or visit this website for product, sales, support, documentation, or training information: **http://www.vanguardms.com**
Comments About This Manual	To help us improve our product documentation, please complete the prepaid comment card included with this manual and return it by fax to (508) 339-9592. If you prefer, provide your name, company, and telephone number, and someone in the documentation group will contact you to discuss your comments.

Customer Response Card
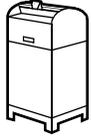
Vanguard Managed Solutions would like your help in improving its product documentation. Please complete and return this card by fax to (508) 339-6814; Attention: Product Documentaton, to provide your feedback.

To discuss comments with a member of our documentation group, provide telephone information at the bottom of this page. **Thank you** for your help.

Name _____

Company Name _____

Address _____

_____

_____

Document Title: Vanguard Applications Ware Software Installation and Coldloading Manual

Part Number: T0028, Rev M

Please rate this document for usability:

☐ Excellent ☐ Good ☐ Average ☐ Below Average ☐ Poor

What did you like about the document? _____

_____

_____

_____

_____

What information, if any, is missing from the document? _____

_____

_____

_____

_____

Please identify any sections/concepts that are unclear or explained inadequately.

_____

_____

_____

_____

Additional comments/suggestions. _____

_____

_____

_____

_____

Telephone _____ Ext. _____ Best time to call_____

Cut Here
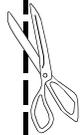
Overview

Introduction

This chapter describes operating software images options, how to find them, and how to load them.

Methods of Installing Software

There are three methods of installing software in nodes containing Vanguard Products. You can install software by:

- Using the Vanguard Software Loader.
- Downloading software from a PC.
- Using TFTP software from a LAN.

This manual does not cover software installation using the Vanguard Software Loader. For more information on this, please refer to the *Vanguard Software Loader Users Guide* (Part Number T0057).

■**Note**

When loading software into 6500^{PLUS} nodes, you can also use the NSO disk option. Refer to Chapter 5 for additional information.

After the software is installed in one device, you can crossload the software into other like nodes.

Vanguide Applications

For information on installing and configuring software in nodes with the Vanguide applications, please refer to these related documents.

Part Number	Documentation	Includes
T0056	Vanguide Application Set Installation Guide	Instruction on installing and removing the Vanguide Applications Ware software.
T0058	Vanguard Configuration Loader	Instruction on transferring Configuration Memory files between your PC and your Vanguard products.
T0057	Vanguard Software Loader	Instruction on transferring software image files between your PC and your Vanguard products.
T0030	Vanguard Software Builder	Instruction on creating custom software images for your Vanguard products.

Software Images

Introduction

This section describes:

- where to obtain operating software and coldloading software
- how to unlock the operating software images

Where To Obtain Operating Software Images

You can obtain operating software images for your Vanguard product from one of these sources:

- the Vanguide 6.4 and greater CD-ROM, using this path:

\Vanguard\Sfw_imgs\xxx

where xxx represents the directory corresponding to the various Vanguard devices.

- the World Wide Web (WWW), using this URL:

http://www.vanguardms.com

Unlocking Software Images

Each licensed Vanguard Applications Ware has a serial number that corresponds to your software release, product, and software license. The serial number unlocks only the software image matching the software release, product, and licensed Vanguard Applications Ware in use.

Depending on your license, the setup program launches the appropriate executable that installs the selected software image.

Please refer to the *Vanguide Application Set Installation Manual* (Part Number T0056) for more information on unlocking software images. Also, please refer to the appropriate software release documentation to see which software image and licensed Vanguard Applications Ware is supported by a specific Vanguard product.

Coldloading

Introduction   Coldloading is the process of transferring software images (.xrc files) from a PC to your Vanguard product. To operate a Vanguard product, you must load software images into the products FLASH memory.

ColdLoad Files   There are a number of coldload files available for each Vanguard product. If you are coldloading, you must use these files.

Product	*Coldload Files*	
Vanguard 100	cl00v115.xrc cl00v192.xrc cl00v576.xrc	cl00v96.xrc v100load.xrc
Vanguard 305	cl01v115.xrc cl01v192.xrc cl01v576.xrc	cl01v96.xrc v300load.xrc
Vanguard 310 series	v310load.xrc	v312load.xrc
Vanguard 320	c320v115.xrc c320v384.xrc c320v576.xrc	c320v96.xrc v320load.xrc
Vanguard 340, 340 Enhanced and 342	c34v115.xrc c34v192.xrc c34v288.xrc	c34v384.xrc c34v576.xrc c34v96.xrc
Vanguard 6400	C64V115.xrc C64V192.xrc C64V288.xrc	C64V384.xrc C64V576.xrc C64V96.xrc
Vanguard 6520	6520load.xrc cl00b115.xrc cl00b19.xrc	cl00b56.xrc cl00b96.xrc
Vanguard 6560	6560load.xrc cl00r115.xrc cl00r19.xrc	cl00r384.xrc cl00r56.xrc cl00r96.xrc
Vanguard 650D	c650i115.xrc c650i192.xrc	c650i576.xrc c650i96.xrc
Vanguard 6435	C64V115.xrc C64V192.xrc C64V288.xrc	C64V384.xrc C64V576.xrc C64V96.xrc
Vanguard 6455	C64V115.xrc C64V192.xrc C64V288.xrc	C64V384.xrc C64V576.xrc C64V96.xrc
Vanguard 7300 Series	**Current Bank**	**Alternate Bank**
■**Note** Please refer to the current 7300 Series Software Release Notice for detailed information.	c73cv115.xrc c73cv192.xrc c73cv288.xrc c73cv384.xrc c73cv576.xrc c73cv96.xrc	c73av115.xrc c73av192.xrc c73av288.xrc c73av384.xrc c73av576.xrc c73av96.xrc

Operating Software Characteristics

Introduction

Before you can operate a Vanguard product in a network, you must load operating software images into the node's FLASH-based memory.

Operating software images have these characteristics:

- They are stored in either 1 or 2 MB (3 or 4 MB in 6500^{PLUS} models) of FLASH memory in a compressed format.
- They are decompressed into RAM and executed out of RAM upon node powerup or cold reboot.

■**Note**

Only the Vanguard 6500^{PLUS} supports the loading of software from NSO disks.

■**Note**

You can only perform software downloading from like nodes only. For example, a Vanguard 100 can transfer operating software to other Vanguard 100s but cannot transfer software to Vanguard 320 nodes.

Vanguard 310 Series

The Vanguard 310 Series consists of two different models; Vanguard 311^{PLUS} and Vanguard 312^{PLUS}. They are similar except that the Vanguard 312^{PLUS} offers POTS support.

Identifying Your Board

Different boards use different coldloaders. There are two ways to identify which board you are running.

- If the node is operational, the board assembly information can be retrieved from page four of the Node stats, as shown in Figure 1-1.

- If the node is not operational and is waiting for a coldload, remove the cover from the unit. The assembly numbers are marked on the board on a barcode label. See "Vanguard 310 Series Circuit Board Identification" section on page 1-5 to help you identify your board.

```
Node:              Address:        Date:         Time:
 Detailed Node Statistics                         Page:   4 of  4

Board Type:   Number of ports: 5  Status: Running

Assembly: 72442G12  Version:  A  Serial Number: 006831538

Memory Configuration:
    EPROM: 4 KBytes     DRAM: 4      bytes    FLASH: 65535   bytes
    Software: V4.97p00_Omaha_311+   FLASH Used: 1304492 bytes

Port Configuration:
    Port 1 Interface Type:   ISDN          U
    Port 2 Interface Type:   ISDN          U
    Port 3 Interface Type:   ISDN          U
    Port 4 Interface Type:   EIA-232-D    DCE
    Port 5 Interface Type:   ETHERNET      10BASE-2

CPU utilization: 19%
```

Figure 1-1. Example Node Statistics Screen

Vanguard 310 Series Circuit Board Identification

This table identifies which coldloader file works with which hardware. Coldloader files marked with a check mark (√) work with the corresponding hardware revision.

Product:	Model:	Board Rev:	Prom ID:	Cloader C310VXXX.xrc	Cloader C312VXXX.xrc
VG312	U+ 2 Pots	72791G12	0.4		√
	ST+2Pots	72810G02	0.4		√

■**Note**

Devices containing Board Revs 72791G52 or 72810G51 cannot load Software Release 4.91 or older. The coldload file supplied with Release 4.97, loads all of the VG31X products. Use this coldloader whenever you are upgrading a Vanguard 310 with new Applications Ware software.

Coldloading The Vanguard 320

Commencing with Applications Ware Release 5.2, a Vanguard 320 with boot PROM of version 3.0 or higher requires coldloads and software images of Release 5.2 or higher.

Determining the Bootprom Revision

With these changes, you must determine what version of boot PROM has been installed in your Vanguard 320. The version of boot PROM determines which coldloader must be used to load software into the Vanguard 320. Follow these steps to check the boot PROM version of your Vanguard 320:

Step	Action
1	Access the CTP.
2	Select **Detailed Node Statistics** from the Status/Statistics menu.
3	Note the PROM revision. Refer to Figure 1-2.

```
Node:              Address:              Date:              Time:
Detailed Node Statistics                                   Page 1 of 4


Node number: 0
Product Type: VANGUARD 320
Node Serial #: 16160574
Prom revision: 3.0
```
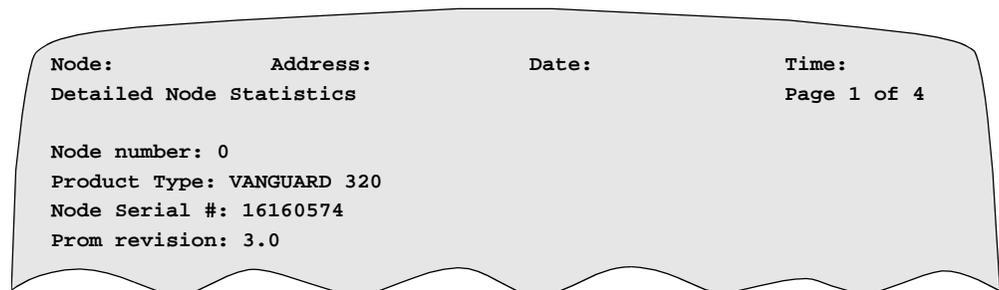
Figure 1-2. Locating the PROM Revision in Detailed Node Statistics

Using the Correct Coldloader

Ensure that you use the correct coldloader to coldload images into your Vanguard 320. Consult this table to determine which coldloader to use.

If the Boot PROM is...	...and you want to load a Software Image of...	you can use Coldloader...
Rev 2.0 and lower	Any revision	Any version of the coldloader
Rev 3.0 and higher	5.2 and higher	5.2 and higher

Troubleshooting Error messages appear on your terminal emulator if you use incompatible bootprom and coldloaders. Refer to this table for troubleshooting tips when you encounter an error.

Error Message	Description	Action
After loading, the node displays the message **V320 - wrong cloader was loaded**.	Your coldloader is not compatible with the Boot PROM installed in the Vanguard 320. This error message appears if you attempt to use a 5.1M or lower coldloader for Boot PROM Rev. 3.0 or higher.	Download the latest coldloader software. The latest coldload software can be found on the CD ROM.
After loading, the node displays the message **V320 - incompatible image was loaded**.	You attempted to load a software image that is not compatible with the Boot PROM installed in the Vanguard 320. This error appears if you attempt to load a 5.1M or lower software image onto a Vanguard 320 that is installed with Boot PROM Rev. 3.0 or higher.	Download the latest software image.
A **V320 - failed erase and/ or programming procedure** error message appears.	This is caused by an error in FLASH programming.	Reset the node using the reset switch located on the front panel, or power cycle the node.
After loading, the node displays **VG320 - awaiting coldload**.	A wrong or corrupted image has been loaded into the node and is being ignored by the Vanguard 320.	Ensure that the image you are downloading is intended for the platform.

Chapter 2
Downloading Software From a PC

Overview

Introduction

This chapter describes all procedures necessary to download software into Vanguard products from a PC computer.

Coldloading is, normally, a service procedure used to download a software image to a node with corrupted FLASH memory. However, you can also use this procedure to seed nodes containing Vanguard products with software upgrades.

Before You Begin

Make sure you perform these tasks before you coldload your Vanguard product:

- Use a program that allows terminal emulation.
- Corrupt the FLASH image on the Vanguard product. To initiate the coldload process, a corrupted image must be recognized in FLASH. Refer to the appropriate section for corrupting FLASH Images for details.
- Make sure you have a straight through cable (hardware handshaking).

Connecting your Vanguard to a PC

Connecting to a PC Vanguard products can be coldloaded with operating software using any communication package that can do raw binary transfers. This example shows how to connect your Vanguard product or 650D to a PC and how to modify and save ASCII protocol options.

Step	*Action*
1	Connect the modem serial port on your PC to one of these ports: • Vanguard 100 - use Port 3 • Vanguard 200 - use Port 6 • Vanguard 305 - use Port 4 • Vanguard 310 Series - use Port 4 • Vanguard 320 - use Port 4 • Vanguard 340, 340 Enhanced - use Port 4 • Vanguard 342 - use Port 4 • Vanguard 6400 - use Port 4 • Vanguard 6520/6560 - use Port 6 • 650D - use Port 3 • Vanguard 7300 Series - use DB9 Port on CPU card
2	Launch your data communications application.
3	Set these ASCII protocol options and then save the configuration: • Echo locally = no • Expand Blank Lines = no • Expand Tabs = no • Character Pacing (msecs) = 0 • Line pacing (1/10 sec) = 0 • Pace character = 0 • Strip 8th bit = no • ASCII download timeout (Seconds) = none • CR translation (upload) = none • LF translation (upload) = none • CR translation (dnload) = none • LF translation (dnload) = none
4	Set up the terminal for a data speed of 9600. **■Note** Some communications applications may require that you select **Raw ASCII** as the upload protocol.
5	Press **Return** a few times, if necessary, for the prompt to appear.
6	If an asterisk appears, type **ctp**. If the OK prompt appears, type **atds0**. Press **Return**.
7	Press **Return** for password.

Downloading Software From a PC

Corrupting FLASH Memory

Introduction   You must corrupt the FLASH memory before you begin the coldload procedure.

⚠ Caution

Corrupting FLASH will corrupt both Primary and Alternate (purchased as an added option) FLASH devices. The only way to avoid corrupting the Alternate FLASH is to carefully remove it from the device prior to initiating the corruption procedure.

Prior to removing Alternate FLASH memory devices, you must power down the device and use appropriate Electro-Static Discharge (ESD) procedures

⚠ Mise en Garde

La corruption des FLASH endommagera les dispositifs FLASH primaire et secondaire (achetés en option). Pour ne pas endommager le FLASH secondaire, dégagez-le avec précaution de son dispositif avant de lancer la procédure de corruption.

Avant d'enlever les dispositifs de mémoire FLASH secondaires, éteignez l'appareil et suivez les procédures de décharge électrostatique appropriées.

⚠ Vorsicht

Durch Modifizierung des FLASH-Speichers werden sowohl die primären als auch die alternativen (als Add-On-Option erhältlichen) FLASH-Geräte modifiziert (verfälscht). Eine Verfälschung des alternativen FLASH-Speichers kann nur vermieden werden, indem Sie ihn vorsichtig aus dem Gerät entfernen, bevor Sie den Modifikationsvorgang starten.

Vor dem Entfernen der alternativen FLASH-Speichergeräte müssen Sie das Gerät abschalten und die entsprechenden Maßnahmen zur elektrostatischen Entladung (ESD) ausführen.

Corrupting Procedure

Follow these steps to corrupt the FLASH memory.

Step	*Action*	*Result*
1	Select **FLASH Memory** from the CTP Main menu.	The FLASH Memory menu appears.
2	Select **Force Cold Load** from the FLASH Memory menu.	This prompt appears: **Flash memory contains all of the operating software. If this step is taken, the contents of the installed Flash memory will be erased and can not be recovered.** **Proceed? (Y/N): Y**
3	Press **Y** and **Return**.	
4	Select **Boot** from the CTP Main menu.	The Boot Menu appears.
5	Select **Node (Cold)**.	A prompt appears, asking you if you want to proceed.
6	Press **Y** to commence cold booting the device.	• On the Vanguard 6400 series, the LCD message should say "ERR: Bad FLASH." • On Vanguard 6520/6560 models, the status indicator should display **40**, or **41** for the alternate bank. • On all other Vanguard products, a green STATUS LED should be flashing rapidly. ■**Note** These displays indicate that FLASH memory is corrupt and that the node is ready to be cold loaded. If FLASH has not been corrupted, refer to the previous sections on Corrupting FLASH Memory.
7	Quit from your terminal emulation program, and proceed to "Coldloading Vanguard Products" on page 2-5.	

Coldloading Vanguard Products

Introduction   The process of coldloading involves two major tasks:

Task	*Action*	*Description*
1	Load a coldloader file.	A coldloader file (XRC file) configures your device to receive the software image at a certain data speed (in this case, 9600 bps). These files have this format: **CNNNVSSS.XRC** where: • **NNN** = the node/model #, such as 100/200 • **SSS** = Download Speed Required
2	Load a software image.	Operating software images contain the application requirements for your Vanguard product or 650D. These XRC files have this format: **###dYY.XRC** where: • **###** = identifies the software release number, • **d** = identifies the model type, and • **YY** = identifies the option number.

How to Coldload a Vanguard Product

Follow these steps to coldload an operating software image into a Vanguard product.

Step	Action	Result
1	Set up the terminal for a data speed of 9600 and (if necessary) select **Raw ASCII** as the upload protocol.	Your modem port is configured for binary file transfer at 9600 bps 8n1. An open file menu should appear.
2	Enter the full pathname of the appropriate cold loader 'XRC' file (first unzip this file).	The boot file is loaded onto the Vanguard node. During the transfer (about 10 seconds), the yellow receive data LED (Port 3 on Vanguard 100s and Port 6 on Vanguard 200s) flickers and the green status LED is on solid. On the Vanguard 6400 products, the LCD displays "BootPROM Vnn." When the transfer is done, the green status LED flashes. On the Vanguard 6400, the LCD displays "Need Coldload." If the red test LED comes on (indicating an error), or the LCD on the Vanguard 6400 displays "ERR: Bad FLASH", power-cycle the node, and go to Step 1. This also sets up the ports listed above to accept the next file (the operating software) at 57600 bps.
3	Set up the terminal for a data speed of 57600 and (if necessary) select **Raw ASCII** as the upload protocol.	Your modem port is configured for binary file transfer at 57600 bps 8n1. An open file menu should appear.

Step	*Action*	*Result* (continued)

4	Unzip the desired XRC file and then enter the full pathname of that software image file.	While this transfer is taking place, the yellow receive data LED (Port 3) flickers. This transfer takes a few minutes to complete. If the red test LED comes on, an error has occurred. Should this happen, power cycle the node, and return to Step 1.
		
		Vanguard 6400 - The front panel LCD cycles through these messages, in this order (these messages correspond to the different points throughout the data transfer):
		
		  • Erasing FLASH
		  • Send FLASH Image
		  • Writing to FLASH
		  • Coldload Done
		
		If the LCD displays "ERR: Bad FLASH" (indicating an error), power-cycle the node and go to Step 1.
		
		Vanguard 200/305/310/320/34x - There are two parts to the down-load process:
		
		  • During the first part (about 2 min. elapsed time), the yellow Receive Data LED, and the green STATUS LED, will flicker. (If there is a power interruption, the original FLASH image remains.)
		  • During the second part (which takes about eight minutes), the green STATUS LED flickers.

Downloading Software From a PC

Step	*Action*	*Result* (continued)
4 **(Cont.)**		When downloading is complete, the node resets itself: • The TEST LED blinks for a few seconds (indicating diagnostics tests). • The STATUS, TEST, and Watchdog LEDS come on for two seconds. • The STATUS LED blinks at a steady rate (indicating decompression of the operating software code). ■**Note** If the red TEST LED stays on (indicating an error), power-cycle the node and go to Step 1. ■**Note** If the STATUS LED blinks rapidly (indicating power loss during transfer or failure of FLASH programming), press the Reset switch and go to Step 1. *Vanguard 6400* - The front panel LCD cycles through these messages, in this order (these messages correspond to the different points throughout the node reset): • BootPROM Vnn • Loading FIPL • Loading FBIST • Testing Node • BootPROM Vnn • Loading FIPL • Loading • Booting • BootPROM Vnn • ---Node UP--- ■**Note** If the LCD displays "ERR: Bad FLASH" (indicating an error), power-cycle the node and go to Step 1.

Coldloading Vanguard 6520/6560 Products

How To Coldload the Vanguard 6520/6560

Follow these steps to coldload an operating software image into a Vanguard 6520/6560.

Step	Action	Result
1	Set up the terminal for a data speed of 9600 and (if necessary) select **Raw ASCII** as the upload protocol.	This loads the boot file to the 6520/6560 and sets up port 6 to accept the next file at 57600 bps. Your modem port is configured for binary file transfer at 9600 bps 8n1. The 6520/6560 front panel blinks as copy proceeds. It first displays **44**, then **45**. This means that the FLASH is erased.
2	Unzip the desired XRC file and then enter the full pathname of that software image file.	Your modem port is configured for binary file transfer at 57600 bps 8n1 and the file transfer begins. If the Vanguard 6520/6560 has two FLASH modules, you see codes **46** and **47**. This transfer takes a few minutes to complete.
3	Upon successful completion of the load, the node reboots.	Normally, the front panel displays any code other than twin dashes (- -). Refer to the *Vanguard 6520/6560 Installation Manual* (T0126) for additional code information.

Using the ZAP Utility

What Is It?

If you type **ZAP** while the startup diagnostics are running the DRAM tests, you will interrupt the normal startup flow and get into the ZAP mode. This invokes a special utility to either erase the software image or the CMEM image in the node. This also lets you reload a new software image or start from blank CMEM to isolate the cause of the problem.

```
Executing Vanguard Startup Diagnostics (Rev: 1.04)...
Testing DRAM...
   $00030000-$003FFFFF
Startup Diagnostics Interrupted !

Vanguard 320 Diagnostics ZAP Mode Menu (Rev: 1.04)
==================================================
Enter: <ESC> Exit
         1 - Force ColdLoad            2 - Clear CMEM
```

If you select Clear CMEM, the CMEM are cleared:

```
Enter Selection: 2
Erasing Configuration Memory...
Exiting ZAP/INTERRUPT Mode. Please Wait...


Executing Vanguard Startup Diagnostics (Rev: 1.04)...
Testing DRAM...
   $00030000-$003FFFFF
```

If you select Force Coldload, the **"awaiting coldload"** message will be displayed. However, the actual software in the flash is not erased until valid coldloader software is successfully loaded.

7300 Series Version 1 and Version 2 Zap Menus

Vanguard 7300 Series Version 1 and Version 2 Zap instructions can be found on the Release 6.1 Software Release Notice. For more information, refer to (Part Number T0001-42).

Chapter 3
Downloading From a LAN via TFTP

Overview

Introduction   This chapter describes how to TFTP download software images to Vanguard products.

Downloading   Downloading images can be accomplished using any communication protocol supported by a Vanguard product, provided that IP connectivity exists between devices.

Downloading Software Images By TFTP

Introduction

You can use TFTP (Trivial File Transfer Protocol) to download software images from a TFTP remote server to nodes containing Vanguard Products. You can also use TFTP to upload and download CMEM configuration files.

What Is TFTP?

TFTP is the TCP/IP standard protocol for file transfer. It has minimal capability and overhead. Any LAN-connected workstation with IP connectivity to a Network Access Product that supports the TFTP protocol can act as a load server.

TFTP transfers configuration data and software image files without regard to content. It also provides packet sequencing to ensure proper delivery order, and checksumming to ensure data integrity. Only one configuration transfer can occur at any one time.

Accessing TFTP Features

You can access TFTP via these methods:

- Using SNMP (IP connectivity between the destination node and the TFTP server is required)
- Using FLASH Memory menu options

TFTP file transfers can use the IP connectivity configured for the SNMP manager/agent traffic. Configuration and software transfers follow the same IP routing paths as SNMP management data.

Before You Begin

Before you begin the TFTP software download procedure:

- Ensure that the operational software you want to download to the node resides on the TFTP server.
- Obtain the file name and Operation Type objects since TFTP prompts you for the server's file name during the download procedure.
- Obtain the IP Address of the server since TFTP prompts you for the server's IP address during the download procedure.

Downloading Software Image Files

This table identifies the downloading procedure.

Step	Action	Result
1	Configure IP connectivity between Vanguard Products and the TFTP Server.	The TFTP Server becomes reachable from the node containing the Vanguard Product.
2	PING the TFTP server.	This ensures you have enabled IP connectivity between the remote server and the node.
3	Select **FLASH Memory** from the CTP Main menu.	The FLASH Memory menu appears.
4	Select **Current** from the TFTP SW Download menu.	The **File Name:** prompt appears.

Step	*Action*	*Result* (continued)
5	Enter the filename, for example, **c320v115.xrc.**	The **IP address:** prompt appears.
6	Enter IP address of the TFTP server, for example, **134.33.131.2.**	The **Ready to initiate TFTP transfer (y/n):** prompt appears.
7	Enter **Y** to initiate the transfer.	This message appears: **TFTP transfer has been initiated:** ■**Note** While the TFTP transfer is occurring, do not power cycle your Vanguard product!

	If...	*Then...*
	This message appears: **TFTP Operation successful**	The software image file has downloaded. It is now safe to power cycle your Vanguard product.
	This message appears: **TFTP: Local transfer failure**	Your TFTP transfer did not work properly because: • the IP address or file name was incorrect, or • your server is improperly configured to allow for the TFTP file transfers

Step	*Action*	*Result* (continued)
8	After the message **TFTP: Local transfer failure** appears, this report is displayed: **FLASH CHECKSUM ERROR, CURRENT BANK**	The background checksum routine detected a corrupt flash image, which occurred when you tried to use TFTP to load the Vanguard product. ■**Note** Do not cold boot or power cycle your device because the FLASH image is now corrupted and must be overwritten by an uncorrupted flash image. The Vanguard product is still running its software from DRAM.
9	Change any configurable parameters on the Vanguard product.	It is safe to boot the Vanguard product if necessary after changing certain parameters to make them active. The operating software will not change and you can then attempt another TFTP transfer.

TFTP Status and Statistics

Introduction

The remote TFTP server indicates the success or failure of any file transfer operation once processing is complete.

In a Vanguard product, TFTP also stores status information for the most recent or in-progress operations for access by the SNMP Manager. No configuration record is kept for TFTP parameters.

How to Display Statistics

This table describes how to display the TFTP Status and Statistics screen.

Step	*Action*	*Result*
1	Select **Status/Statistics** from the CTP Main menu.	The Status/Statistics menu appears.
2	Select **TFTP Stats** from the Status/Statistics menu.	The TFTP Status and Statistics screen appears, as shown in Figure 3-1.
3	Press **CTRL-R** or **CTRL-T**.	**CTRL-R** prints the statistics. **CTRL-T** returns you to the top menu. Any other response returns to the Status/Statistics menu.

TFTP Status and Statistics Screen

Figure 3-1 shows the TFTP Status and Statistics screen, which displays information related to the most recent or in-progress file transfer operation, such as the transfer of software images or configurations.

```
Node:             Address:              Date:                 Time:
TFTP Status and Statistics                                    Page: 1 of 1


Status:    TFTP transfer in progress
Operation: Configuration upload from current bank of CMEM
IP Address:192.0.0.0
File Name:
Time Stamp:
Byte Count:300



 Press any key to continue (ESC. to exit)...
```

Figure 3-1. TFTP Stats Screen

TFTP Status and Statistics Screen Attributes

This table describes the screen attributes for the TFTP Status and Statistics screen shown in Figure 3-1.

Term	*Tells you...*
Status	Displays the status of the operation. One of these text strings is possible: • No transfers since node last booted • Transfer in progress • Operation successful • CMEM access failure • Local transfer failure (the error code and error message from the last TFTP error packet are included) • Remote transfer failure (the error code and error message from the last TFTP error packet are included) • System failure • UDP registration failure • FLASH erasure in progress • FLASH erasure failure • FLASH write failure • Error in software image file
Operation	Identifies the most recent or in-progress file transfer operation. One of these text strings is possible: • TFTP Save Configuration • TFTP Restore Configuration • Current, from the TFTP sw download menu (if a Vanguard 6520/6560 is involved, the text string may read **TFTP sw download -> Alternate**, since these two devices are equipped with dual FLASH)
IP address	Identifies the IP address of the remote TFTP server; X.X.X.X where X is less than 256.
File Name	Names the file being transferred in a text string of no more than 80 characters.
Time Stamp	Displays the time of the file transfer, such as **dd-mmm-yyyy hh-mm-ss** (all values are numbers, except for mmm, which are the first 3 characters of the name of the month).
Byte Count	Indicates the running total of the number of bytes transferred.

Chapter 4
Crossloading Nodes FLASH-to-FLASH

Overview

Introduction

This section describes crossloading new software to nodes where FLASH memory has not been corrupted.

Some Basics on Crossloading

In order to be crossloaded, one node (a Server Node) must already have software installed. You can only crossload the same product type (for example, you can crossload a Vanguard 320 to other Vanguard 320s).

■**Note**

Unless otherwise indicated, these instructions apply equally to crossloading software into all Vanguard products. Crossloading nodes can be done using any X.25 like protocol. Consequently, the descriptions that follow do not detail any one specific communications protocol.

You can crossload software images simultaneously from one product to as many as five other similar products in your network. This concept is illustrated in Figure 4-1.

⚠ **Caution**

Back up the contents of your Configuration Memory (CMEM) prior to downloading any software image. If you do not back up the contents of CMEM, you risk losing it if the FLASH transfer fails.

⚠ **Mise en Garde**

Faites une copie du contenu de votre mémoire de configuration (CMEM) avant de télécharger une image logicielle. Si vous n'effectuez pas cette copie, vous risquez de perdre le contenu de la mémoire de configuration si le transfert FLASH échoue.

⚠ **Vorsicht**

Erstellen Sie eine Sicherungskopie des Konfigurationsspeichers (CMEM), bevor Sie Softwarekonfigurationen herunterladen. Andernfalls riskieren Sie den Verlust des CMEM, sollte die FLASH-Speicherübertragung fehlschlagen.

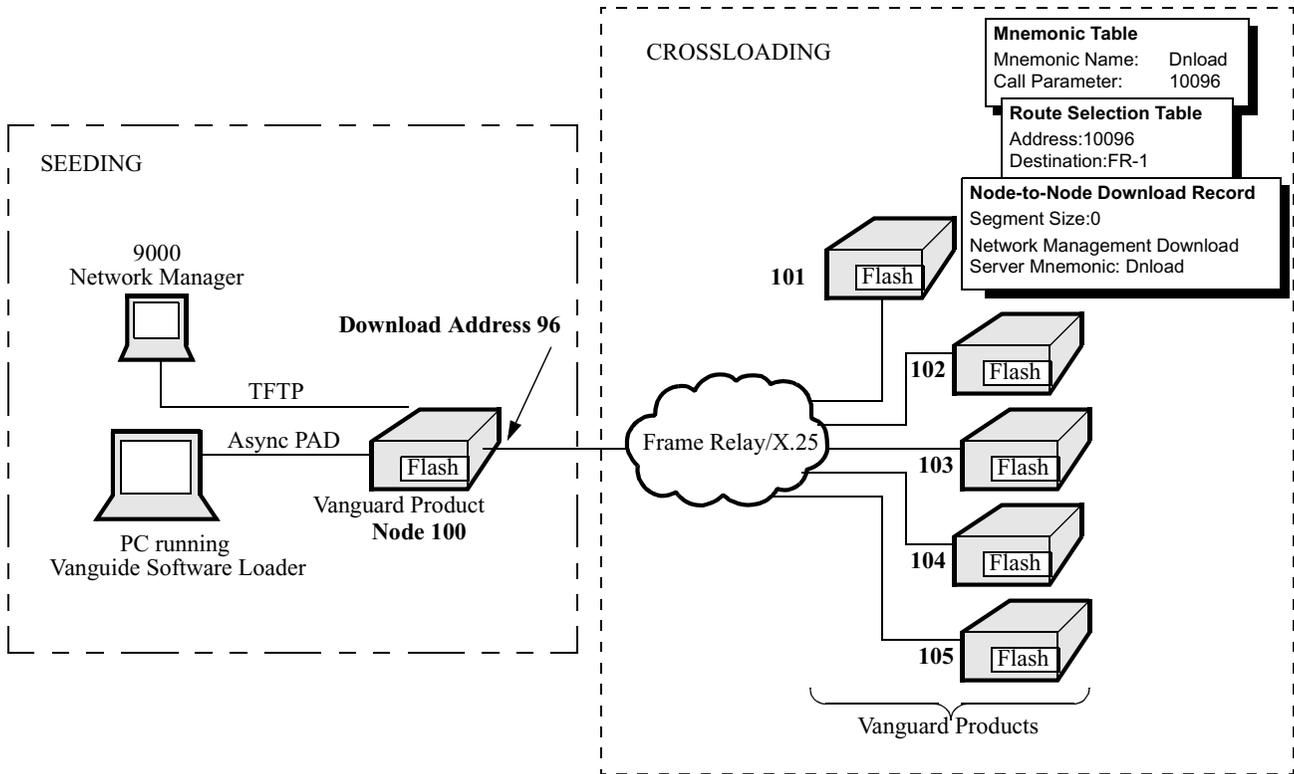For more information on backing up CMEMs, please refer to Chapter 6, Saving And Restoring Configurations".

Figure 4-1. Crossloading Software to Similar Devices

FLASH Banks and FLASH-to-FLASH Transfer

About FLASH Banks

FLASH memory consists of either one or two FLASH banks on each node that stores copies of the operating software. The Current bank is the bank from which the node was last loaded. The Alternate bank is always the other bank. When the node is booted from the Alternate bank, the Alternate bank becomes the Current bank. For example, Figure 4-2 shows the FLASH banks on a Vanguard 6520.

You can transfer software from the Current bank of the local node to the Alternate banks of remote nodes or vice versa.
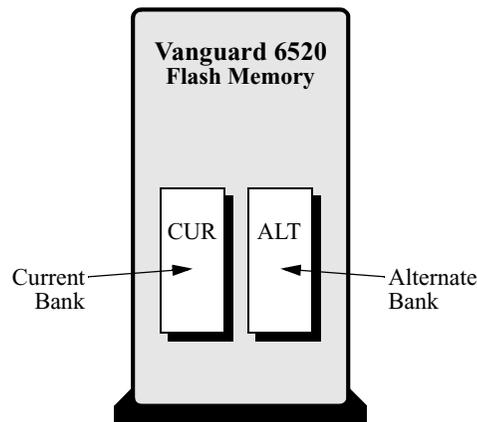
Figure 4-2. Vanguard 6520 FLASH Banks

Crossloading Remote Non-6500 Nodes

Introduction   Once a Vanguard product is seeded with operating software, it can simultaneously crossload operating software to as many as five similar nodes across X.25-like links.

The crossloading occurs in the background using existing internodal links and has minimal affect on data passing through the node.

■**Note**

On some devices, crossloading is limited to 2 MB.

Figure 4-3 shows critical parameters that you must configure to crossload software if both the remote node receiving the software, and the server node, are running Release 4.23 or greater.
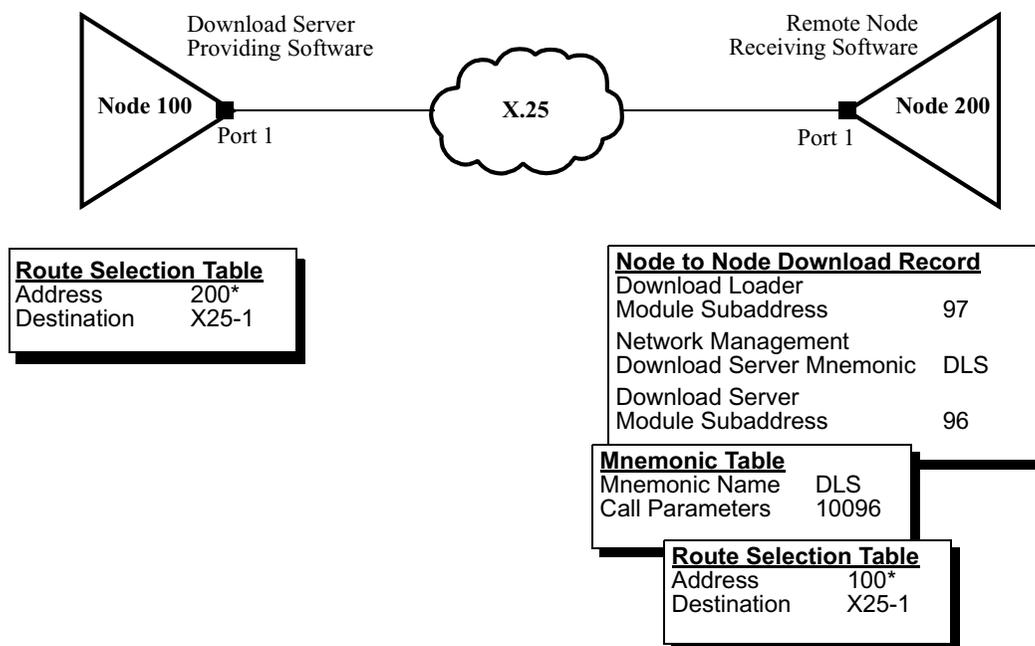

Figure 4-3. Critical Crossloading Parameters

Use these procedures to crossload software options if both the remote node receiving the software and the server node are running Release 4.23 or greater.

On the server node, use 96 as the sub-address to call to download the server module.

Crossloading Remote Nodes	Complete these tasks to crossload remote nodes containing Vanguard Products.

Task	*Procedure*
1	Configure the Route Selection Table for the server node running the desired software option.
2	Configure the Mnemonic Table for the remote node receiving the software.
3	Configure the Route Selection Table for the remote node receiving the software.
4	Configure the Node to Node Download Record for the remote node receiving the software.
5	Boot all Tables and Records.
6	Copy the software from the server node directly to the FLASH.
7	Check the statistics in the remote node. ■**Note** Use FLASH-to-FLASH Stats from the Statistics menu to check on the progress of the operation. Refer to the *Vanguard Configuration Basics Manual* (Part Number T0113) for a description of FLASH statistics.
8	Cold boot the remote node.

Configuring the Server Node Route Selection Table

Configuration   Follow these steps to configure critical parameters in the Route Selection Table for the server node.

Step	*Action*	*Result/Description*
1	Select **Configure Network Services** from the Configure menu.	The Configure Network Services menu appears.
2	Select **Route Selection Table** from the Configure Network Services menu.	The Route Selection Table prompts appear.
3	Configure these parameters from the Route Selection Table: **Address:** **#1 Destination:** **#1 Priority:**	 Specifies the Network Address for calls routed beyond this node. Specifies the network address to which calls are routed. Specifies the priority for call forwarding to ports within this Route Selection Table. Specifying High priority means no delays.

Configure the Mnemonic Table for the Remote Node

Configuration Follow these steps to configure critical parameters in the Mnemonic Table for the remote node.

Step	Action	Result/Description
1	Select **Configure Network Services** from the Configure menu.	The Configure Network Services menu appears.
2	Select **Mnemonic Table** from the Configure Network Services menu.	The Mnemonic Table prompts appear.
3	Configure these parameters from the Mnemonic Table: **Mnemonic Name:** **Call Parameter:**	 The mnemonic name must match the mnemonic name specified in the Node-to-Node Download record for the remote node. The call parameter must match the node number and Download Address of the server node.

Configure the Route Selection Table for the Remote Node

Configuration   Follow these steps to configure critical parameters in the Route Selection Table for the remote node.

Step	*Action*	*Result/Description*
1	Select **Route Selection Table** from the **Configure Network Services** menu.	The Route Selection prompts appear.
2	Configure these parameters from the Route Selection Table:	
	Address:	Specifies server node and subaddress.
	#1 Destination:	Specifies the port or station used to connect with the server node.
	#1 Priority:	Specifies the priority for call forwarding to ports within this Route Selection Table. (Highest = 1; Lowest = 15)

Configure the Node-to-Node Download Record for Remote Nodes

Configuration

Follow these steps to configure the Node-to-Node Download record parameters in the remote node that will receive the software.

Step	Action	Result/Description
1	Select **Node-to-Node Download** from the Configure menu.	The Node-to-Node record prompts appear.
2	Configure these parameters from the Node-to-Node Download record:	
	Segment Size: 0	Indicates the size of the data packet. Normally, you can use the default setting.
	Network Management Download Server Mnemonic:	This is the mnemonic name entered in Step 3 of the "Configuring the Server Node Route Selection Table" section.

Boot All Tables and Records

Introduction   Follow these steps to boot all tables and records in the remote node that will receive the software.

Step	Action	Result/Description
1	Select **Boot** from the Main menu.	The Boot Menu appears.
2	Select **Table and Node Record** From the Boot Menu**.**	This prompt appears: **Boot Configuration Table and Node Record [y/n]**
3	Press the **y**, **Return**, and **Esc** keys.	This sequence returns you to the Main Menu. This can also be accomplished by pressing **Ctrl T.**

Copy Software from Server to FLASH

Copying Software   Follow these steps to perform FLASH-to-FLASH transfer of software.

Step	Action	Result/Description
1	Select **FLASH Memory** from the CTP Main menu.	The FLASH Memory record appears.
2	Select the **Remote Copy** operation. ■ **Note** If you are crossloading a Vanguard 6520/6560, select the operation appropriate to the FLASH bank you want to load, for example, Remote copy SW Current from the Current menu.	The Remote Copy menu, which lists the throughput options, appears.
3	Select **High** from the Remote Copy menu to indicate that crossloading takes precedence over data transfer. If **Low** is selected, data transfer has a higher priority then crossloading the image.	No delay occurs. The prompt **Start Flash to Flash Transfer? (Y/N):** appears.
4	Enter **Y** to begin the FLASH-to-FLASH Transfer.	The downloading node: • Verifies a configured server address. • Establishes a server call. • Erases FLASH memory. • Begins the Copy operation. There may a delay of up to three minutes while the erase operation occurs.
	If you are crossloading...	*Then...*
	A Vanguard 6520/6560 node.	The CTP displays this message. **Copying software from the server's Current bank to local Current bank.**
	Any other Vanguard product node.	The CTP displays this message: **Copying software from the server to flash memory.**

Chapter 5
Installing/Crossloading 6500^{PLUS} Nodes

Overview

Introduction

This chapter describes how to install software into 6500^{PLUS} using the NSO Disks supplied with this product, and to crossload software into similar nodes using the RAM-to-RAM method.

You perform software downloads to install new software or to replace corrupted FLASH memory. Before you can operate a 6500^{PLUS} node in a network, you must load operating software into the node's FLASH-based memory.

Operating software has these characteristics:

- Operating software images are stored in 2 Mbytes of FLASH memory in a compressed format.
- Operating software images are decompressed into RAM and executed out of RAM upon node powerup or reboot.

Installing Software Using the NSO Disk

Introduction

You can install, or seed, a 6500^{PLUS} node using the NSO Disk.

Hardware Requirements

To seed a node, this hardware is required:

- A 6500^{PLUS} with 3.xx or 4.xx PROMs, an NSO disk drive, and a FLASH card to be programmed.
- An ASYNC terminal connection to the CTP.
- NSO disks for the desired operation.

■**Note**

Each 6500^{PLUS} node to which Extended Images are to be installed, require 5 Megabytes of FLASH memory.

Software Options for Release 4.15 and Greater

For release 4.15 and later, each software option is available in a two-disk set labelled:

- Disk #1 - Economy option.
- Disk #2 - Extended option.

The Economy option contains the same software images as the corresponding PROM set. The Extended option is a full 5-MB release.

The Economy part of each FLASH can be loaded into any CPU^{PLUS} card that has 3 MB of DRAM. Loading both the Economy and Extended software requires a CPU^{PLUS} card with 5MB of DRAM.

■**Note**

Before you begin, be sure you have Disk #1 and Disk #2, and that both disks are for the same software applications package option.

Seeding a Node Using the NSO Disk

Follow these steps to seed a node using the NSO disk:

Step	Action	Result
1	Insert Disk #1 into the node's NSO card (disk drive). Press the RESET button on the CPU^{PLUS} card to boot the node.	As the node boots, the Economy image of the upgrade software loads into local RAM.
2	After the node comes up and the asterisk (*) prompt appears, connect to the CTP. Examine the node statistics to confirm that the desired option is loaded.	On the first page of the Node Statistics screen, the Download Code Revision shows the new revision of the software and the Download Code Source shows NSO.
3	Select **Copy Disk(s) to FLASH** from the Flash Memory menu	This prompt appears: **FLASH will be erased, Proceed (y/n)**

Step	*Action*		*Result*
4	Enter **n** (no) to abort.		The operation aborts.
	Enter **y** (yes) to continue.		The CTP is unavailable for about one minute while the FLASH is being erased.
			This prompt appears:
			Insert disk number 1, Proceed? (y/n)
5	If you are installing the Extended software option, enter **y** (yes) and proceed to Step 6.		The CTP is unavailable for about one minute while proceeds.
			Then this message appears:
	If you are installing the Economy option, enter **n** (no), and continue at Step 7.		**Insert disk number 2, Proceed? (y/n)** The FLASH Memory menu appears.
6	*If...*	*Then...*	
	You are installing the Extended option	Remove the NSO Disk #1 and insert Disk #2 of the same option.	
		Enter **y** (yes) at **Insert disk number 2, Proceed? (y/n):** to start copying the second disk	The CTP is unavailable for about 30 seconds while copying Disk #2 to FLASH.
		Access the Boot menu and enable the Extended software control option.	
7	Remove the NSO disk and press the RESET button to restart the node.		The node comes up and the * prompt appears.
8	Check the node statistics to confirm that the software for the Extended software is loaded from FLASH and that the size is more than 3,100,000 bytes.		

Seeding a 6500^{PLUS} Node Using the NSO Disk

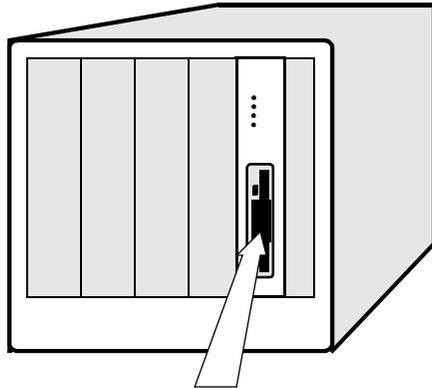Figure 5-1 shows a 6500^{PLUS} node with the NSO disk.

Figure 5-1. 6500^{PLUS} Node With NSO Disk

Crossloading 6500^{PLUS} Nodes Using RAM-to-RAM

Introduction 6500^{PLUS} nodes running 3.xx or 4.15 software must obtain remote software using a RAM-to-RAM transfer. They do not have the FLASH-to-FLASH crossloading capability available in later releases.

Before You Begin Before you begin the RAM-to-RAM crossload procedure:

- Remove disk from the NSO card (if present) on the remote node receiving the software.
- Disable FLASH (if applicable) on the remote node receiving software by doing this:
  - Select Flash Memory from the CTP Main menu.
  - Select Disable Flash Memory.

Crossloading RAM-to-RAM Follow these steps to crossload software to a remote 6500^{PLUS} node running 3.xx or 4.15 software:

Step	Action	Result
1	Define the mnemonic name, in the server node, assigned to the Network management Download Server parameter in the Node-to-Node download record.	
2	Configure these management records for the remote node receiving the software:	The remote node requests software from the 6500^{PLUS} server node with the desired software option.
	a) Select **Management** from the Configure menu	The Configure Management menu appears.
	b) Configure these parameters: –	The Network Management Record Configuration prompts appears.
	– Segment Size: = 0	Indicates the size of the data packet. Normally, you can use the default setting.
	– Network Management Download Server Mnemonic = Dnload	Use the same mnemonic name assigned to the Network Management Download Server parameter in the Node-to-Node Download record for the server node.

Step	*Action*	*Result* (continued)
3	Select **Table and Node record** from the Boot menu in the remote node.	The Table and node record is updated. ■**Note** Complete steps 4 and 5 if you want to transfer the software and save to FLASH in a two step process. Otherwise, complete step 6 to complete the procedure in one step with no verification.
4	Cold boot the remote node receiving the software.	The Economy part of the software option is crossloaded using RAM-to-RAM. This procedure takes a few minutes and occurs in the background. When the asterisk (*) prompt appears, connect to the CTP and check node statistics. Since crossloading is ongoing, the Software source shows PROM (loading RAM). When the procedure is finished, the * prompt appears. When you connect to the CTP and check the Node Statistics, the Download Code revision and the Download Code Source shows Remote.
5	Select **Copy Software to Flash Memory** from the Flash Memory menu**.**	This message appears: **Copy Software to FLASH memory/ Proceed (y/n)** Once you enter **y**, a warning appears and asks you if you want to proceed. If you do, the Economy part of the software option is saved to FLASH. The RAM-to-RAM crossloading is finished.
6	Select **Update Software** from the Boot menu.	The Economy part of the software option is crossloaded using RAM-to-RAM and then saved to FLASH in one step.

Example of RAM-to-RAM Crossloading
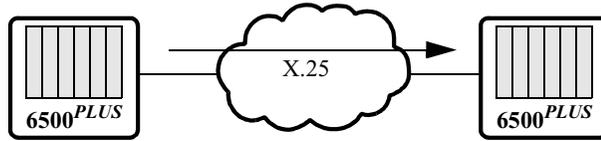
Figure 5-2 shows RAM-to-RAM crossloading.

Figure 5-2. RAM-to-RAM Crossloading

Chapter 6
Saving and Restoring Configurations

Overview

Introduction

This chapter describes the processes involved in saving and restoring configurations using Kermit or TFTP.

You can save and restore a configuration with all the parameter settings. Saving a configuration retains a copy of your configuration on a PC disk so you can retrieve it later, if you want to restore it. A configuration is restored when it is retrieved from a PC disk and placed into a node's configuration memory (CMEM).

When to Save/ Restore

When a configuration is restored, the configuration in configuration memory is overwritten.

- Assign each configuration a unique name so there is no confusion about which is the correct configuration file for a node.
- Save CMEM contents before performing an upgrade or replacing a bad battery to avoid losing a configuration you may later need.
- The configuration that is restored is not implemented until you boot the node using the Node Boot command.

Node Boot

After the CMEM is downloaded to the node through TFTP or KERMIT, you must boot the node using the Node Boot command.

Initiating Save/ Restore Operations

Introduction   Figure 6-1 shows the Configuration Save/Restore menu, available from the Main menu.

```
Node:          Address:              Date:          Time:
Menu: Configuration Save/Restore                    Path: (Main.15)
```

                    — KERMIT Save Configuration
                    — KERMIT Restore Configuration
                    — TFTP Save Configuration
                    — TFTP Restore Configuration
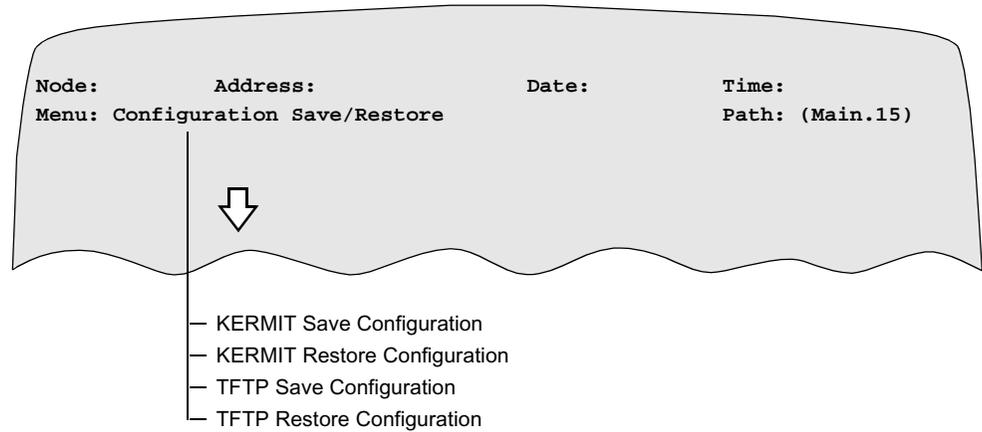
Figure 6-1. Configuration Save/Restore Menu

Methods of Saving/   You can save or restore CMEM contents using:
Restoring
                    • A TFTP server over the LAN
                    • A PC running Kermit or TFTP

Saving and Restoring Configurations with a TFTP Server on a LAN

Introduction

You can use TFTP to save and restore Vanguard 100/200, 6500^{PLUS} or 6520/6560 configurations with all their parameter settings. A configuration is saved when it is stored on a disk in a customer workstation.

You should save a configuration before:

- Downloading software
- Performing an upgrade
- Replacing a bad battery, to avoid losing a configuration you may later need

Use this procedure to save or restore CMEM contents to a TFTP server.

Step	*Action*	*Result*
1	Configure IP connectivity between Vanguard nodes and a TFTP server. Make sure you can PING the TFTP server.	TFTP server is reachable from the appropriate Vanguard 100/200, 6520/6560, or 6500^{PLUS} node.
2	Select **Configuration Save/Restore** from the CTP Main menu.	The Configuration Save/Restore menu appears.
3	Select one of these options and press return: • **TFTP Save Configuration** • **TFTP Restore Configuration**	The **Enter file name:** prompt appears.
4	Enter a configuration file name.	The **Enter IP address:** prompt appears.
5	Enter the IP address. There is no default IP Address.	The **Ready to initiate TFTP transfer?:** prompt appears.
6	Enter **Y** (yes) to start the transfer.	The transfer begins. If the operation is successful, this message appears: **Operation Successful.** If the operation fails, the message **Local Transfer Failure** appears.
	Enter **N** (no) to return to the previous menu.	The previous menu appears. No transfer takes place.
7	After a Restore operation, perform a warm boot to start the software.	The node reboots.

Saving and Restoring Configurations Using Kermit or TFTP

Introduction
You can save and restore CMEM contents to a PC running terminal emulation from a data communications program that supports Kermit and TFTP file transfer protocols.

Prior to saving or restoring Vanguard configurations, you need to install a data communications program on a PC to provide terminal emulation from the PC to the Control Terminal Port (CTP).

■**Note**
Using Kermit or TFTP ties up the CTP connection for the duration of the Save or Restore.

How To Save and Restore
This table describes how to save and restore a configuration using Kermit or TFTP.

Step	Action	Result
1	Select **Configuration Save/Restore** from the Main menu.	The Configuration Save/Restore menu appears.
2	Select one of these: • **KERMIT Save Configuration** • **KERMIT Restore** • **TFTP Save Configuration** • **TFTP Restore Configuration**	Characters such as S~*@_#W appear at the prompt.
3	Depending on the data communications program installed, the steps for using Kermit or TFTP may vary. Follow the directions to receive or send a file for your program.	

If...	Then...
You are saving a configuration to a PC.	a) A message appears stating that the transfer is complete. b) A file with the name of the node followed by .MEM appears in the directory where the data communications program is installed. ■**Note** You can change the directory where the downloaded file appears.
You are restoring a configuration to a node, enter the file name containing the configuration. Then, perform a warm boot.	This message appears: **File Transfer completed.**

Save/Restore Vanguard 320 Configurations with Kermit or TFTP

Figure 6-2 shows the saving and restoring of configuration files between a PC running Kermit or TFTP and a Vanguard 320. The PC is connected to Port 3 or 4 of the Vanguard 320.
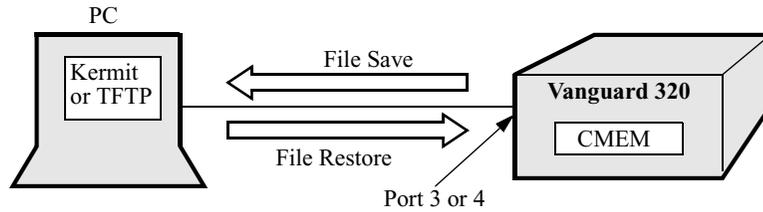

Figure 6-2. Saving and Restoring Vanguard 320 Configurations Using Kermit or TFTP

6500^{PLUS} Save/ Restore Configuration

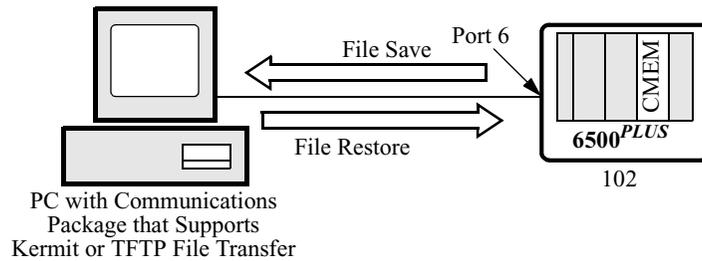Figure 6-3 is an example of saving a 6500^{PLUS} configuration to a PC using Kermit or TFTP.

Figure 6-3. Saving and Restoring Configurations Using Kermit or TFTP

Saving/ Restoring Vanguard 6520/ 6560 Configurations

Figure 6-4 shows the saving and restoring of configuration files between a PC running Kermit or TFTP, a data communications package, and a Vanguard 6520. The PC is connected to port 6 of the Vanguard 6520.
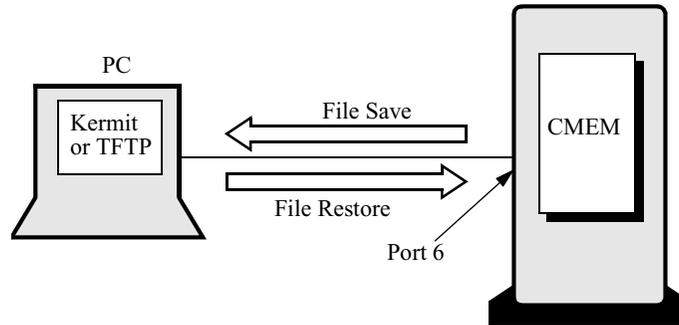
Figure 6-4. Saving/Restoring Vanguard 6520/6560 Configurations Using Kermit or TFTP

Saving And Restoring Configurations

Vanguard Trivial File Transfer Protocol (TFTP) Server

Introduction   The TFTP Server Module provides the capability to download software image files and CMEM configuration files to a remote TFTP client using the TFTP file transfer protocol over the UDP/IP protocol stack. Multiple TFTP transfers are permitted at any one time. Parallel software image and CMEM configuration file transfers via different applications are permitted. The TFTP client on the PC, UNIX or Vanguard node can initiate to download software images and CMEM configuration files from the TFTP Server in the Vanguard node. The multiple TFTP client (up to ten) can initiate file transfer at any one time.

Typical Example   Three examples are defined:

1) Two Vanguards connected together via their Ethernet ports through a LAN are able to perform a TFTP image or CMEM transfer from the Vanguard acting as a TFTP server to the Vanguard acting as a TFTP client.

2) Two Vanguards connected together via their serial interface (i.e. LCON on the Frame relay or X25) are able to perform a TFTP image or CMEM transfer from the Vanguard acting as a TFTP server to the Vanguard acting as a TFTP client.

3) Vanguard connected to a PC via a hub or Ethernet crossover cable should be able to perform an image or CMEM transfer from the Vanguard acting as a TFTP Server to the PC acting as a TFTP Client.

External behavior   The TFTP Server provides packet sequencing to ensure proper delivery order and UDP provides check summing on each packet to ensure data integrity. The TFTP Server Module implementation of the TFTP protocol adheres to RFC 1350 and supports file transfers over UDP to remote TFTP clients that also adhere to RFC 1350.

Operator Interface   A CTP menu interface is provided to the operator to enable and disable the TFTP Server and to access status information about the most recent operation completed or the operation in progress. The parameter required to enable and disable a TFTP Server will be the single parameter. The status and statistics information available to a CTP operator will be displayed by the sequence of the TFTP Server's internal session. There is no configuration record (CMEM) for the TFTP Server parameter.

Configure TFTP Server module

TFTP Server Configuration

The user can configure to enable TFTP Server module with parameter value "enable" and to disable TFTP Server with parameter "disable" like:

Configure -> Configure TFTP Server -> Tftp Server Enable/Disable:

After the TFTP Server is enabled, it shows an alarm message:

"TFTP_SERVER: Server. is Enabled! on Port:69"

The user also can configure to disable TFTP Server module with parameter value "disable". After TFTP Server is disabled, it releases all memory and shows an alarm message:

"TFTP_SERVER: Server is Disabled! on Port: 69"

Image Copy Node to Node

The user can copy software image from node to node using TFTP Server and Client. The commands for the TFTP Client on node is same as existing function.

TFTP sw download -> current

The file name of image should be "*.xrc". The TFTP Server on node can download software image to the multiple node with TFTP Client (up to ten). But the TFTP Server on Tiger platform is allowed to transfer only one software image at any one time, because Tiger platform's file system does not support multiple file access.

After initiating image file transfer by the TFTP Client, the TFTP Server generates an XRC file format with flash binary data and show alarm message:

"Image Downloading Start with 'filename' to 'IP Address"

Image Copy Node to PC/UNIX

The user can copy software image from node to PC or UNIX system using TFTP Client. The file name of software image should be "*.xrc" and file transfer mode should be binary mode, as shown below:

"tftp -I IP_Address GET *.xrc"

The TFTP Server on node can download software image to the multiple TFTP Client (up to ten). But the TFTP Server on Tiger platform is allowed to transfer only one software image at any one time, because Tiger platform's file system does not support multiple file access.

After initiating image file transfer by the TFTP Client, the TFTP Server generates an XRC file format with flash binary data and shows the alarm message below:

"Image Downloading Start with 'filename' to 'IP Address' ".

The TFTP Client will receive "*.xrc" file and save it into the PC or UNIX platform.

CMEM Copy Node to Node

The user can copy configuration from node to node using TFTP Server and Client. The commands for the TFTP Client on node is same as existing function.

TFTP restore configuration

The file name of configuration should be "*.mem". The TFTP Server on node can download configuration to the multiple node with TFTP Client (up to 10). After initiating configuration file transfer by the TFTP Client, the TFTP Server will generate binary file format with configuration data and show alarm message:

"CMEM Downloading Start with 'filename' to 'IP Address' ".

CMEM Copy Node to PC/UNIX

The user can copy configuration from node to PC or UNIX system using TFTP Client. The file name of configuration should be "*.mem" and file transfer mode should be binary mode like :

   "tftp -I IP_Address GET *.mem"

The TFTP Server on node can download configuration to the multiple TFTP Client (up to 10). After initiating configuration file transfer by the TFTP Client, the TFTP Server will generate binary file format with configuration data and show alarm message like:

  "CMEM Downloading Start with 'filename' to 'IP Address' ".

The TFTP Client will receive "*.mem" file and save it into the PC or UNIX platform.

Description Copy Node to PC/UNIX

The user can copy description from node to PC or UNIX system using TFTP Client. The file name of description should be "*.des" and file transfer mode should be text mode like :

   "tftp IP_Address GET *.des"

The TFTP Server on node can download description to the multiple TFTP Client (up to 10). After initiating description file transfer by the TFTP Client, the TFTP Server will generate text file format with description data and show alarm message like:

  "Descript Downloading Start with 'filename' to 'IP Address' ".

The TFTP Client will receive "*.des" file and save it into the PC or UNIX platform.

Introduction

The following sections apply to U.S.A. customers only. Non-U.S.A. customers with questions or concerns regarding return procedures should contact their Vanguard Managed Solutions subsidiary or distributor.

Equipment Return Procedures

If you have questions about equipment return procedures, on-site service or unit exchange service call the Vanguard Managed Solutions Technical Support Center at (800) 544-0062 for advice and assistance.

In Case of Damage

If the equipment is damaged in transit, contact the shipper.

If you have additional concerns in case of failure, about missing parts, or to return equipment, contact your nearest Vanguard Managed Solutions representative.

For Locations	Contact...
Inside the United States	Vanguard Managed Solutions, LLC 575 West Street, Mansfield, MA 02048-1193 Phone (800) 544-0062.
Outside the United States	the nearest Vanguard Managed Solutions distributor. For a listing of our Sales and Service Offices, visit our Web site at: **http://www.vanguardms.com/**

Expiration of Lease

To return equipment upon expiration of a lease agreement, contact the Vanguard Managed Solutions Customer Operations Center at (800) 446-0144 for return authorization and instructions. You will be asked to provide the following information:

- Product name and description
- Serial number
- Customer order number
- Reason for return

Factory Repair To return equipment for factory repair, call the Vanguard Managed Solutions Technical Support Center at (800) 544-0062, for return authorization and instructions. When you call, you will be given a Return Material Authorization (RMA) control number. Mark this number clearly on the shipping container for ease of identification and faster service. The RMA control number provides a convenient tracking reference for both parties. Please have the following information available for each piece of equipment you return:

- Product name and description
- Serial number
- Failure symptoms

Packaging Guidelines for Equipment Return Data communications equipment or parts that are to be returned to Vanguard Managed Solutions for any reason must be properly packaged to prevent damage in shipment and handling.

If the original packing material and shipping container are available, reuse these items to return equipment. If these items are not available, it is your responsibility to package the contents in a manner that protects the equipment from damage during normal shipping and handling. Responsibility for damage to equipment during transit must be resolved between you and the carrier. Vanguard Managed Solutions can provide you with specific packaging instructions upon request.

Index

V

W

Z