Vanguard Managed Solutions

Vanguard Applications Ware
Release 6.4

Alarms and Reports Manual

Notice

©2004 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Unpublished - rights reserved under the copyright laws of the United States.

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 of Vanguard Managed Solutions, 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 Vanguard Managed Solutions Software License Agreement.

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

Writer: Denise Skinner
Part No. T0005, Rev T
Publication Code DS
First Printing March 1999

Manual is current for Release 6.4 of Vanguard Applications Ware.

To comment, use the Customer Response Card located in this manual, or send an E-Mail to:
LGEN031@vanguardms.com

Contents

About The Vanguard Applications Ware; Alarms and Reports Manual

Special Notices and Translations

Customer Information

Chapter 1. Alarms and Reports Format

Alarms and Reports Presentation 1-2
How Do Alarms Get Generated 1-5
Alarm Message Format 1-7
Alarm Throttling 1-9
Trap Throttling 1-12
Changing Priority 1-13

Chapter 2. Port Alarms and Reports

Chapter 3. Station Alarms and Reports

Chapter 4. Channel Alarms and Reports

Chapter 5. Session Alarms and Reports

Chapter 6. DEBUG Alarms and Reports

Chapter 7. Hardware Generated Alarms and Reports

Chapter 8. ATM Alarms and Reports

Chapter 9. BootP, IP, IPX, OSPF, QoS, VPN, ARP, ETH, GW, ICMP, RIP, SNA, TKR, UDP, PIM, MBR, MFE and XN Alarms and Reports

Contents (continued)

Chapter 10. General and Miscellaneous Alarms and Reports

Chapter 11. Vanguard 7300 Alarms and Reports

7300 Alarms 11-2

Chapter 12. VPN TUNNEL Alarms and Reports

Chapter 13. Border Gateway Protocol and Board Management Alarms and Reports

Chapter 14. DHCP, RADIUS, VLAN, VRRP and PPPo(X) Alarms and Reports

Trap Index

Alarm Index

About The Vanguard Applications Ware; Alarms and Reports Manual

Overview

Introduction

This manual contains a listing of all alarm and report messages generated by the Vanguard Applications Ware. It explains the actions you must perform in order to correct unexpected network situations that may arise while using any of the Applications Ware licenses on Vanguard products.

What is an Alarm

An alarm message is generated by Vanguard Applications Ware, to identify any change in state that occurs within a node itself or in the Applications Ware running on that node.

What is a Report

A report is an information notice that Applications Ware displays on your computer screen whenever specific network events take place. Generally speaking, a report requires no corrective action.

Applicability

This manual is accurate for release 6.2 of Vanguard Applications Ware.

What's In This Manual

This manual is divided into these chapters:

This Chapter...	*Describes...*
Chapter 1, Alarms and Reports Format	how alarms are presented within this manual, how and when they are generated, how to throttle the flow of alarms, and how to change the priority of an alarm.
Chapter 2, Port Alarms and Reports	the alarms and reports that are associated with Vanguard Ports.
Chapter 3, Station Alarms and Reports	the alarms and reports that are associated with a Vanguard Station.
Chapter 4, Channel Alarms and Reports	the alarms and reports that are associated with a Vanguard Channel.
Chapter 5, Session Alarms and Reports	the alarms and reports that are associated with Vanguard Sessions.
Chapter 6, DEBUG Alarms and Reports	the alarms and reports that are associated with Vanguard DEBUG.
Chapter 7, Hardware Generated Alarms and Reports	the alarms and reports that are associated with Vanguard hardware components.

This Chapter...	***Describes...*** *(continued)*
Chapter 8, ATM Alarms and Reports	all alarms and reports generated by the ATM protocol.
Chapter 9, BootP, IP, IPX, QoS, VPN, ARP, ETH, GW, ICMP, RIP, SNA, TKR, UDP, PIM, MBR, MFE and XN Alarms and Reports	all alarms and reports for: IP (Internet Protocol), IPX (Internet Packet Exchange), OSPF (Open Shortest Path First), QoS (Quality of Service), VPN (Virtual Private Network), ARP (Address Resolution Protocol), ETH (Ethernet), GW (Gateway), ICMP (Internet Control Message Protocol), RIP (Routing Information Protocol), SNA (SNABSC), TKR (Token Ring), UDP (User Datagram Protocol), and XN (Xerox Network Core) protocols. **■ Note** Many of these alarms and reports do not have Trap Numbers upon which to search.
Chapter 10, General and Miscellaneous Alarms and Reports	general and miscellaneous alarms and reports that can not be found in any other Chapter.
Chapter 11, Vanguard 7300 Alarms and Reports	general and miscellaneous alarms and reports that are Vanguard 7300 specific.
Chapter 12, Vanguard VPN Tunnel Alarms and Reports	special Virtual Private Network (VPN) Tunnel alarms and reports.
Chapter 13, Border Gateway Protocol (BGP) and Board Management Alarms and Reports	general and miscellaneous alarms and reports that are BGP and Board Management specific. **■ Note** Many of these alarms and reports do not have Trap Numbers upon which to search.
Chapter 14, PPPoE, VLAN, VRRP, RADIUS, and DHCP	general and miscellaneous alarms and reports that are PPP and IP specific.
Trap Index	the page location for every alarm and report organized by SNMP trap number.
Alarm Index	the page location for every alarm and report organized by the alarm message.

Indexes

This manual contains two separate indexes that will help you to locate any alarm you may be looking for. These indexes itemize every alarm and report found in this manual by either the Trap Number, which is useful if you are using an SNMP Manager, or the Alarm message itself. If you are reporting alarms to your CTP screen or outputting to a printer, this index will be of greater assistance in your search.

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

Følgende overskrifter fremhæver nogle af oplysningerne i vejledningen. De tjener hvert et specifikt formål og vises i følgende format:

■Bemærk

Bemærk anvendes til at fremhæve vigtig information.

Forsigtig

Forsigtig understreger oplysninger, som, hvis de ikke bliver fulgt, kan føre 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 tiettyjä oppaan tietoja. Kullakin on oma erikoistarkoituksensa ja ne esitetään seuraavassa muodossa:

Huomaa

Huomautusta käytetään korostamaan tärkeätä tietoa.

Vaara

Vaarailmoitus antaa tietoa, jonka huomiotta jättäminen voi johtaa ohjelmiston, laitteiston tai tietojen vahingoittumiseen.

Varoitus

Varoitus on kaikkein vakavin ilmoitus ja se kertoo mahdollisesta loukkaantumisriskistä.

French

Messages spéciaux

Les messages suivants mettent en valeur certaines informations dans le guide. Chacun d’eux remplit une fonction spéciale et est affiché dans le format indiqué :

Important

Important est utilisé pour souligner des informations critiques au sujet d’une procédure.

Mise en Garde

Une mise en garde vous fournit des informations qui, si elles ne sont pas observées, peuvent se traduire par des dommages pour le logiciel, le matériel ou les données.

Avertissement

Un avertissement constitue le message le plus sérieux, 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, daß Nichtbefolgung zu Software-, Hardware- oder Datenschäden führen kann.

Warnung

Eine Warnung weist Sie darauf hin, daß ernsthafte Körperverletzungsgefahr besteht.

Italian

Simboli speciali

I seguenti simboli, ciascuno con una speciale funzione, evidenziano determinate informazioni all'interno del manuale. Il formato è 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, all'hardware o ai dati.

Avvertenza

Questo tipo di avvertimento indica la presenza di condizioni di rischio che possono causare lesioni fisiche. Si tratta del simbolo più 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 håndboken. Hver merknadstype har en spesiell hensikt og vises på følgende format:

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

Forsiktig
Forsiktig gir deg informasjon om situasjoner som kan føre til skade på programvare, datamaskin eller data dersom den blir fulgt.

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

Customer Information

Customer Questions

Customers who have questions about Vanguard Managed Solutions products or services should contact your VanguardMS 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 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

In an effort to improve product documentation, please complete and return this card by fax to (508) 339-9592; Attention: Product Documentaton. Provide us your feedback.

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

Name _____

Company Name _____

Address _____

_____

_____

Document Title: Vanguard Applications Ware Release 6.1 Alarms and Reports Manual

Part Number: T0005, Revision T

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

Chapter 1
Alarms and Reports Format

Overview

Introduction

This chapter explains the Alarms and Reports that are generated by Vanguard Applications Ware software, and provides the corrective actions necessary to ensure your network continues operating in as an efficient manner as possible.

This chapter contains information on:

- "Alarms and Reports Presentation" on page 1-2
- "How Do Alarms Get Generated" on page 1-5
- "Alarm Message Format" on page 1-7
- "Alarm Throttling" on page 1-9
- "Trap Throttling" on page 1-12

Before you Begin

Before using this manual for the first time, read the *Vanguard Configuration Basics Manual* (Part Number T0113). This basics manual explains how to configure a node to deal with alarms and reports.

Caution

It is important that you understand the concepts of alarm and report generation and what to do with them before attempting to perform any of the Corrective Actions referenced in this manual.

Alarms and Reports Presentation

Introduction

The alarms and reports in this manual appear in the format shown in Figure 1-1.

Alarm Text	Trap No:	Priority:	Severity:	Description	Cleared By:	Corrective Action

Figure 1-1. Alarms and Reports Presentation

This format was designed to help you identify a specific alarm or report and determine what to do about it as quickly as possible.

Alarm Text

When possible, this field shows the exact message that appears on your screen. However, in many cases a variable has been inserted to represent such things as Port/Slot/Station Numbers, hexadecimal codes, or to identify strings of characters/ messages. The use of these variables is defined for every alarm or report that they are used for.

If you are not using the Network Management System to monitor your network, alarms and reports are displayed via your CTP screen or printed to a local printer. In either case, you do not see a Trap Number. To find a specific alarm description, you need to identify, from the displayed message, where your problem is occurring. If this alarm were displayed for example,

FR1-1 - PORT STATUS WARNING - PORT DISABLED

You would recognize that the **FRI-1** component of the alarm identifies a specific *PORT*. To locate the appropriate alarm description and corrective actions you would search through this manual for this criteria:

***PORT (n)* - PORT STATUS WARNING - PORT DISABLED**

Use similar search techniques when looking for alarms for session, stations, and channels.

Trap No.

Each alarm and report is assigned a specific reference number, referred to as Traps. Trap Numbers are required by the Network Management System to identify specific events and work with them.

Priority

The priority number is generated by the Vanguard Control Terminal Port (CTP). There are four different types of alarms and reports. These are:

- High (Priority 1) These alarms indicate that a serious condition exists which may affect such major node functions as: Node and Port Channel Boots, Link Status (Up or Down), and Background diagnostic failure.
- Medium (Priority 2) - This indicates that a situation exists that is less serious in nature that a High priority alarm. Though Medium priority alarms do not necessarily require immediate corrective action, they do demand careful observation. Medium priority alarms include, for example, such things as receiving a frame from an invalid address on a Frame Relay interface.
- Low (Priority 3) - This type of alarm includes such things as: receiving a frame from a Frame Relay Station that was disabled, or a packets size is greater than the maximum allowable on an ISDN D-Channel.
- Connection (identified in this manual as CONN) - Alarms with CONN priority relate to the establishment of a call or connection between two sessions. This type of alarm is particularly useful for monitoring functions such as ISDN Call Establishment.

Note

It is possible to change the priority displayed for alarms and reports generated by Applications Ware. For additional information, please refer to the "Trap Throttling" on page 1-12.

Severity

The Severity Number is generated by the Network Management System and includes five specific levels including:

- Normal - These alarms are for general monitoring purposes only and there should be no corrective actions necessary.
- Minor - Minor alarms do not affect services directly although corrective action may be necessary to prevent them from becoming more serious.
- Major - These alarms relate to the development of a condition that affects service, such as a degradation of a voice link. These alarms should be monitored closely to prevent them becoming more serious.
- Warning - These alarms have the potential for becoming much more serious and the situation causing them, have to be monitored very carefully to prevent their becoming more serious.
- Critical - Critical alarms are generated when a condition affecting services occurs, i.e., a Frame Relay interface link going down, takes place. These alarms require immediate attention.

Note

There is no direct correlation between Priority and Severity. For example, you could find an alarm with a High priority (the most severe) and a Normal Severity (the lowest priority). Although somewhat confusing, remember that the Network Management System uses the Severity and Priority levels for specific internal purposes.

Description

This column explains what has happened to display a specific alarm. In many cases, a variety of causes may exist. Wherever such instances occur, a complete description of all messages is provided. When appropriate, references are also made to related manuals in the Vanguard Applications Ware documentation set.

Cleared By

This column identifies those events that must take place in order for an existing event to be cleared. These activities are referenced by Trap Number, and are used by the network management system.

For example, the alarm identified by Trap Number 1000, Power Supply Down, can only be cleared when the Power Supply Up (Trap Number 1001) event takes place.

Corrective Action

This information identifies the actions you would have to perform to correct the problem responsible for a specific alarm message being displayed. Some messages need no corrective action. When possible, additional references are included to direct you to the appropriate Vanguard Applications Ware documentation set.

How Do Alarms Get Generated

Introduction

You configure alarm characteristics from the Control Terminal Port, much like configuring any other aspect of Vanguard products.

There are two specific parameters to configure Alarm Selection and Alarm Distribution. Both can be accessed from the Node record to determine the type of reports that are generated and where they are sent (control terminal and/or printer).

If the specified reporting device is not connected, the reports are lost. If reports are destined for a remote location, a call is made to establish a connection. After the reports are sent, the connection is terminated. If the call is not accepted, 60 retries are made, one every 10 seconds. This is repeated after 30 minutes.

6500*PLUS* Modulus Operation

When the 6500*PLUS* is mounted in a Modulus 9 or 21 enclosure, the Power Supply Down alarm is generated only when the power supply fails. The alarm is not generated when the power supply is removed from the chassis. In addition, the Power Supply Up alarm is not generated when the power supply is inserted into a Modulus 9 or 21 chassis.

When the 6500*PLUS* is mounted in a Modulus 18 enclosure, the Power Supply Down alarm is generated when the power supply is removed, and the Power Supply Up alarm is generated when it is inserted.

Logging Level

Bridging and routing protocols can also display a logging level, which is a field that classifies each message by the type of event that generated it. Logging levels are:

- Packet trace
- Unusual trace
- Common trace

Configuring Alarms

To configure alarms to be generated, complete this procedure and refer to Figure 1-2:

Step	*Action*	*Result*
1	Select **Configure** from the CTP Main menu.	The Configure menu appears.
2	Select **Node** from the Configure menu.	The first configuration parameter appears on your screen.
3	Scroll through the displayed parameters until Alarm Distribution is displayed.	
4	***If you want to...***	***... enter...***
	Have alarms displayed on your CTP screen	**CTP**
	Have a hard copy of all alarms	**PRIN**
	Have no alarms displayed or printed	**NONE**

Step	Action	Result
5	Press **Enter**.	The Alarm Printer Mnemonic parameter appears.
6	Enter an 8 character name for your printer. This is usually the network address for your printer. If you want alarms displayed on screen, leave this parameter <blank>.	
7	Press **Enter**.	The Alarm Selection parameter appears.
8	Enter the types of alarms you want to be notified of. You can press the question mark (?) and press Enter to display the CTP help screen and obtain complete instructions on what your alarm selection choices are.	
9	Press **Enter**.	The Threshold Alarm Timer parameter appears.
10	Enter the amount of time (in minutes) that you want your node to wait before it can generate the same alarm.	
11	Press **ESC** and save the configuration changes you have made.	You have now configured the way in which alarms are generated and the frequency with which they are delivered to you.

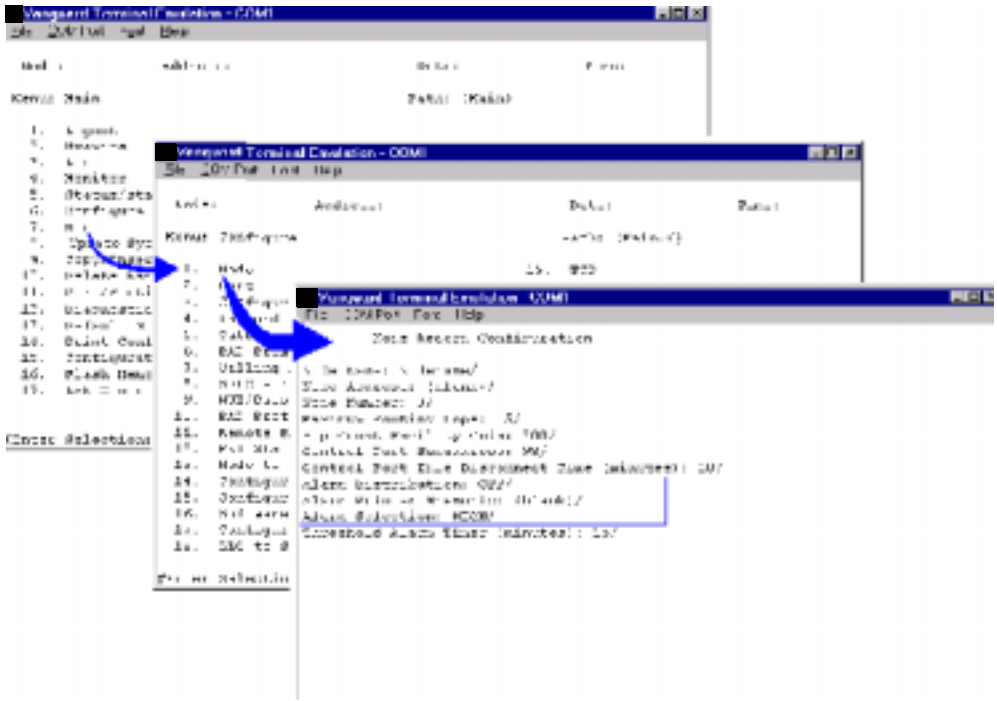


Figure 1-2. How to Configure Alarms Using the CTP

Alarm Message Format

Introduction

The following sections describe alarm formats.

Formats

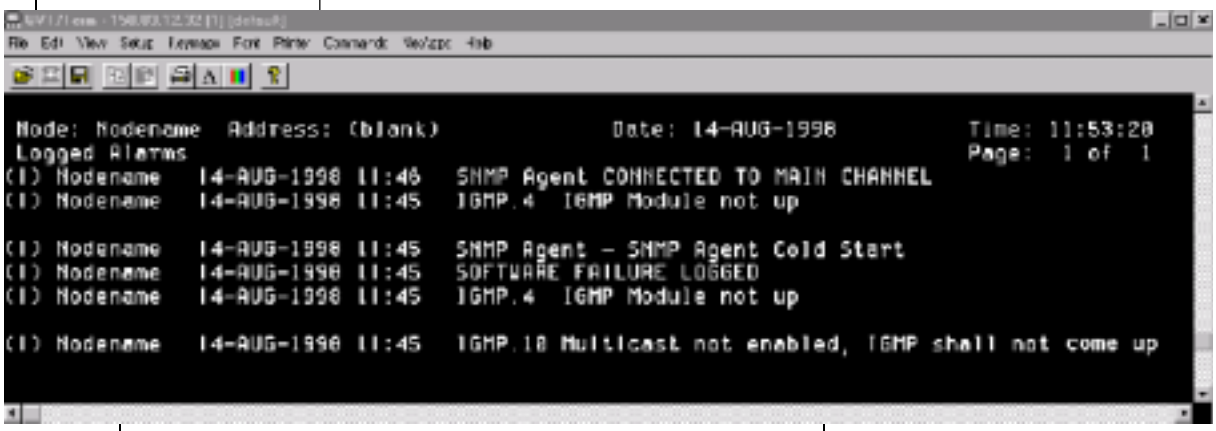
Figure 1-3 shows the format for most Vanguard product alarms and reports as they are viewed from a standard CTP port.

Priority

This identifies the priority level assigned to a particular alarm or message by the Vanguard Applications Ware. Refer to the "Priority" section on page 3 for additional information.

Date/Time Stamp

This identifies exactly when the alarm condition occurred.



Nodename

This is the name of the node that you configured during software installation.

Alarm Text

This text identifies the alarm or message. it includes a report subject (SNMP Agent, IGMP, etc.) and a short descriptive message (CONNECTED TO MAIN CHANNEL, SNMP Agent Cold Start, etc.).

Figure 1-3. Alarms and Reports Example (CTP Display)

Date/Time Stamp

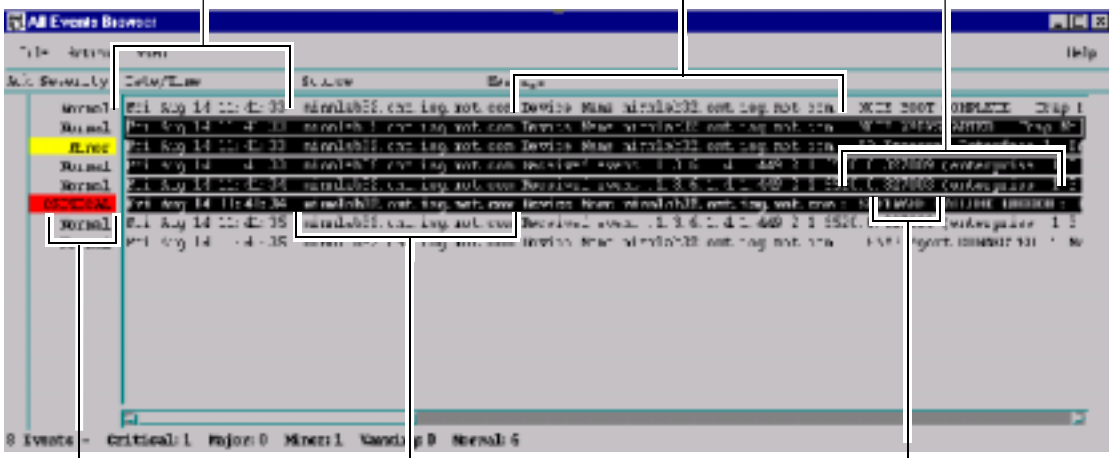
This identifies exactly when the alarm condition occurred.

Device Name

This field identifies the name of the device which caused the alarm to be generated.

Alarm Text

This text identifies the alarm or message with a short description.



Severity

This identifies the alarm severity that the Network Management application assigns to a particular alarm or message. Refer to the "Severity" section on page 3 for additional information.

Trap Number

This number is automatically generated, and is unique, for each alarm and/or report.

Device Address

This field identifies the address of the device which caused the alarm to be generated.

Figure 1-4. Alarms and Reports Example (Network Management Display)

Alarm Throttling

Filtering of Alarms

The ability to throttle alarms is available with release 6.1 or greater. When a node is in critical condition different restart/recovery/report mechanisms are activated. The result is a flood of alarms that report the same problem. Redundant alarms can now be filtered out using throttling.

The alarm throttling mechanism provides the capability of filtering out individual alarms that are the most annoying.

Step	*Action*	*Result*
1	Select **Configure** from the CTP Main menu.	The Configure menu appears.
2	Select **Node** from the Configure Menu. Scroll through the parameters to Alarm Throttling. Set the parameter to **Enable**.	**Alarm Throttling: Enabled/** Alarm Throttling must be Enabled to configure the parameters. When Alarm Throttling is set to Disabled, all alarms return to their default settings and filtering cannot be done. **■Note** You must do a “table and node record” boot for this take effect.
3	Select **Configure** from the CTP Main menu again.	The Configure menu appears.
4	Select **Alarm Throttling** from the Configure menu.	The Alarm Throttling menu appears.
5	Identify the alarm that you want to reconfigure. You need to do this by referencing the Alarm number. If you do not know the alarm number, find the required trap number in one of the Appendices found in this manual and record the corresponding Alarm Number.	You are prompted to start changing parameters.

Configuration Parameters

These parameters must be set in order to configure throttling of alarms:

Entry Number

Range:	1 to 64
Default:	1
Description	Specifies the entry number used to reference the table record.

Alarm Number

Range:	1000 to 2147483647
Default:	1000
Description	Specifies the alarm number to be throttled. Refer to the appropriate chapter in this manual to identify the correct alarm number.

Maximum number of alarms allowed to be generated

Range:	0 to 65535
Default:	5
Description	Specifies the maximum number of alarms that can be generated during the throttling period. When this number of alarms is exceeded, all excessive traps are throttled during the throttling period.

Throttling period (minutes)

Range:	0 to 4096
Default:	15
Description	Specifies the number of minutes that are assigned as the throttling period. During this time, only the number of alarms specified as the “Maximum number of alarms allowed to be generated” is sent. All others are throttled. Any new alarms are sent once the Throttling period has expired. When set to zero (0), alarms are generated but not throttled.

Alarm Level

Range:	UNCHANGED, HIGH, MED, LOW, CONN
Default:	UNCHANGED
Description	Specifies the priority level that should be used for the selected trap. If you select UNCHANGED and have entered non-zero values for the “Maximum number of alarms allowed to be generated” and “Throttling period” parameters, throttling occur as configured but the alarm level does not change. **■ Note** Refer to the Priority section for additional explanations of these levels.

Deleting Alarms

Alarm records can be deleted one-by-one, or all at once.

Main Menu->Delete Record->Alarms Throttling->

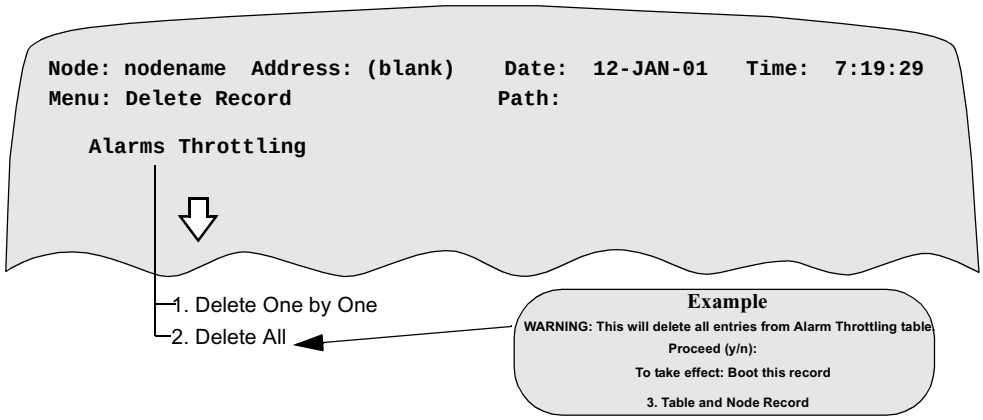


Figure 1-5. Delete Record Menu

Note

To delete the records you must perform a Table and Node Record Boot.

Trap Throttling

Introduction

Vanguard Applications Ware consists of many modules that are, quite often, totally independent of each other. When a node enters a critical state, for example when one of the links goes down, many different modules start to report the same error. This often results in a flood of traps being generated.

The generation of the multiple traps can very quickly congest the Network Management System (NMS) and, because each trap carries the same information, generating so many traps does not simplify the investigation of potential problems. In fact, the generation of multiple traps can sometimes hinder the identification of a problem rather than simplify it. receiving one, or perhaps two traps should be sufficient to identify what node is having a problem, and what that problem is.

For this reason, the SNMP agent on any Vanguard node can throttle these repetitive traps, and you can define the throttling parameters to filter out annoying traps.

Note

64 different traps can be throttled .

For additional information on traps, reports and fatal errors, refer to the Vanguard *Basic Configuration Manual* (Part Number T0113).

Throttling

Throttling is performed on a time basis (that is, a node only generates a number of traps per specified period of time). Repetitive traps generated after the specified period of time expires are not generated.

Configure the node to generate the specified number of traps during the specified time period. Figure 1-6 illustrates this concept, where **T** is the specified time period, **X** the maximum number of traps that can be generated, and **Y** the throttled traps.

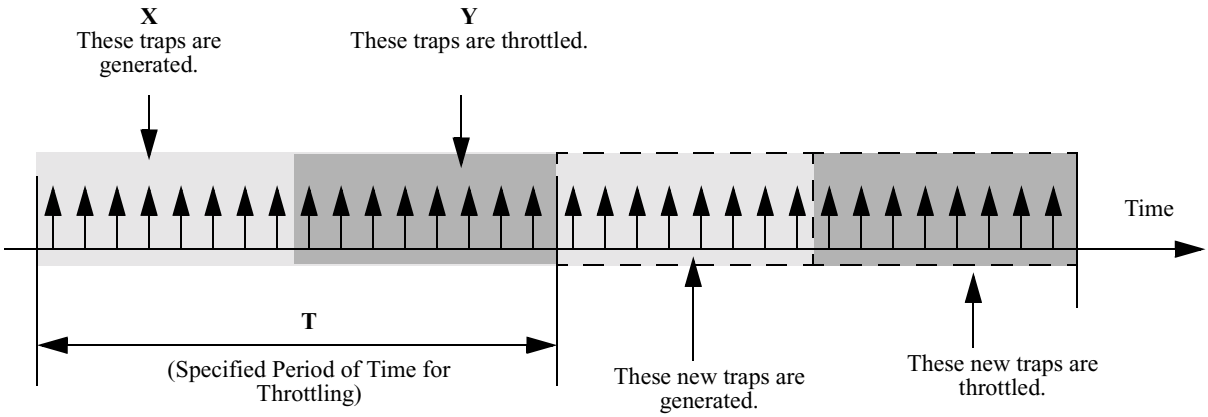


Figure 1-6. Throttling Mechanism

To perform throttling, these three parameters are required:

- trap number (a unique number for each event)
- allowed number of traps that can be generated
- the period of time during which the specified number of traps are generated.

Changing Priority

Introduction

Previously, the assigned Priority (sometimes referred to as the Report Level) was fixed and could not be changed.

The priority is used to control which traps can be generated and which should be suppressed. For example, if the node is configured such that all MEDIUM priority reports are forwarded as traps, all MEDIUM priority reports generated in the node are forwarded in the form of the trap.

However, some situations may arise where you want to change the priority of a particular report. If one report having MEDIUM priority is generated all of the time and you, being aware of the problem, want to suppress trap generation for the report, you could change the priority to LOW and configure the node to suppress all LOW priority reports. This would result in the suppression of the that one report, while all other MEDIUM priority reports would continue to be forwarded as traps.

■Note

The level redefinition feature allows you to change reports by changing the priory of the alarms.

Changing Priority Configuration

The configuration of throttling parameters (trap number, number of traps allowed to be sent and period of time) and defining a new trap level, is performed via the CTP and SNMP. Complete this procedure to reconfigure the priority levels for a specific alarm(s):

■Note

Please refer to the table called cdx6500SNMPTrapThrottleTable found in the file called cdx_6500.mib, located on the Vanguide CD-ROM supporting release 5.3M and later, for SNMP object definitions relating to Trap Throttling.

Step	*Action*	*Result*
1	Select **Configure** from the CTP Main menu.	The Configure menu appears.
2	Select **Configure SNMP** from the Configure menu.	The Configure SNMP menu appears.
3	Identify the alarm that you want to reconfigure. You need to do this by referencing the Trap number. If you do not know the trap number, find the required alarm in one of the Appendices found in this manual and record the corresponding Trap No.	
4	Select **Trap Throttling** from the Configure SNMP menu.	You are prompted to start changing parameters.

Configuration Parameters

These parameters must be set in order to configure throttling of traps:

Entry Number

Range:	1 to 64
Default:	1
Description	Specifies the entry number used to reference the table record.

Trap Number

Range:	1000 to 2147483647
Default:	1000
Description	Specifies the trap number to be throttled. Refer to the appropriate chapter in this manual to identify the correct trap number.

Maximum number of traps allowed to be generated

Range:	0 to 65535
Default:	5
Description	Specifies the maximum number of traps that can be generated during the throttling period. When this number of traps is exceeded, all excessive traps are throttled during the throttling period.

Throttling period (seconds)

Range:	0 to 65535
Default:	60
Description	Specifies the number of seconds that are assigned as the throttling period. During this time, only the number of traps specified as the “Maximum number of traps allowed to be generated” is sent. All others are throttled. Any new traps are sent once the Throttling period has expired. When set to zero (0), traps are generated but not throttled.

Trap level

Range:	UNCHANGED, HIGH, MED, LOW
Default:	UNCHANGED
Description	Specifies the priority level that should be used for the selected trap. If you select UNCHANGED and have entered non-zero values for the “Maximum number of traps allowed to be generated” and “Throttling period” parameters, throttling occur as configured but the trap level does not change. **■ Note** Refer to the Priority section for additional explanations of these levels.

Chapter 2
Port Alarms and Reports

Introduction

This chapter describes those alarms and reports that are generated due to activity surrounding a port on a Vanguard node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BACKUP LINK ACTIVATED	42010	High	Major	This alarm indicates that the backup X.25 link is active and that all alternate links are down.	42007	Check that the alternate links are properly configured.
BRI - *PORT (n)* - PORT BOOT COMPLETE	241010	High	Normal	This message indicates that a port has successfully been booted. The value *PORT (n)* identifies the port number.		This is an information message only. No corrective action is required.
BRI - *PORT (n)* - PORT BOOT FAILED. REASON CODE = *(cause)*	241009	High	Normal	This alarm indicates that an attempt to boot a BRI port has failed. The value *PORT (n)* identifies the port number that failed while *(cause)* gives the Reason Code for this error.		Evaluate the reason code to determine why the port boot failed.
BUFFER NOT AVAILABLE FOR STP CONFIG BPDUs	137005	High	Minor			Contact your customer service representative if this alarm is displayed.
BUFFER NOT AVAILABLE FOR STP TCN BPDUs	137006	High	Minor			Contact your customer service representative if this alarm is displayed.
BUFFER POOL UTILIZATION > THRESHOLD ON CARD *(n)*	3000	Medium	Warning	This message indicates that the buffer pool utilization threshold, on a 6500 PLUS card, has exceeded the configured threshold. The value *(n)* identifies which card this alarm applies to.		Contact customer service representative if this message is displayed.
CFIAB		Medium	Warning	Call Failure - ABT (Abort timer) detected but no carrier.		Check the attached device.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
CFICB		Medium	Warning	Call Failure Indication - local DCE busy.		Check the attached device.
CFIDT		Medium	Warning	Call Failure - No Dial Tone.		Check the attached device.
CFINT		Medium	Warning	Call Failure - No answer back tone.		Check the attached device.
CFIRT		Medium	Warning	Call Failure Indication - Ringback detected.		Check the attached device.
CALL THRESHOLD EXCEEDED	250009	High	Warning	This message indicates that the number of calls, since the switched access path was established for this dial-in port, have exceeded the configured value. No further calls will be permitted on this port and the switched access path will be disconnected once all the existing calls are cleared.	250000	This message is for information only. No corrective actions are necessary.
CVS - Connection to *PORT (n)* terminated before match	373003	Low		This message indicates that the SVC from the calling voice port was disconnected before a match was found. This could happen because the caller hung up or the FRI link between the Calling voice port and the node containing the CVS table went down. The value *PORT (n)* identifies the port which has been disconnected.		This is an information message only. There are no corrective actions necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
DIAGNOSTIC FAILURE ON BOARD *(##)*, *PORT (n)*	19009	High	Critical	This alarm indicates that during diagnostic testing, the board number *(##)* was accessible *PORT (n)* failed the actual diagnostic tests.		Contact your customer service representative for additional information.
DIAGNOSTIC FAILURE ON FLASH SIMM	19011	High	Critical	This error message results from diagnostic tests run on a FLASH SIMM other than the one from which the system was loaded.		Contact your customer service representative for additional information.
DORA - CONFIGURATION ERROR - *(cause)*	252001	Medium	Critical	This alarm indicates that a configuration error exists in the DORA table. The specific error is identified by the *(cause)* indicated and listed below: • NO CONF - No Configuration exists. • NO PRI DORM - Primary DORM DNA has not been configured. • NO PSN ID - PSTN Call Identifier has not been configured. • NO PREFIX - PSTN Prefix has not been configured. • PRI DORM ERR - A Primary DORM DNA Error exists. • SEC DORM ERR - A Secondary DORM DNA Error exists.		To correct this problem: a) Configure the correct X.25 Addresses for DNA, or the Priority and Secondary DORMs in the Dial Out Routing Agent Table. b) Boot the table.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
DORA - DIAL-OUT REQ *(E.164)* ABANDONED - *(cause)*	252004	Low	Major	This message indicates that a dial-out request has been abandoned by DORA due to either: • USER CLR - Cleared by user. • TIMEOUT - Dial-Out Process timer expired. The value *(E.164)* identifies the E.164 address of the dial-out request.		This message is for information only. No corrective actions are necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
DORA - DORM *(address)* COMMUNICATION ERROR - X25 CAUSE *(cause)*	252003	Medium	Normal	This alarm indicates that the local DORA is unable to communicate with the DORM of the indicated X25 Address. The value *(address)* identifies that X.25 address, while *(cause)* will be: • NP - The destination could not be reached. • OCC - The called number is busy. • NC- The network is congested. • INV - An invalid facility was requested. • NA - Access has been barred. • ERR - A local procedure error has occurred. • RPE - Remote procedure error. • DER - The called number is out of order. • ICD - There is an incompatible destination. • FSN - Fast select acceptance has not been subscribed.		To correct this problem, investigate the cause of the failure and restore communication.
DORA - STAT OVERFLow - *(parameter)*	252005	Low	Warning	This message shows that statistics indicated for the value *(parameter)* have overflowed.		This message is for information only. No corrective actions are necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DORA - TABLE OVERFLow	252000	Medium	Major	This alarm indicates that the number of X.32 dial-out ports configured on this node has exceeded the maximum limit of 32.		To correct this problem, check the number of dial out ports configured on the node. The maximum number of X.32 dial-out ports can not exceed 32.
DORA - UNKNOWN CALLER - *(address)*	252002	Medium	Normal	This alarm indicates that a DORA has received a call from an unknown source or indicated X.25 Address. The value *(address)* identifies that X.25 address.		To correct this problem: a) Investigate, and correct, the cause of problem. This will be either and address or configuration problem. b) Boot the table.
DSPM PROTOCOL INITIALIZATION FAILED -*PORT (n)*	281011	High	Normal	This alarm indicates that a Voice port failed initialization. The value *PORT (n)* identifies the port number affected.		If the voice port is configured for H323 operation, verify that the H323 software is installed in the node.
Flow *(src addr -dst addr), (protocol), (src port -dst port)* dropped	403003	Low	Warning	This message indicates that a packet belonging to a flow is dropped because none of the nexthops configured in corresponding flow entry are active.		Reconfigure the policy so at least one of the nexthops configured is currently active.
Flow *(src addr -dst addr), (protocol), (src port -dst port)* is active on nexthop *nnnn*	403002	Low	Normal	This message indicates that the first packet of a flow entry is forwarded by PBR to a nexthop IP address *nnnn* or a serial interface.		This message is for information only. No corrective actions are necessary.
Flow *(src addr -dst addr), (protocol), (src port -dst port)* is expired	403004	Low	Normal	This message indicates that a currently active flow is expired.		This message is for information only. No corrective actions are necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
Flow *(src addr -dst addr), (protocol), (src port -dst port)* is no more active on nexthop *nnnn*	403006	Low	Normal	This message indicates that the nexthop of a currently active flow has gone down.		This message is for information only. No corrective actions are necessary.
Flow *(src addr -dst addr), (protocol), (src port -dst port)* is out of allowed Time of Week	403005	Low	Normal	This message indicates that a currently active flow goes out of the time duration configured in the corresponding TOW profile.		This message is for information only. No corrective actions are necessary.
Flow *(src addr -dst addr), (protocol), (src port -dst port) has* primary link available.	403007	Low	Normal	This message indicates that the primary link is available for the flow which is currently using the backup link		This message is for information only. No corrective actions are necessary.
Illegal Port Type	236006	Medium		This message indicates that AppleTalk is not supported on the specified port type (AppleTalk can be configured only for Ethernet and LCON).		To correct this problem, ensure that AppleTalk is enabled on all port types that it supports.
ILLEGAL PORT TYPE FOR D-CHANNEL	278007	High	Critical			Contact your customer service representative if this alarm is displayed.
INVALID PRI SIGNALLING : PORT = **%d** : STATE = **%d** SIG. STATE = **%d**, STIMULOUS = **%d**	283029	Medium				Contact your customer service representative if this alarm is displayed.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
LBU *PORT (n)* is now servicing multiple ports.	242003	High	Normal	This alarm indicates that a backup link is now serving multiple monitor ports. The value *PORT (n)* identifies the port number.		This is an information message only. No corrective action is required.
MISSING DIM ON BOARD *(x)*, *PORT (n)*	19010	High	Critical	This alarm is generated when diagnostic tests indicate that a DIM is missing from the motherboard. The value *(x)* indicates the board affected while *PORT (n)* identifies the port on that board.		Contact your customer service representative for additional information.
NCI - *PORT (n)* VIOLATIONS, PORT DEGRADED	251002	Medium	Warning	This alarm indicates that a port has been degraded because the maximum number of NUI validation failures configured for that port has been exceeded. This will busy out the port for one minute. During this time, although no new SVCs can be initiated on that port, existing calls will remain unaffected. The port is automatically enabled after one minute for further call attempts. The value *PORT (n)* identifies the PAD, X.25, or X.32 port affected.		To correct this problem, you should investigate the cause of excessive NUI violations on the port and correct this condition.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
NCI - *PORT (n)* VIOLATIONS, PORT DISCONNECTED	251000	Medium	Critical	This alarm indicates that a port has been disconnected because the maximum number of NUI validation failures configured for that port has been exceeded. The port is available for use immediately after it is disconnected. This clears all SVCs on X.25 and X.32 ports. The value *PORT (n)* identifies the PAD, X.25, or X.32 port affected.		To correct this problem, you should investigate the cause of excessive NUI violations on the port and correct this condition.
NCI - *PORT (n)* VIOLATIONS, PORT LOCKED	251001	Medium	Critical	This alarm indicates that a port has been locked because the maximum number of NUI validation failures configured for that port has been exceeded. The port is available for use immediately after it is disconnected. This clears all SVCs on X.25 and X.32 ports. The value *PORT (n)* identifies the PAD, X.25, or X.32 port affected.		To correct this problem, you should investigate the cause of excessive NUI violations on the port, correct this condition, and enable the port.
NCI *PORT (n)* VIOLATIONS, NO ACTION	251003	Medium	Warning	This alarm indicates that the number of NUI violations on an X.28, X.25, or X.32 access port has exceeded the maximum number of NUI validation failures configured for that port.The value *PORT (n)* identifies the port number affected.		To correct this problem, you should investigate the cause of excessive NUI violations on the port.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
No zone for seed routing port	236006	Medium		This message indicates that AppleTalk, on a interface has not been configured with a default zone.		Configure a default zone and then boot the node.
PBR cache cleared	403008	Low	Warning	This message indicates that the PBR cache is cleared.		This is an information message only. There are no corrective actions necessary.
PBR cache overflow	403009	Low	Warning	This message indicates that the PBR cache overflow occurred (that is, the number of PBR sessions exceeds the maximum allowed PBR sessions in the node.		This is an information message only. There are no corrective actions necessary.
PORT (n) (i/o) PORT UTILIZATION > THRESHOLD	300003	High	Warning	This message indicates that the current receive/transmit utilization of available bandwidth exceeds 60% of its capacity. The value *PORT (n)* indicates the port affected while *(i/o)* indicates whether the input or output port utilization threshold has been exceeded.	300000	This is an information message only. There are no corrective actions necessary.
PORT (n) - ACCESS PORT DOWN	42012	Low	Normal	This alarm indicates that primary link is down.The value *PORT (n)* identifies the X.25 port that is down.		To correct this problem: • Check the physical link connection. • Check the port speed and changes as required. • Check that the correct DCE/DTE interfaces are configured.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) - ACCESS PORT DOWN	43012	Low	Normal	This alarm indicates that a primary link is Down. The value *PORT (n)* identifies the port affected.		To correct this problem: • Check the physical link connection. • Check the port speed and changes as required. • Check that the correct DCE/ DTE interfaces are configured.
PORT (n) - ACCESS PORT DOWN	195012	Low	Normal	This alarm indicates that the primary link is down. The value *PORT (n)* identifies the port affected.		To correct this problem: • Check the physical link connection. • Check the port speed and changes as required. • Check that the correct DCE/ DTE interfaces are configured.
PORT (n) - ACCESS PORT UP	42013	Low	Normal	This message indicate that primary link is now operational. The value *PORT (n)* identifies the X.25 port affected.		This is an information message only. No corrective action is required.
PORT (n) - ACCESS PORT UP	43013	Low	Normal	This message indicate that primary link is now operational. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - ACCESS PORT UP	195013	Low	Normal	This message indicate that primary link is now operational. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - ALLOCATED *(x)* BYTES FOR PPP TRACING	268007	High	Normal	This message indicates that PPP tracing has been turned on. The value *PORT (n)* identifies the PPP port affected while *(x)* identifies the number of bytes allocated.		This message is for information only. No corrective actions are necessary.
PORT (n) - AUTOCALL RETRIES EXHAUSTED, REBOOT THE PORT	227005	High	Critical	This alarm indicates that the configured number of Autocall Retries has been exhausted. The value *PORT (n)* identifies the port affected.		To correct this problem: • Check the X.25 link. • Check the Routing Table configuration.
PORT (n) - BAD FRAME TYPE *(x)*	42011	Low	Minor	This alarm indicates that a bad frame type was received. The value *PORT (n)* identifies the X.25 port that received the bad frame, while *(x)* identifies the frame type itself. **■Note** This alarm is generated by a Siemens SDLC or HDLC port.	42007	Check the port connections to ensure that they are properly connected.
PORT (n) - BAD FRAME TYPE *(x)*	43011	Low	Minor	This alarm indicates that a bad frame type was received. The value *PORT (n)* identifies the port that received the bad frame, while *(x)* identifies the frame type itself. **■Note** This alarm is generated by a Siemens SDLC or HDLC port.	43007	Check the port connections to ensure that they are properly connected.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - BAD FRAME TYPE *(x)*	195011	Low	Minor	This alarm indicates that a bad frame type was received. The value *PORT (n)* identifies the port that received the bad frame, while *(x)* identifies the frame type itself. **■Note** This alarm is generated by a Siemens SDLC or HDLC port.		Check the port connections to ensure that they are properly connected.
PORT (n) - BAD N*(R) (n)*	43009	Low	Minor	This alarm indicates that a Received bad acknowledge sequence number. The value *PORT (n)* identifies the port affected while *(n)* identifies the sequence number.	43007	Check the device connections and verify that the correct device is attached.
PORT (n) - BAD N(R) *(sn)*	42009	Low	Minor	This alarm indicates that a Received bad acknowledge sequence number. The value *PORT (n)* identifies the X.25 port affected while *(sn)* identifies the sequence number.	42007	Check the device connections and verify that the correct device is attached.
PORT (n) - BAD N*(R) (sn)*	195009	Low	Minor	This alarm indicates that a Received bad acknowledge sequence number. The value *PORT (n)* identifies the port affected while *(sn)* identifies the sequence number.		Check the device connections and verify that the correct device is attached.
PORT (n) - BAD P*(K)*				This alarm indicates a packet was received with the wrong K window number, or corruption of out of sync frames.		Check the K, W, and P packet sizes at both ends. Make sure the packet window sizes match at both ends.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - BAD PID IN CALL FROM *(remote address)*	318013	High	Minor	This alarm indicates that a call has been received from the remote address mentioned in the report, containing an invalid Protocol ID in the CUD of the call packet. The value *PORT (n)* indicates the port number that received the call, while *(remote address)* identifies the address of the remote node.	318000	This alarm is intended to alert against call attempts from unauthorized sources. Check the call originator.
PORT (n) - BAD TID IN CALL FROM *(remote address)*	318012	High	Minor	This alarm indicates that a call has been received, from the remote address mentioned in the report, containing an invalid Terminal ID in the CUD of the call packet. The value *PORT (n)* indicates the port number that received the call, while *(remote address)* identifies the address of the remote node.	318000	This report is intended to alert against call attempts from unauthorized sources. Check the call originator.
PORT (n) - BOOT TO NEW PORT FAILURE, PORT DOES NOT SUPPORT DYNAMIC CREATE	2004	High	Critical	This alarm indicates that the new port type does not support dynamic port boot. The value *PORT (n)* identifies the port affected.	2002	Boot the node to install a new port type if this is acceptable. Otherwise, select another port type and reboot.
PORT (n) - BROADCAST OVERRUN	44003	Low	Major	This alarm is generated when broadcast data to this channel, or port, is lost. The value *PORT (n)* indicates the port number.		Decrease the amount of broadcast data.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - CALL CLEARED BY HOST *(cause)*	215008	Medium	Normal	This message indicates that the call towards the host is cleared. The cause code for the clear is displayed along with the report. The value *PORT (n)* identifies the port number affected while *(cause)* identifies the cause code for clearing the call.		Refer to the appropriate Applications Ware Feature Protocols Documentation for explanations of the displayed cause code and correct as required.
PORT (n) - CALL CLEARED BY NETWORK, CAUSE CODE *(x)*	227012	Medium	Minor	This alarm indicates that an X.25 call has been cleared by the network. The value *PORT (n)* identifies the port affected, while *(x)* identifies the X.25 Cause code.		Check the X.25 cabling and, if the problem is not corrected, refer to the X.25 Basic Configuration Manual to identify the cause codes.
PORT (n) - CALL CLEARED BY REMOTE TNPP PAD	227007	Medium	Normal	This alarm indicates that an X.25 call has been cleared by the remote TNPP PAD The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - CALL REJECTED BY LEVEL3 *(cause)*	215009	Medium	Major	This alarm indicates that the call towards the host has failed to establish itself. The value *PORT (n)* identifies the port number affected, while *(cause)* identifies the cause code.		Check the configuration of the Autocall Mnemonic parameter in the Mnemonic Table. **■ Note** Refer to the appropriate Applications Ware Feature Protocols Documentation for explanations of the displayed cause code and correct as required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - CALL REJECTED BY LEVEL3 - *(cause)*	227008	Medium	Minor	This alarm indicates that an X.25 call to a remote TNPP PAD has been cleared by internal layer 3. The value *PORT (n)* identifies the port affected while *(cause)* identifies one of these potential causes of the problem: • 0: No address specified • 1: The call is made while the previous connection was being established. • 2: A timeout occurred before the call accept is received from the remote end. • 3: A call collision was detected. • 4: A call accept has failed.		To correct this problem: a) Reboot the port. b) Check the mnemonic. c) Check the autocall timer values on both TNPP PADs to avoid call collision.
PORT (n) - COMMAND SYNTAX ERROR	150005	High	Warning	This message should never be displayed.	150000	Contact your customer service representative for additional information.
PORT (n) - CONNECTED TO HOST	215022	Low	Normal	This message indicates that a call, toward a host, has been established.		This is an information message only. No corrective action is required.
PORT (n) - CONNECTION TOWARDS HOST IN PROGRESS	215001	Low	Normal	This message indicates that an X.25 connection, towards a host, is in progress. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - CONTROL FIELD EMPTY CALL REJECTED	215023	Low	Minor	This alarm indicates that the opening frame of the T3POS control field, from the POS terminal, is blank. This condition is not permitted by the T3POS protocol specification.		Check the POS implementation in the protocol. **■ Note** Refer to the T3POS manual in the Vanguard *Serial Feature Protocols Manual* (Part Number T0102) for additional information.
PORT (n) - CONTROL FRAME FROM HOST, CALL CLEARED	215014	Medium	Minor	This message indicates that no control frame (frame starts with SOH character) is allowed from the host and the X.25 call towards host. The connection towards the POS terminal is cleared. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required. **■ Note** Refer to the T3POS manual in the *Vanguard Serial Feature Protocols Manual* (Part Number T0102) for additional information.
PORT (n) - CONTROLLER DOWN *(device)*	86009	High	Major	This alarm indicates that a device is not responding to a poll. The value *PORT (n)* identifies the port affected while *(device)* identifies the device that is not responding.	86010	Check the configured device address and correct as required.
PORT (n) - CONTROLLER OPERATIONAL *(device)*	86010	High	Normal	This alarm indicates that a device has responded to a poll. The value *PORT (n)* identifies the port affected while *(device)* identifies the device that has responded.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - CONNECTION TOWARDS REMOTE TNPP PAD IN PROGRESS	227004	Low	Normal	This message indicates that the X.25 connection the remote TNPP PAD is in progress. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - DLE-EOT TIMEOUT, CALL CLEARED	215004	High	Minor	This message indicates that, for a period of 4 minutes (DLE EOT) no data transfer took place. When this happens the call towards the X.25 host is cleared. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.
PORT (n) - DEBUG TRACE IS ON	268009	High	Normal	This message indicates that the debug trace has been turned on.		This message is for information only. No corrective actions are necessary.
PORT (n) - DEVICE UNAVAILABLE *(device)* DATA LOSS	86011	High	Major	This alarm indicates that data, for the specified device, has been received when the device was unavailable. The value *PORT (n)* identifies the port affected while *(device)* identifies the device that was unavailable.	86000	To correct this problem: a) Verify that the device connections are correct. b) Check power connections to the device.
PORT (n) - DIAL OUT NOT SUPPORTED, CALL REJECTED	215012	Medium	Minor	This message indicates that a T3POS PAD port is configured for the DIMO connection type; dial-outs are not allowed with this connection type. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required. **■ Note** Refer to the T3POS manual in the *Vanguard Serial Feature Protocols Manual* (Part Number T0102) for additional information.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - DISCONNECTED DUE TO LINE ERRORS	56006	High	Major	This message indicates that a call was disconnected due to protocol errors. The value *PORT (n)* indicates the port number.	56000	Check the protocol sequence.
PORT (n) - DLE EOT RECEIVED CALL CLEARED	215002	Medium	Minor	This message indicates that the T3POS end sequence (DLE EOT) is received from the terminal and the X.25 Call towards the host is cleared. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.
PORT (n) - DYNAMIC PORT BEING CREATED	20007	Medium		This message indicates that the software has completely destroyed the old port type and is in the process of creating the new port type via the dynamic port. Depending on Node loading this activity may take an extended amount of time. This delay is to minimize the data passing effect on other ports/devices/stations/ channels.		This is an information message only. No corrective action is required.
PORT (n) - DYNAMIC PORT COMPLETED	20008	High		This message indicates that the software has completed a dynamic port. This destroys and recreates the ports data structures before initialization. The standard port simply re-initializes data structures.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - DYNAMIC PORT STARTED	20006	High		This message indicates that the software is in the process of destroying the current on-line port type via the dynamic port. Depending on Node loading this activity may take an extended amount of time. This delay is to minimize the data passing effect on other ports/devices/stations/ channels. The value *PORT (n)* identifies the port that has been reconfigured.		This is an information message only. No corrective action is required.
PORT (n) - END-TO-END PACKET RELEASED - RX ERROR ORDER	87020	High		This alarm is typically a Telco issue. Either pieces of segmented frames are being dropped or discarded in the network due to physical level problems or congestion, or the Telco is delivering them out of order.		Ensure the circuit is clean and if using frame relay ensure that the provider is not dropping or discarding any frames. Contact your customer service representative if you need assistance with this alarm.
PORT (n) - FAILURE PORT DOES NOT EXIST	20009	High		This alarm indicates the port is not seen as existing in the node. n is the port number.		Check the port number and confirm that it exists as a physical/virtual port.
PORT (n) - FAILURE PORT DOES NOT EXIST	20009	High		This alarm indicates that the port is not seen as existing in the node. n is the port number.		Check the port number and confirm that it exists as a physical/virtual port.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - FAT TIMER EXPIRED, LINE DISCONNECTING	215000	High	Minor	This alarm indicates that the dial-up link between a T3POS PAD port and a POS terminal is being disconnected. This is typically due to no response having been received during the T6 (Frame Arrival Timer) timeout. The value *PORT (n)* identifies the port number affected.		Determine whether the POS terminal is operating correctly.
PORT (n) - FRAME RECEIVED FROM UNKNOWN DLCI: *(dddd)*	187000	Medium	Warning	This alarm indicates that a frame with an invalid DLCI number has been received from the link. The value *PORT (n)* identifies the FRA station affected, while *(dddd)* identifies the unknown DLCI.		Ensure all stations are configured with DLCI numbers that correspond to those provisioned by the network.
PORT (n) - FRMR *(XX/XX/XX)*	42006	Low	Minor	This alarm indicates that a received frame was rejected while in the normal sequencing mode. The value *PORT (n)* indicates the X.25 port affected while *(XX)* identifies the hexadecimal value and length of the FRMR information field.	42007	Check the configured frame size and verify that the attached equipment is properly connected and configured.
PORT (n) - FRMR *(XX/XX/XX)*	43006	Low	Minor	This alarm indicates that a received frame was rejected while in the normal sequencing mode. The value *PORT (n)* indicates the port affected while *(XX)* identifies the hexadecimal value and length of the FRMR information field.	43007	Check the configured frame size and verify that the attached equipment is properly connected and configured.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) - FRMR *(XX/XX/XX)*	195006	Low	Minor	This alarm indicates that a received frame was rejected while in the normal sequencing mode. The value *PORT (n)* indicates the port affected while *(XX)* identifies the hexadecimal value and length of the FRMR information field.		Check the configured frame size and verify that the attached equipment is properly connected and configured.
PORT (n) - FRMR *(XX/XX/XX/XX/XX)*	42005	Low	Minor	This alarm indicates that a received frame was rejected while in the extended sequencing mode. The value *PORT (n)* indicates the X.25 port affected while *(XX)* identifies the hexadecimal value and length of the FRMR information field.	42007	Check the configured frame size and verify that the attached equipment is properly connected and configured.
PORT (n) - FRMR *(XX/XX/XX/XX/XX)*	43005	Low	Minor	This alarm indicates that a received frame was rejected while in the extended sequencing mode. The value *PORT (n)* indicates the port affected while *(XX)* identifies the hexadecimal value and length of the FRMR information field.	43007	Check the configured frame size and verify that the attached equipment is properly connected and configured.
PORT (n) - FRMR *(XX/XX/XX/XX/XX)*	195005	Low	Minor	This alarm indicates that a received frame was rejected while in the extended sequencing mode. The value *PORT (n)* indicates the port affected while *(XX)* identifies the hexadecimal value and length of the FRMR information field.		Check the configured frame size and verify that the attached equipment is properly connected and configured.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - HOST FRAME SIZE EXCEEDED, CALL CLEARED	215013	Medium	Minor	This alarm indicates that the length of the T3POS data frame, received from the host, exceeds the configured limit. The value *PORT (n)* identifies the port number affected.		Change the MAXIMUM FRAME SIZE parameter of the Port record. **■ Note** Refer to the T3POS manual in the *Vanguard Serial Feature Protocols Manual* (Part Number T0102) for additional information.
PORT (n) - HP ENQ/ ACK TIMEOUT	44002	Medium	Minor	This alarm is indicates that a PAD port, configured as HPENQ/ ACK, failed to receive the Acknowledgment from the attached terminal within 10 seconds of sending an ENQ. The value *PORT (n)* indicates the port number.		Verify that cable and equipment are working properly.
PORT (n) - I.430 DIM INSTALLED ON INVALID PORT	341000	High	Critical	This alarm indicates that a DIM has been installed in the wrong port. *PORT (n)* identifies the port affected.		Reinstall the DIM in the correct port number.
PORT (n) - INVITATION TO CLEAR FROM HOST, CALL CLEARED	215019	Medium	Minor	This message indicates that an Invitation to Clear message has been received from the host and that the call, towards the host, and the connection to POS terminal are being cleared.		This is an information message only. No corrective action is required. **■ Note** Refer to the T3POS manual in the *Vanguard Serial Feature Protocols Manual* (Part Number T0102) for more information.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - INITIALIZATION FAILED	268008	High	Critical	This message indicates that a port boot has failed to initialize. The value *PORT (n)* identifies the PPP port affected.	268000	Check the port configuration and all equipment connected to that node.
PORT (n) - INITIALIZATION FAILED, SOFTWARE BUG DETECTED in *(code)* at line *(line)*	110016	High	Critical	This alarm indicates that a problem with one of the software modules has been detected. The value *PORT (n)* indicates the port affected, *(code)* identifies the source code containing the error and *(n)* identifies the exact location of the error.		This alarm should never be displayed. If it does appear, contact customer service and report a software bug.
PORT (n) - INPUT BUFFER OVERRUN	44000	Medium	Major	This alarm indicates that an X.25 port output queue has overflowed and data has been lost. The value *PORT (n)* indicates the port number.		Check the flow control parameters on the adjacent port.
PORT (n) - INPUT QUEUE OVERRUN	215007	Medium	Major	This alarm indicates that the queue towards the remote host is full. The value *PORT (n)* identifies the port number affected.		The X.25 link may be congested. **■ Note** Refer to the *X.25 Configuration Basics Manual* in the *Vanguard Basic Protocols Manual* (Part Number T0106) for additional information.
PORT (n) - INSUFFICIENT DYNAMIC MEMORY, PORT DOWN GRADED TO NULL PORT	2005	High	Critical	This alarm indicates that the new port type requires more memory than available. The value *PORT (n)* identifies the port affected.	2002	Add more memory to the Dynamic Port Creation heaps in your Vanguard device. **■ Note** Refer to your Vanguard Installation Guide for additional information.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - INSUFFICIENT DYNAMIC MEMORY, PORT DOWN GRADED TO NULL PORT	19017	High	Critical	This alarm indicates that the new port type requires more memory than available. The value *PORT (n)* identifies the port affected.		Contact your customer service representative for additional information.
PORT (n) - INVALID CONTROL FIELD, CALL REJECTED	215020	Medium	Minor	This report indicates that the control fields of the opening T3POS frame received from the POS terminal contains invalid X.28 mnemonic string		Perform these checks to find the cause of this problem and correct as necessary: • Check the Autocall mnemonic configuration. • Check for the routing table configuration for X.25 address. **Note** Refer to the T3POS manual in the *Vanguard Serial Feature Protocols Manual* (Part Number T0102) for more information.
PORT (n) - INVALID FRAME FROM POS, CALL CLEARED	215003	Medium	Minor	This alarm indicates that invalid T3POS frames have been received in response from the POS terminal. The value *PORT (n)* identifies the port number affected.		This alarm is a good indication that the POS terminal is misbehaving.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - INVALID MSS FROM HOST, CALL CLEARED	215011	Medium	Minor	This alarm indicates that invalid Mode Select Switch (MSS) is received from the host in Call request packet. The value *PORT (n)* identifies the port number affected.		The Host implementation does not support the T3POS Protocol specification. **■ Note** Refer to the T3POS manual in the *Vanguard Serial Feature Protocols Manual* (Part Number T0102) for additional information.
PORT (n) - INVALID MSS FROM POS, CALL REJECTED	215010	Medium	Minor	This alarm indicates that an invalid Mode Select Switch (MSS) has been received from the POS terminal, and that the call towards the host is not established. The value *PORT (n)* identifies the port number affected.		The POS terminal does not support the T3POS Protocol specification. **■ Note** Refer to the T3POS manual in the Vanguard *Serial Feature Protocols Manual (Part* Number T0102) for additional information.
PORT (n) - LINE DOWN	86007	High	Major	This alarm indicates that all devices, on the HPAD side, are down, or that a poll was not received on the TPAD side. The value *PORT (n)* identifies the port affected.	86008	To correct this problem: a) Verify that the device addresses are correct. b) Check power connections to the device.
PORT (n) - LINE DOWN	110007	High	Major	This alarm indicates that all devices, on the HPAD side, are down, or that a poll was not received on the TPAD side. The value *PORT (n)* identifies the port affected.	110000, 110008	To correct this problem: a) Verify that the device addresses are correct. b) Check power connections to the device.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - LINE FAILURE, LINE DISCONNECTED	215005	High	Major	This alarm indicates that the dial-up connection between a T3POS PAD port and the POS terminal is disconnected. The value *PORT (n)* identifies the port number affected.		Check the physical connection and correct as required.
PORT (n) - LINE OPERATIONAL	86008	High	Normal	This message indicates that either: • At least one device is responding to a poll on HPAD port. • A poll has been received on a TPAD port. • The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - LINK BLOCKED	42008	Low	Minor	This alarm indicates that a link is blocked. The value *PORT (n)* identifies the X.25 port affected.	42007	Reduce the speed of the attached device.
PORT (n) - LINK BLOCKED	43008	Low	Minor	This alarm indicates that a link is blocked. The value *PORT (n)* identifies the port affected.	43007	Reduce the speed of the attached device.
PORT (n) - LINK BLOCKED	195008	Low	Minor	This alarm indicates that a link is blocked. The value *PORT (n)* identifies the port affected.		Reduce the speed of the attached device.
PORT (n) - LINK UP	42007	High	Normal	This message indicates that a link has entered the data transfer mode and is an indication of a successful SABM-UA exchange. The value *PORT (n)* identifies the X.25 port affected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - LINK UP	43007	High	Normal	This message indicates that a link has entered the data transfer mode and is an indication of a successful SABM-UA exchange. The value *PORT (n)* identifies the port affected.	43007	This is an information message only. No corrective action is required.
PORT (n) - LINK UP	195007	High	Normal	This message indicates that a link has entered the data transfer mode and is an indication of a successful SABM-UA exchange. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - LIST IS EMPTY	86012	High		This message indicates that no data packets were found, in the list for that device, while doing end to end acknowledge of a packet. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - LIST IS NOT EMPTY	86013	High		This message indicates that data packets were found in the outgoing list for that device while extracting a complete BSC DATA block from the queue of received blocks from DSP. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - MNEMONIC IS EITHERBLANK OR NOT CONFIGURED - *(cause)*	227009	Medium	Critical	This alarm indicates that the mnemonic is not configured correctly. The value *PORT (n)* identifies the port affected while *(cause)* identifies one of these potential causes of the problem: • 1: Invalid Mnemonic • 2: No period is allowed in the mnemonic • 9: Mnemonic not found in Mnemonic Table • 10: Mnemonic length too long		To correct this problem: a) Reconfigure the mnemonic and the mnemonic table. b) Reboot the port and tables.
PORT (n) - NO COMMANDS	150006	High	Normal	This message should never be displayed.		Contact your customer service representative for additional information.
PORT (n) - NO RESPONSE	56005	High	Minor	This alarm indicates that a device attached to your Vanguard has not responded properly to an ENQ call. The port has rejected the call. The value *PORT (n)* identifies the port affected.	56000	To correct this problem, identify the device and verify that all cables are properly attached and the device is operating correctly.
PORT (n) - NON-RECOVERABLE INBOUND ERROR	86005	High	Major	This alarm indicates that an incomplete inbound operation, for example, a response to ACK or NAK not being received or an EOM character not received, has occurred. The value *PORT (n)* identifies the port affected.	88000	To correct this problem: • Check the port connections. • Check for noise on the line. • Verify that the port is set for the correct speed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - NON-RECOVERABLE INBOUND ERROR	110005	High	Major	This alarm indicates that an incomplete inbound operation, for example, a response to ACK or NAK not being received or an EOM character not received, has occurred. The value *PORT (n)* identifies the port affected.	110000	To correct this problem: • Check the port connections. • Check for noise on the line. • Verify that the port is set for the correct speed.
PORT (n) - NON-RECOVERABLE OUTBOUND ERROR	86006	High	Major	This alarm indicates that an incomplete outbound operation has occurred. The value *PORT (n)* identifies the port affected.	96000	To correct this problem: • Check the port connections. • Check for noise on the line. • Verify that the port is set for the correct speed.
PORT (n) - NON-RECOVERABLE OUTBOUND ERROR	110006	High	Major	This alarm indicates that an incomplete outbound operation has occurred. The value *PORT (n)* identifies the port affected.	110000	To correct this problem: • Check the port connections. • Check for noise on the line. • Verify that the port is set for the correct speed.
PORT (n) - NOT AUTHORIZED TO USE POLLED ASYNC OPTION	44004	High	Critical	This alarm is generated when you attempt to enable the Polled Async feature without first enabling the CSK. The value *PORT (n)* indicates the port number.		Enable the Polled Async CSK and reboot the PAD port. **■ Note** Refer to the *Vanguard Configuration Basics Manual* (Part Number T0113) for instructions on enabling a CSK.
PORT (n) - OUTBOUND LINK BLOCKED	308047	Low	Minor	This alarm indicates that the message queue to a TPAD port is blocked. The value *PORT (n)* indicates the port number affected.	308046	Check the link speed between HPAD and TPAD.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - OUTBOUND LINK UNBLOCKED	308048	Low	Normal	This alarm indicates that the message queue to a TPAD port is no longer blocked. The value *PORT (n)* indicates the port number affected.		This is an information message only. There are no corrective actions necessary.
PORT (n) - OUTPUT BUFFER OVERRUN	44006	Medium	Major	This report indicates that the data queue towards the terminal is full. The value *PORT (n)* indicates the port number.		Check if the Async connection between PAD port and the terminal is flow-controlled due to speed mismatch.
PORT (n) - OUTPUT QUEUE OVERRUN	215006	Medium	Major	This alarm indicates that the queue towards the POS terminal is full. The value *PORT (n)* identifies the port number affected.		Ensure that the X.25 port and the T3POS PAD port speeds are configured to the same value.
PORT (n) - OVERSIZE FRAME *(s)* FROM REMOTE LINK	42014	Medium	Minor	This alarm indicates that a frame is too big to be sent out over the remote link. The value *PORT (n)* indicates the port number and *(s)* indicates the frame size. **■Note** This applies to Siemens SDLC or HDLC ports only.	42007	Check the configured frame size and modify as required to allow the frame to be sent out.
PORT (n) - OVERSIZE FRAME *(s)* FROM REMOTE LINK	43014	Medium	Minor	This alarm indicates that a frame is too big to be sent out over the remote link. The value *PORT (n)* indicates the port number and *(s)* indicates the frame size. **■Note** This applies to Siemens SDLC or HDLC ports only.	43007	Check the configured frame size and modify as required to allow the frame to be sent out.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - OVERSIZE FRAME *(s)* FROM REMOTE LINK	195014	Medium	Minor	This alarm indicates that a frame is too big to be sent out over the remote link. The value *PORT (n)* indicates the port number and *(s)* indicates the frame size. **■Note** This applies to Siemens SDLC or HDLC ports only.		Check the configured frame size and modify as required to allow the frame to be sent out.
PORT (n) - PACKET LEVEL RESTART	46000	Low	Normal	This message indicates that a packet-level restart sequence has been completed. All calls have been cleared and all PVC channels reset. The value *PORT (n)* indicates the port number.		This is an information message only. No corrective action is required.
PORT (n) - PORTSTATUS WARNING - *(cause)*	112017	Low	Warning	This alarm indicates that a node boot has been initiated and the specified port has been disabled. This message is generated as the port is initialized and warns that the port is in the disabled state. The value *PORT (n)* identifies the port number affected, while (cause) identifies the reason for this alarm.	112000	Correct the problem indicated in the alarm message.
PORT (n) - PORT ALREADY DISABLE	280008			This message indicates that you have already disabled the port. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT ALREADY ENABLE	280010	High	Normal	This message indicates that you have already enabled the port. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) - PORT BOOT COMPLETED	282000	Low	Normal	This message is displayed whenever a port boot is completed. The value *PORT (n)* identifies the port that has been booted.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	39000	High	Normal	This message is displayed when the port boot is completed. The value *PORT (n)* identifies the NULL port that has been booted.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	49000	High	Normal	The boot process has been completed in response to a Boot command to a port. The value *PORT (n)* indicates the port number.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	51000	High	Normal	This message indicates that the X.25 port has been successfully booted. The value *PORT (n)* identifies the port number.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	56000	High	Normal	This message indicates that the boot process has been completed in response to a Port Boot command. The value *PORT (n)* indicates the port number.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	57000	High	Normal	This message indicates that a port boot has been successfully completed. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT BOOT COMPLETE	69000	High	Normal	The boot process has been completed in response to a Boot command to a port. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	74000	High	Normal	This message indicates that the port boot process has been completed. The value *PORT (n)* indicates the port number affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	86000	High	Normal	This message indicates that a successful NCR BSC port boot has taken place. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	97000	High	Normal	This message indicates that an RS366 port boot operation has been successfully completed. The value *PORT (n)* identifies the number of the port that was booted.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	110000	High	Normal	The identified port has been reset, re-initialized, and is ready for use. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	112000	High	Normal	The identified port has been reset, re-initialized, and is ready for use. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) - PORT BOOT COMPLETE	125000	High	Normal	This message indicates that a port has been successfully booted. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	126000	High	Normal	This message indicates that a port boot has been successfully completed. The value *PORT (n)* identifies the port affected.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT BOOT COMPLETE	150000	High	Normal	This message is displayed whenever a port boot is completed. The value *PORT (n)* identifies the port that has been booted.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	186000	High	Normal	This message indicates that a port has been successfully booted. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	216000	High	Normal	This message is displayed whenever a port boot is completed. The value *PORT (n)* identifies the port that has been booted.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	228000	High	Normal	This message is displayed whenever a port boot is completed. The value *PORT (n)* identifies the port that has been booted.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	231000	High	Normal	This message indicates that a Port boot has finished. The value *PORT (n)* identifies the port number.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT BOOT COMPLETE	243000	High	Normal	This message is displayed whenever a port boot is completed. The value *PORT (n)* identifies the port that has been booted.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	245002	High	Normal	This message indicates that a Port boot has finished. The value *PORT (n)* identifies the port number.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT BOOT COMPLETE	250000	High	Normal	This message indicates that a Port boot has finished. The value *PORT (n)* identifies the port number.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT BOOT COMPLETE	268000	High	Normal	This message indicates that a port boot has been completed successfully. The value *PORT (n)* identifies the PPP port affected.		This message is for information only. No corrective actions are necessary.
PORT (n) - PORT BOOT COMPLETE	280005	High	Normal	This message indicates that a Voice port has successfully complete the boot operation. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT COMPLETE	308000	High	Normal	This message is displayed when a port boot is complete. The value *PORT (n)* indicates the port number affected.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT BOOT COMPLETE	318000	High	Normal	This message is displayed whenever an SPP port boot is completed. The value *PORT (n)* identifies the port that has been booted.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) - PORT BOOT COMPLETE	2000	High	Normal	This message is displayed whenever a port boot is completed. The value *PORT (n)* identifies the port that has been booted.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT FAILED	69013	High	Normal	This alarm indicates that a Port Boot command was sent but not acted upon correctly. A descriptive parameter string will also be present. The value *PORT (n)* identifies the port affected.		There are three possible causes for this error: • You may have exceeded the maximum number of ports. • A Node Boot may be necessary if a parameter requiring Node Boot has been changed. • The port may have been disabled, and must be re-enabled.
PORT (n) - PORT BOOT FAILED, CAUSE: *(cause)*	282001	High	Normal	This alarm indicates that a Port Boot command was sent but not acted upon correctly. The value *PORT (n)* identifies the port affected, while the value (cause) identifies why the port boot operation has failed.		There are three possible causes for this error: • You may have exceeded the maximum number of ports. • A Node Boot may be necessary if a parameter requiring Node Boot has been changed. • The port may have been disabled, and must be re-enabled.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT BOOT FAILURE	86001	High	Normal	This message indicates that an RS366 port boot has failed to take place. The value *PORT (n)* identifies the port affected.		To correct this problem: • Configure the NCRBSC port record if it does not exist. • Boot the node if port type has changed. • Boot the node if Data Port number was changed for that port. • Enable the port and then boot the port.
PORT (n) - PORT BOOT FAILURE	97001	High	Normal	This alarm indicates that an RS366 port boot operation has failed. The value *PORT (n)* identifies the port number affected.		To correct this problem: • Configure RS366 port record if does not exist. • Boot the node if port type was changed for that port number. • Boot the node if Data Port number was changed for that port. • Enable the port and then boot the port.
PORT (n) - PORT BOOT FAILURE	150001	High	Normal	This message indicates that a Frame Relay port failed to boot. The value *PORT (n)* identifies the port affected, while *(cause)* identifies the reason for the failure.		Correct the cause of this problem. A Node boot may be necessary to correct this problem.
PORT (n) - PORT BOOT FAILURE	231001	High	Normal	This message indicates that a Port boot has failed. The value *PORT (n)* identifies the port number affected.		Evaluate the *(cause)* string to determine why the port boot failed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT BOOT FAILURE	243001	High	Normal	This message is displayed whenever you attempt to disable a port that a is already disabled. The value *PORT (n)* indicates the port that has not been disabled.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT BOOT FAILURE *(cause)*	2001	High	Normal	This alarm is displayed whenever a port boot has failed. The value *PORT (n)* indicates the port that failed to boot, and the *(cause)* provides you with a brief description of what problems occurred.		Review the explanation given with this alarm and correct the situation as required before rebooting the port. **■ Note** Refer to the Vanguard Applications Ware Documentation Set for additional information.
PORT (n) - PORT BOOT FAILURE *(cause)*	49001	High	Normal	This message indicates that a Port Boot command was sent but not acted upon correctly. The value *PORT (n)* indicates the port number and *(cause)* describes the cause of the failure.		These conditions may exist. Verify their existence and correct as necessary: • You may have not licensed that many ports. • The maximum number of ports may have been exceeded. • You may have to perform a Node Boot if parameters requiring a Node Boot have been changed. • The Port may have been disabled; enable the port

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT BOOT FAILURE *(cause)*	51001	High	Normal	This alarm indicates that a Port Boot command was sent but not acted upon correctly. The value *PORT (n)* indicates the port number and *(cause)* describes the cause of the failure.		You may have more ports configured than you are licensed to use i.e., the maximum number of ports may have been exceeded. Perform a Node Boot if a parameter requiring a Node boot is changed, also, the port may have been disabled so enable the port.
PORT (n) - PORT BOOT FAILURE *(cause)*	74001	High	Normal	This alarm indicates that a boot command was sent to a specific port on your node but the boot process has failed. The value *PORT (n)* indicates the port that has failed to boot, while *(cause)* identifies the reason for boot failure.		There are two possible corrective actions that you can perform: • If the maximum number of ports has been incorrectly configured, you should perform a Node Boot for the changed Port Record parameter to take affect. • If the Port is disabled, enable it and reboot the port.
PORT (n) - PORT BOOT FAILURE - *(cause)*	19013	High	Critical	This alarm indicates that a port boot failed. The value *PORT (n)* indicates the port that failed to boot, and the *(cause)* provides you with a brief description of what problems occurred.		Review the explanation given with this alarm and correct the situation as required before rebooting the port. **■ Note** Refer to the Vanguard Applications Ware Documentation Set for additional information.

Alarm Text	**Trap No.**	**Priority**	**Severity**	**Description**	**Cleared By:**	**Corrective Action** *(continued)*
PORT (n) - PORT BOOT FAILURE - *(cause)*	56001	High	Normal	This message indicates that a Port Boot command was sent but not acted upon correctly. The value *PORT (n)* indicates the port number and *(cause)* describes the cause of the failure, as listed below: a) NO CONFIGURATION: No configuration is currently loaded. b) PORT TYPE CHANGED: The port type has been changed. c) PORT CONNECTION TYPE CHANGED: The port connection type has been changed. d) PORT DISABLED: The port is disabled.		Correct the problem causing this alarm by performing the procedure that corresponds to the *(cause)* of the alarm: a) Check the configurations b) Boot the node. c) Boot the node. d) This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) - PORT BOOT FAILURE - *(cause)*	57001	High	Normal	This alarm indicates that a port has failed to boot. The value *PORT (n)* identifies the port number affected and the *(cause)* will be as indicated below: a) NO CONFIGURATION: No configuration is currently loaded. b) PORT TYPE CHANGED: Port type was changed. c) # DEVICES HAS CHANGED: The number of device was changed. d) PORT DISABLED: The Port is disabled.		Correct the problem causing this alarm by performing the procedure that corresponds to the *(cause)* of the alarm: a) Check the configurations. b) Boot the node. c) Boot the node. d) This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT FAILURE - *(cause)*	110001	High	Normal	This alarm is displayed whenever a port boot has failed. The value *PORT (n)* indicates the port that failed to boot, and the *(cause)* provides you with a brief description of what problems occurred.		Resolve the conflicts identified in the alarm message to correct this problem.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT BOOT FAILURE - *(cause)*	112001	High	Normal	This alarm indicates that a user initiated port boot has failed. The value *PORT (n)* identifies the port number affected while *(cause)* indicates one of the following reasons for the failure: • There is no port record for the specified port. • You have attempted to boot a port type that is different than the port that you have specified. • The port that you attempted to boot is disabled. • The number of stations has been altered. • The DCP level has changed. • The number of MX25 PVCs or the starting PVC number has changed. • The number of MX25 SVCs of the starting SVC number has changed.		Resolve the conflicts identified in the alarm message to correct this problem.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT BOOT FAILURE - *(cause)*	125001	High	Normal	This alarm indicates that, for one of the following reasons, a port has failed to boot. The value *PORT (n)* identifies the port number affected, while *(cause)* indicates the reason for the failure. There can be several reasons: • No configuration in CMEM. • Port type was changed by the user. • User changed number of devices in the port record. • PAD type has changed (TPAD/HPAD). • Port is disabled.		If reason a) through d) occur, perform a Node boot, otherwise enable the port before attempting to boot it.
PORT (n) - PORT BOOT FAILURE - *(cause)*	126001	High	Normal	This alarm indicates that a port boot has failed. The value *PORT (n)* identifies the port affected, while *(cause)* identifies why the failure occurred, as listed below: a) Port Type has changed. b) No CMEM Record. c) Port is disabled. d) Tx Queue Size Has changed.		Depending on the displayed cause, perform one of the following: a) Check to see if the Port is disabled. b) Determine whether the Port type has changed before booting. c) Verify that the port record exists. d) Check if the Parameter “TX Queue Size value has been changed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT BOOT FAILURE - *(cause)*	186001	High	Normal	This message indicates that a Frame Relay port failed to boot. The value *PORT (n)* identifies the port affected, while *(cause)* identifies the reason for the failure.		Correct the cause of this problem. A Node boot may be necessary to correct this problem.
PORT (n) - PORT BOOT FAILURE - *(cause)*	228001	High	Warning	This message is displayed whenever a TNPP port fails to boot properly. The value *PORT (n)* identifies the TNPP port affected, while *(cause)* indicates that one of these reasons for the failure, has occurred: • No Port record available in CMEM • Port Type id changed • Port is disabled.		To correct this problem, reconfigure the port and then perform a Port Boot.
PORT (n) - PORT BOOT FAILURE - *(cause)*	245003	High	Normal	This message indicates that a Port boot has failed. The value *PORT (n)* identifies the port number while *(cause)* identifies the reason for the failure.		Evaluate the *(cause)* string to determine why the port boot failed.
PORT (n) - PORT BOOT FAILURE - (cause)	268001	High	Normal	This message indicates that a port could not be booted for the given reason. The value *PORT (n)* identifies the PPP port affected, while the value *(cause)* identifies the cause of the problem.		A node boot may be required to correct this problem.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT BOOT FAILURE - *(cause)*	280004	High	Normal	This alarm indicates that a Voice port has failed a port boot operation in the software initialization. The value *PORT (n)* identifies the port affected, while *(cause)* identifies one of these possible causes of this failure: • The selected Voice Coder is not present in FLASH. • The selected Voice Coder is not authorized.		To correct this problem: a) Change the voice port configuration to a Voice Coder that is present. b) Install the correct CSK. c) Check that the maximum number of voice ports configured for selected coder is not exceeded.
PORT (n) - PORT BOOT FAILURE - *(cause)*	308001	High	Normal	This alarm indicates that the port boot failed. The value *PORT (n)* indicates the port number affected while the *(cause)* string identifies the reason for the failure.		Review the explanation given with this alarm and correct the situation as required before rebooting the port **■ Note** Refer to the Vanguard Applications Ware Documentation Set for additional information.
PORT (n) - PORT BOOT FAILURE - *(cause)*	318001	High	Normal	This message indicates that an SPP port boot operation cannot be performed. The value *PORT (n)* indicates the port number while *(cause)* indicates the reason the failure occurred.		The reason for failure could be: • The port record is not configured in the CMEM • The port is not an SPP port. Reconfigure the port. • Parameters requiring a node boot have been altered, so a port boot will not suffice. Reconfigure the port. • The port is disabled. Enable the port.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT BOOT FAILURE - *(cause)*	216001	High	Normal	This message indicates a T3POS port failed to boot properly. The value *PORT (n)* identifies the T3POS port affected, while *(cause)* indicates that one of these reasons for the failure, has occurred: • No Port record available in CMEM • Port Type id changed • Port is disabled		To correct this problem, reconfigure the port and then perform a Port Boot.
PORT (n) - PORT BOOT FAILURE - *(cause)*	250001	High	Normal	This alarm indicates a port boot has failed. The value *PORT (n)* indicates the port that failed to boot, and the *(cause)* provides you with a brief description of what problems occurred.		Review the explanation given with this alarm and correct the situation as required before rebooting the port. **■ Note** Refer to the Vanguard Applications Ware Documentation Set for additional information.
PORT (n) - PORT BOOT FAILURE - (explanation)	39001	High	Normal	This message indicates the port boot has failed. The value *PORT (n)* identifies the NULL port that has been booted.		This is an information message only. No corrective action is required.
PORT (n) - PORT BUSY OUT	280007	High	Normal	This message indicates that a voice port has been BUSYOUT by the user. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT BUSY-OUT	74014	High	Warning	This message indicates that a port has been successfully busied-out via the Port/Station Control Menu.		This is an information message only. No corrective action is required.
PORT (n) - PORT BUSY-OUT	126008	High	Normal	This message indicates that a port has been busied out via the CTP. The value *PORT (n)* identifies the port affected.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT BUSY-OUT	308014	High	Warning	This message indicates that a port has been busied out from the CTP. The value *PORT (n)* indicates the port number affected.	308000	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT BUSY-OUT COMPLETE	69018	High	Normal	This message indicates that a port has been successfully busied-out via the Port/Station Control Menu. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT BUSY-OUT FAILURE *(cause)*	74015	High	Normal	This message indicates that an unsupported operation has been attempted. The value *PORT (n)* identifies the port affected while *(cause)* describes the cause of the failure.		This is an information message only. No corrective action is required.
PORT (n) - PORT BUSY-OUT FAILED	69016	High	Normal	This message indicates that a port could not be busied out because it was disabled or already busied out. The value *PORT (n)* identifies the port affected.		If the port is disabled, enable port first and then busy out port.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) - PORT CONNECTION CLEARED	228006	High	Normal	This message indicates that the rate of data transfer through this port has exceeded the per-port threshold in the node record. The value *PORT (n)* indicates the port affected.		Contact your customer service representative for additional information.
PORT (n) - PORT CONNECTION CLEARED	250006	Medium	Normal	This message indicates that the rate of data transfer through this port has exceeded the per-port threshold in the node record. The value *PORT (n)* indicates the port affected.		Contact your customer service representative for additional information.
PORT (n) - PORT DISABLE FAILURE *(cause)*	74003	High	Normal	This message indicates that you attempted to disable a port that a is already disabled. The value *PORT (n)* indicates the port that has not been disabled, while *(cause)* identifies the reason for the failure.		Refer to the appropriate Applications Ware Feature Protocols Documentation for explanations of the displayed cause code and correct as required.
PORT (n) - PORT DISABLE FAILURE - *(cause)*	308003	High	Normal	This message indicates a failure occurred while disabling a Port. The value *PORT (n)* indicates the port number affected while the *(cause)* string identifies the reason for the failure.		This alarm is typically displayed when the port has already been disabled.
PORT (n) - PORT DISABLE FAILED	69015	High	Normal	This message indicates that the port is already disabled. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT DISABLE FAILURE	97005	High	Normal	This message indicates that you have tried to disable a port that is already disabled. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT DISABLE FAILURE	112003	High	Normal	This alarm indicates that you have tried to disable a port that is already disabled. The value *PORT (n)* identifies the port number affected.		Do not try to disable a port that is already disabled.
PORT (n) - PORT DISABLE FAILURE	228003	High	Normal	This message indicates that you attempted to disable a port that a is already disabled. The value *PORT (n)* indicates the port that has not been disabled, while *(cause)* identifies the reason for the failure.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT DISABLE FAILURE	250003	High	Normal	This message indicates that you attempted to disable a port that a is already disabled. The value *PORT (n)* indicates the port that has not been disabled.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT DISABLE FAILURE	318003	High	Normal	This message indicates that an SPP port could not be disabled because it is already disabled. The value *PORT (n)* indicates the port number.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) - PORT DISABLE FAILURE	216003	High	Normal	This message indicates that you attempted to disable a port that a is already disabled. The value *PORT (n)* indicates the port that has not been disabled, while *(cause)* identifies the reason for the failure.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT DISABLED	39002	High	Warning	This message indicates that a port has been disabled. The value *PORT (n)* identifies the disabled NULL port number.	39003	This is an information message only. No corrective action is required.
PORT (n) - PORT DISABLED	49002	High	Warning	This message indicates that the port has been disabled by a CTP command. The value *PORT (n)* indicates the port number.	49003	This is an information message only. No corrective action is required.
PORT (n) - PORT DISABLED	56002	High	Warning	This message indicates that a Port is now disabled. The value *PORT (n)* indicates the port number.	56003	This is an information message only. No corrective action is required.
PORT (n) - PORT DISABLED	57002	High	Warning	This message indicates that a port has now been disable. The value *PORT (n)* identifies the port number affected.	57003	This is an information message only. No corrective action is required.
PORT (n) - PORT DISABLED	74002	High	Warning	This message indicates that the port was successfully disabled. The value *PORT (n)* indicates the port that has been disabled.	74004	This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT DISABLED	86002	High	Warning	This alarm indicates that a response to either a port boot or port disable command has occurred. The value *PORT (n)* identifies the port affected.	86003	Enable the port and then perform a port boot to correct this problem. There are no corrective actions required when this alarm is the result of a port already being disabled.
PORT (n) - PORT DISABLED	97002	High	Warning	This alarm indicates that a port boot, or port disable operation, has failed. The value *PORT (n)* identifies the port number disabled.	97003	To correct this problem, enable the port and then boot the port **Note** No action is required if the operation was "port disable".
PORT (n) - PORT DISABLED	110002	High	Warning	This message indicates that you have tried to disable a port that is already disabled. The value *PORT (n)* identifies the port number affected.	110003	This is an information message only. No corrective action is required
PORT (n) - PORT DISABLED	112002	High	Warning	This message indicates that you have tried to disable a port that is already disabled. The value *PORT (n)* identifies the port number affected.	112004	This is an information message only. No corrective action is required.
PORT (n) - PORT DISABLED	125002	High	Warning	This message indicates that a port has been disabled. The value *PORT (n)* identifies the port number affected	125003	This is an information message only. No corrective action is required.
PORT (n) - PORT DISABLED	126002	High	Warning	This message indicates that port specified has been disabled via the CTP. The value *PORT (n)* identifies the port affected.	126004	This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT DISABLED	150002	High	Warning	This message indicates that a Frame Relay port has been disabled by a user. The value *PORT (n)* identifies the port affected.	150002	This is an information message only. No corrective action is required.
PORT (n) - PORT DISABLED	186002	High	Warning	This message indicates that a FRA port has been disabled by a user. The value *PORT (n)* identifies the port affected.	186002	This is an information message only. No corrective action is required.
PORT (n) - PORT DISABLED	216002	High	Warning	This message indicates that a Port has been successfully disabled. The value *PORT (n)* identifies the disabled port.	216004	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT DISABLED	228002	High	Normal	This message indicates that a Port has been successfully disabled. The value *PORT (n)* identifies the disabled port.	228004	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT DISABLED	243002	High	Warning	This message indicates that a Port has been successfully disabled. The value *PORT (n)* identifies the disabled port.	243003	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT DISABLED	245005	High	Warning	This message indicates that a port is disabled. The value *PORT (n)* identifies the port number.	245010	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT DISABLED	250002	High	Warning	This message indicates that a Port has been successfully disabled. The value *PORT (n)* identifies the disabled port.	250000	This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT DISABLED	268002	High	Warning	This message indicates that a PPP port has been disabled under operator control. The value *PORT (n)* identifies the PPP port affected.	268003	This message is for information only. No corrective actions are necessary.
PORT (n) - PORT DISABLED	280006	High	Warning	This message indicates that either a voice port has been disabled, or the associated T1E1 port has been disabled. The value *PORT (n)* identifies the port affected.	280009	This is an information message only. No corrective action is required.
PORT (n) - PORT DISABLED	282002	Low	Warning	This message indicates that a Port has been successfully disabled. The value *PORT (n)* identifies the disabled port.	282003	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT DISABLED	308002	High	Warning	This message is displayed when the Port is disabled. The value *PORT (n)* indicates the port number affected.	308004	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT DISABLED	318002	High	Warning	This message indicates that an SPP port has been success fully disabled. The value *PORT (n)* indicates the port number.	318004	This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLE FAILED	69014	High	Normal	This message indicates that the port is already enabled. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLE FAILED	86004	High	Normal	This message indicates that the response to a port Enable operation. The value *PORT (n)* identifies the port affected.		No action required, port is already enabled.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT ENABLE FAILED	110004	High	Normal	This message indicates that you have attempted to enable a port that is already enabled. The value *PORT (n)* identifies the port number affected.		Don't try to enable a port that is already enabled.
PORT (n) - PORT ENABLE FAILED	125004	High	Normal	This message indicates that a port could not be enabled because it has already been enabled. The value *PORT (n)* identifies the port number affected		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLE FAILED	150004	High	Normal	This message indicates that the port is already in the enabled state. The value *PORT (n)* indicates the port that has been booted.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLE FAILED - ALREADY ENABLED	56004	High	Normal	This message indicates that a port is already enabled. The value *PORT (n)* indicates the port number.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLE FAILED - ALREADY ENABLED	57004	High	Normal	This message indicates that a port is already enabled. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLE FAILURE	97004	High	Normal	This message indicates that you have tried to enable a port that is already enabled. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT ENABLE FAILURE	112005	High	Normal	This message indicates that you have attempted to enable a port that is already enabled. The value *PORT (n)* identifies the port number affected.		Don't try to enable a port that is already enabled.
PORT (n) - PORT ENABLE FAILURE	228005	High	Normal	This message indicates that the port is already in the enabled state. The value *PORT (n)* indicates the port that has been booted.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLE FAILURE	250005	High	Normal	This message indicates that the port is already in the enabled state. The value *PORT (n)* indicates the port that has been booted.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLE FAILURE	318005	High	Normal	This message indicates that an SPP port could not be enabled because it is already enabled. The value *PORT (n)* indicates the port number.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLE FAILURE	216005	High	Normal	This message indicates that the port is already in the enabled state. The value *PORT (n)* indicates the port that has been booted.	216004	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLE FAILURE *(cause)*	74005	High	Normal	This message indicates that the port is already in the enabled state. The value *PORT (n)* indicates the port affected.		Refer to the appropriate Applications Ware Feature Protocols Documentation for explanations of the displayed cause code and correct as required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT ENABLE FAILURE *(cause)*	306005	High	Normal	This message indicates that the port is already in the enabled state. The value *PORT (n)* indicates the port that has been booted, while *(cause)* identifies the reason for the failure.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLE FAILURE - *(cause)*	308005	High	Normal	This message indicates that a failure occurred while enabling a Port. The value *PORT (n)* indicates the port number affected while the *(cause)* string identifies the reason for the failure.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLED	39003	High	Normal	This message indicates that a port has been enabled. The value *PORT (n)* identifies the enabled NULL port number.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLED	49003	High	Normal	This message indicates that the port has been enabled by a CTP command. The value *PORT (n)* indicates the port number.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLED	56003	High	Normal	This message indicates that a Port is now enabled. The value *PORT (n)* indicates the port number.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLED	57003	High	Normal	This message indicates that a port has now been enabled. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLED	74004	High	Normal	This message indicates that the port has been enabled. The value *PORT (n)* indicates the port affected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT ENABLED	86003	High	Normal	This message indicates the response to a port Enable operation. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLED	97003	High	Normal	This message indicates that a port has been enabled. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLED	110003	High	Normal	This message indicates that a port has been enabled. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLED	112004	High	Normal	This message indicates that a port has been enabled. The value *PORT (n)* identifies the port number affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLED	125003	High	Normal	This message indicates that a port has been enabled. The value *PORT (n)* identifies the port number affected		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLED	126004	High	Normal	This message indicates that the specified has been enabled. The value *PORT (n)* identifies the port affected.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLED	150003	High	Normal	This message indicates that a Frame Relay port has been enabled by a user. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT ENABLED	186003	High	Normal	This message indicates that a FRA port has been enabled by a user. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLED	216004	High	Normal	This message indicates that a port has been successfully enabled. The value *PORT (n)* indicates the port that has been booted.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLED	228004	High	Normal	This message indicates a port has been successfully enabled. The value *PORT (n)* indicates the port that has been booted.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLED	231002	High	Warning	This message indicates a port has been successfully enabled. The value *PORT (n)* indicates the port that has been booted.	231003	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLED	243003	High	Normal	This message indicates a port has been successfully enabled. The value *PORT (n)* indicates the port that has been booted.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLED	245010	High	Normal	This message indicates a port has been successfully enabled. The value *PORT (n)* indicates the port that has been booted.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLED	250004	High	Normal	This message indicates a port has been successfully enabled. The value *PORT (n)* indicates the port that has been booted.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT ENABLED	268003	High	Normal	This message indicates that a PPP port has been enabled under operator control. The value *PORT (n)* identifies the PPP port affected.		This message is for information only. No corrective actions are necessary.
PORT (n) - PORT ENABLED	280009	High	Normal	This message indicates that a voice port has been enabled; most probably by a user on the network. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLED	282003	Low	Normal	This message indicates a port has been successfully enabled. The value *PORT (n)* indicates the port that has been booted.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLED	291003	High	Normal	This message indicates a port has been successfully enabled. The value *PORT (n)* indicates the port that has been booted.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLED	300002	High	Normal	This message indicates that someone has enabled a port via the CTP port. The value *PORT (n)* indicates the port affected.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLED	306004	High	Normal	This message indicates a port has been successfully enabled. The value *PORT (n)* indicates the port that has been booted.		This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT ENABLED	308004	High	Normal	This message indicates a Port is enabled. The value *PORT (n)* indicates the port number affected.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT ENABLED	318004	High	Normal	This message indicates that an SPP port has been success fully enabled. The value *PORT (n)* indicates the port number.		This is an information message only. No corrective action is required.
PORT (n) - PORT ERROR COUNT > THRESHOLD	17001	Medium	Warning	This alarm indicates that the number of received errors (for example, overrun, or CRC) have exceeded the configured threshold. The value *PORT (n)* indicates the port number in question. **■Note** This alarm is generated by a Siemens SDLC or HDLC port.		Check your cables and cable lengths to ensure they are within specifications. If the cables are OK, check the transmission media for line quality.
PORT (n) - PORT ERROR COUNT > THRESHOLD	49005	Medium	Warning	This alarm indicates that the number of received errors (for example, overrun, or CRC) have exceeded the configured threshold. The value *PORT (n)* indicates the port number.	49000	Check your cables and cable lengths to ensure they are within specifications. If the cables are OK, check the transmission media for line quality.
PORT (n) - PORT ERROR COUNT > THRESHOLD	61000	Medium	Warning	This message indicates that the number of received errors, CRC for example, has exceeded the configured threshold. The value *PORT (n)* identifies the port affected.		Check your cables and cable lengths to ensure they are within specifications. If the cables are OK, check the transmission media for line quality.
PORT (n) - PORT ERROR COUNT > THRESHOLD	69007	Medium	Warning	This message indicates that the number of received errors, CRC for example, has exceeded the configured threshold. The value *PORT (n)* identifies the port affected.	69000	Check your cables and cable lengths to ensure they are within specifications. If the cables are OK, check the transmission media for line quality.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT ERROR COUNT > THRESHOLD	74013	Medium	Warning	This message indicates the total number of data errors (reception or transmission) on a port. This value has exceeded the Port Error Threshold parameter. The value *PORT (n)* identifies the port affected. **■Note** This alarm is generated by the Siemens SDLC protocol or an HDLC port.	74000	Complete this procedure to correct this alarm condition. • Check the Detailed Port Statistics screen for the SDLC port. • Note errors reported under the Physical Summary section. • Investigate potential causes of poor transmission line quality.
PORT (n) - PORT ERROR COUNT > THRESHOLD	108000	Medium	Warning	This alarm indicates that the combined number of CRC, parity, and overrun errors has exceeded a threshold value. The threshold value is configured as part of the Node record. The value *PORT (n)* identifies the port number.		Check the link status to correct this problem.
PORT (n) - PORT ERROR COUNT > THRESHOLD	109000	Medium	Warning	This alarm indicates that the combined number of CRC, parity, and overrun errors has exceeded a threshold value. The threshold value is configured as part of the Node record. The value *PORT (n)* identifies the port number.		Check the link status to correct this problem.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT ERROR COUNT > THRESHOLD	219006	Medium	Warning	This message indicates that the total number of data errors (reception or transmission) on a port has exceeded the configured value of the Port Error Threshold parameter. The value *PORT (n)* identifies the port affected.	219000	Complete this procedure to correct this alarm condition. • Check the Detailed Port Statistics screen for the ATPAD port. • Note errors reported under the Physical Summary section. • Investigate potential causes of poor transmission line quality.
PORT (n) - PORT ERROR COUNT > THRESHOLD	231006	Medium	Warning	This message indicates that the total error count (equal to overrun errors plus underrun errors) is greater than that configured for the "Node Error Threshold" parameter. The value *PORT (n)* indicates the port affected.	231000	This is most likely the result of a problem with you node hardware. Have this hardware serviced when convenient. **■ Note** There are no software related corrective actions applicable.
PORT (n) - PORT ERROR COUNT > THRESHOLD	261000	Medium	Warning	This alarm indicates that the combined number of CRC, parity, and overrun errors has exceeded a threshold value. The threshold value is configured as part of the Node record. The value *PORT (n)* identifies the port number.		Check the link status to correct this problem.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) - PORT ERROR COUNT > THRESHOLD	268006	Medium	Warning	This message indicates that the number of frames received in error has exceeded the threshold configured in the Node Record. The value *PORT (n)* identifies the PPP port affected.	268000	To correct this problem: • Monitor the link for the possibility of excessive bit error rates. • Check for proper clocking configuration • Verify that connections are sound and cables are within specified length.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) - PORT INIT FAILURE - *(cause)*	280002	High	Critical	This alarm indicates a failure in the software initialization. The value *PORT (n)* identifies the port affected, while *(cause)* identifies one of these possible causes of this failure: • Invalid port number. • A Voice port has been configured for H323 and the H323 software has not been installed. • The T1/E1 Daughtercard is not installed or operating correctly. • The configured Interface Type does not match the installed daughtercard. • A different E&M Signaling Type has been configured for ports associated with the same E&M card. • The voice coder is not present in FLASH memory or the correct CSK has not been installed.		Check the configuration, the version of installed software, and the hardware on which the software is installed.
PORT (n) - PORT INIT FAILURE, CAUSE: *(cause)*	282004	High	Critical	This alarm indicates a failure in the software initialization. The value *PORT (n)* identifies the port affected, while *(cause)* identifies possible causes of this failure.		Check the configuration, the version of installed software, and the hardware on which the software is installed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT NOT STARTED - *(cause)*	280003	High	Critical	This alarm indicates that a Voice port has not started. re in the software initialization. The value *PORT (n)* identifies the port affected, while *(cause)* identifies one of these possible causes of this failure: • The voice port is DISABLE. • The associated T1/E1 port is DISABLE.		To correct this problem, reconfigure the Voice Port and the T1E1 ports to ENABLE.
PORT (n) - PORT STAT OVERFLow	112015	High	Warning	This alarm indicates a statistic parameter has looped over the maximum counter value and started over from zero. The value *PORT (n)* identifies the port number affected.	112000	This is an information message only. No corrective action is required.
PORT (n) - PORT STAT OVERFLow	215021	Medium	Warning	This message indicates that the counter number has reached its maximum limit. The counter is reset to 0.		This is an information message only. No corrective action is required.
PORT (n) - PORT STATUS WARNING - PORT DISABLED	56008	Low	Warning	This message indicates that the port is disabled. The value *PORT (n)* indicates the port number.	56000	This is an information message only. No corrective action is required.
PORT (n) - PORT STATUS WARNING - *(cause)*	291005	Low	Warning	This alarm indicates when, during a node boot, that the port is disabled. The value *PORT (n)* indicates the port affected while *(cause)* identifies the reason for the alarm itself.	291000	To correct this situation, enable the port.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) - PORT STATUS WARNING - *(cause)*	69019	Low	Warning	This alarm indicates, during a node boot, when the port is disabled. The value *PORT (n)* indicates the port affected while *(cause)* identifies the reason for the warning itself.		To correct this situation, enable the port.
PORT (n) - PORT STATUS WARNING - PORT DISABLED	57011	Low	Warning	This message indicates that a port is disabled. The value *PORT (n)* identifies the port affected.	57000	This is an information message only. No corrective action is required.
PORT (n) - PORT STATUS WARNING, PORT DISABLED	300004	Medium	Warning	This message indicates that you have tried to disable a port that is already disabled. The value *PORT (n)* indicates the port affected.	300000	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT STATUS WARNING *(cause)*	74018	Low	Warning	This alarm indicates, during a node boot, when the port is disabled. The value *PORT (n)* indicates the port affected while *(cause)* identifies the reason for the warning itself.	74000	To correct this situation, enable the port.
PORT (n) - PORT STATUS WARNING *(cause)*	306006	High	Warning	This alarm indicates that the port is disabled. The value *PORT (n)* indicates the port affected while *(cause)* identifies the reason for the warning itself.	306000	To correct this situation, enable the port.
PORT (n) - PORT STATUS WARNING - *(cause)*	49006	Low	Warning	This message indicates that a Port status warning occurred due to a specified cause. The value *PORT (n)* indicates the port number and *(cause)* describes the cause of the failure.	49000	Take action as specified by the *(cause)*.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT STATUS WARNING - *(cause)*	245006	Low	Warning	This warning message is displayed during port initialization. The value *PORT (n)* identifies the port number while *(cause)* identifies the reason for the failure.	245002	Evaluate the string to determine what the problem is.
PORT (n) - PORT STATUS WARNING - *(cause)*	308018	Low		This message indicates that there is an error in initializing the node. The value *PORT (n)* indicates the port number affected while the *(cause)* string identifies the reason for the warning.	308000	Determine reason for failure via explanation. Correct the problem and then reboot the port.
PORT (n) - PORT STATUS WARNING - PORT DISABLED	219005	Low	Warning	This alarm indicates that the status of a port has changed from enabled to disabled. The value *PORT (n)* identifies the disabled port.	219000	Enable the port via the CTP port.
PORT (n) - PORT STATUS WARNING -*(cause)*	126010	Low	Warning	This message indicates that a port (running over T1/E1) has been momentarily disabled. The value *PORT (n)* indicates the port affected while *(cause)* identifies what caused the message to be displayed. **■Note** The possible cause of this alarm is that a T1/E1 card is waiting to come out of an alarm state.	126000	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT STATUS WARNING	228008	Low	Warning	This alarm indicates that, during a node boot, the port was disabled. The value *PORT (n)* indicates the port affected.	228000	To correct this situation, enable the port.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT STATUS WARNING	231005	Low	Warning	This alarm indicates that, during a node boot, the port was disabled. The value *PORT (n)* indicates the port affected.	231000	To correct this situation, enable the port.
PORT (n) - PORT STATUS WARNING	250008	Low	Warning	This message indicates that a port was already disabled at node boot time. The value *PORT (n)* identifies the PPP port affected.	250000	This message is for information only. No corrective actions are necessary.
PORT (n) - PORT STATUS WARNING	268005	Low	Warning	This message indicates that a PPP port was already disabled at node boot time, or has been temporarily disabled while awaiting availability of the PRI interface with which it is associated. The value *PORT (n)* identifies the PPP port affected.	268000	This message is for information only. No corrective actions are necessary.
PORT (n) - PORT STATUS WARNING	186009	Low	Warning	This message indicates that a port was already disabled when the node was booted. The value *PORT (n)* identifies the port affected.	186000	This is an information message only. No corrective action is required.
PORT (n) - PORT STATUS WARNING	243004	Low	Warning	This warning message is displayed during port initialization. The value *PORT (n)* identifies the port number.	243000	Evaluate the string to determine what the problem is.
PORT (n) - PORT STATUS WARNING	318011	High	Warning	This message indicates that the SPP port was in disabled state when the node initialized. The value *PORT (n)* indicates the port number.	318000	Enable the port if it is to be used.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT UTILIZATION > THRESHOLD	17000	Medium	Warning	This alarm indicates that port utilization has exceeded the value configured for the Port Utilization Threshold parameter. The value *PORT (n)* identifies the port in question.		To correct this problem: a) Reduce the device speed. b) Reduce the number of devices that are connected to the port. c) Increase the port speed.
PORT (n) - PORT UTILIZATION > THRESHOLD	49004	Medium	Warning	This message indicates that port utilization has exceeded the configured threshold. Generated if the port utilization reaches the threshold defined in the node record. The value *PORT (n)* indicates the port number.	49000	This is an information message only. No corrective action is required.
PORT (n) - PORT UTILIZATION > THRESHOLD	56007	Medium	Warning	This message indicates that port utilization has exceeded the configured threshold. Generated if the port utilization reaches the threshold defined in the node record. The value *PORT (n)* indicates the port number.	56000	This is an information message only. No corrective action is required.
PORT (n) - PORT UTILIZATION > THRESHOLD	69006	Medium	Warning	This message indicates that the port utilization value has exceeded the threshold value stored in the node record. The value *PORT (n)* identifies the port affected.	69000	Adjust the threshold value in the node record or reduce the traffic on the port if possible
PORT (n) - PORT UTILIZATION > THRESHOLD	74012	Medium	Warning	This message indicates that the utilization of a Port has exceeded the limit configured for the Port Utilization Threshold parameter. The value *PORT (n)* identifies the port affected.	74000	Either off-load some of the traffic from this port or increase the line speed. Consider increasing the configured value of the “Port Utilization Threshold” if it is set unreasonably low.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT UTILIZATION > THRESHOLD	112012	Medium	Warning	This alarm indicates that the port utilization is greater than the value configured for the Maximum Port Utilization parameter in the node configuration record. The value *PORT (n)* identifies the port affected.	112000	There are two possible solutions to this problem: a) Reduce port traffic levels. b) Adjust the threshold parameter in the node record.
PORT (n) - PORT UTILIZATION > THRESHOLD	126006	High	Warning	This message indicates that Port Utilization exceeds the configured Port Utilization value in the Node record. The value *PORT (n)* identifies the port affected.	126000	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT UTILIZATION > THRESHOLD	186004	Medium	Warning	This message indicates that the link utilization is consistently over the threshold configured in the Node Record.		This is an information message only. No corrective action is required.
PORT (n) - PORT UTILIZATION > THRESHOLD	216007	High	Warning	This message indicates that the utilization of a Port has exceeded the limit configured for the Port Utilization Threshold parameter. The value *PORT (n)* identifies the port affected.	216000	Either off-load some of the traffic from this port or increase the line speed. Consider increasing the configured value of the “Port Utilization Threshold” if it is set unreasonably low.
PORT (n) - PORT UTILIZATION > THRESHOLD	219004	Medium	Warning	This message indicates that the utilization of a Port has exceeded the limit configured for the “Port Utilization Threshold” parameter. The value *PORT (n)* identifies the port affected.	219000	Either off-load some of the traffic from this port or increase the line speed. Consider increasing the configured value of the “Port Utilization Threshold” if it is set unreasonably low.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT UTILIZATION > THRESHOLD	228007	High	Warning	This message indicates that the rate of data transfer through this port has exceeded the per-port threshold in the node record. The value *PORT (n)* indicates the port affected.	228000	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT UTILIZATION > THRESHOLD	231003	High	Normal	This message indicates that the rate of data transfer through this port has exceeded the per-port threshold in the node record. The value *PORT (n)* indicates the port affected.	245002	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT UTILIZATION > THRESHOLD	245007	Medium	Warning	This message indicates that the rate of data transfer through this port has exceeded the per-port threshold in the node record. The value *PORT (n)* indicates the port affected.	245002	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT UTILIZATION > THRESHOLD	250007	Medium	Warning	This message indicates that the PPP link utilization has persisted above the threshold configured in the Node Record. The value *PORT (n)* identifies the PPP port affected.	250000	This message is for information only. No corrective actions are necessary.
PORT (n) - PORT UTILIZATION > THRESHOLD	268004	Medium	Warning	This message indicates that the PPP link utilization has persisted above the threshold configured in the Node Record. The value *PORT (n)* identifies the PPP port affected.	268000	This message is for information only. No corrective actions are necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - PORT UTILIZATION > THRESHOLD	291004	Medium	Warning	This message indicates that the current receive/transmit utilization of available bandwidth exceeds 60% of its capacity. The value *PORT (n)* indicates the port affected.	291000	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT UTILIZATION > THRESHOLD	308012	Medium	Warning	This message indicates that port utilization is greater than the threshold. The value *PORT (n)* indicates the port number affected.	308000	This is an information message only. There are no corrective actions necessary.
PORT (n) - PORT UTILIZATION > THRESHOLD	318010	Medium	Warning	This message indicates that the rate of data transfer through this port has exceeded the per-port threshold in the node record. The value *PORT (n)* indicates the port number.		If the station has not been initialized, verify the station number to be enabled.
PORT (n) - REJECTING X25 CALL, ALREADY CONNECTED	227011	Low	Minor	This report indicates that a call, from the remote TNPP PAD, has been received while an earlier call has not yet been cleared. The value *PORT (n)* identifies the port affected.		To correct this problem, reboot the port.
PORT (n) - REMOTE DEVICE IS DOWN	227006	High	Major	This alarm indicates that the remote device is not responding. The value *PORT (n)* identifies the port affected.		To correct this problem, check the remote TNPP device configuration.
PORT (n) - REMOTE DEVICE IS UP	227010	Medium	Normal	This message indicates that the remote TNPP device is up and responding. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - REMOTE PAD IS NOT TNPP PAD, CLEARING CALL	227013	High	Minor	This alarm indicates that an X.25 call has been cleared because it was connected to a non-TNPP PAD. The value *PORT (n)* identifies the port affected.		To correct this problem: a) Check the mnemonic. b) Check the Routing Table.
PORT (n) - RETRY EXCEEDED, CALL CLEARED	215016	Medium	Minor	This alarm indicates that the frame transmitted towards the POS terminal is retried for the configured retry limit. A response to this frame is not received from the POS terminal. In the case of a SIMP connection, the call is disconnected and cleared. The value *PORT (n)* identifies the port number affected.		Verify that the POS terminal is operating properly. **■ Note** Refer to the T3POS manual in the *Vanguard Serial Features Protocol Manual* (Part Number T0102) for additional information.
PORT (n) - RETRY EXCEEDED, LINE DISCONNECTED	215015	Medium	Minor	This alarm indicates that the frame transmitted towards the POS terminal is retried for the configured retry limit. A response to this frame is not received from the POS terminal. In the case of a DIMO connection, the dial-up line is disconnected and the X.25 call towards the host is cleared. The value *PORT (n)* identifies the port number affected.		Verify that the POS terminal is operating properly. **■ Note** Refer to the T3POS manual in the *Vanguard Serial Features Protocol Manual* (Part Number T0102) for additional information.
PORT (n) - RING NUMBER CONFIGURATION ERROR	139005	High		This alarm indicates that the ring number configured in your node is different from the established ring number. The value *PORT (n)* identifies the Token Ring port number affected.		To correct this problem: a) Reconfigure the Ring Number parameter. b) Boot the node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - TERM *(ID)* STPA FRAME DROPPED	44007	Low	Warning	This alarm indicates that a PAD port configured for STPA Host (profile par 114) and the response is received from the remote terminal (with a Terminal ID other than the polled ID). This alarm could also indicate that a response is received after the STPA poll time-out (profile par 120). The value *PORT (n)* indicates the port number while *(ID)* indicates the terminal ID.		Possible causes of this problem are: • Terminal responding is sending the wrong ID in the message. • The X.25 link towards the remote terminal is congested which is causing the delay.
PORT (n) - UNSUPPORTED FRAME SIZE: OPERATING WITH 1024 BYTES	112018	Medium	Minor	This message indicates that a port is booted, and the maximum configured frame size is 4K while the port driver (hardware) only supports 1K frame size. The value *PORT (n)* identifies the port ID.	112000	To correct this problem: • Change to a hardware platform that supports larger frame sizes. • Reconfigure the port and attached devices to use 1024 frame size.
PORT (n) - VIRTUAL CALL RETRY EXCEEDED, LINE DISCONNECTED	215018	Medium	Minor	This alarm indicates that an X.25call establishment towards the host has failed and it exceeded the configured retry limits. This alarm is generated when the connection type configured in the port record as DIMO. The value *PORT (n)* identifies the port number affected.		Perform these checks to find the cause of this problem and correct as necessary: • Check the X.25 connection. • Check the remote X.25 address. **■ Note** Refer to the *X.25 Basics Manual* in the *Vanguard Applications Ware Basic Protocols Manual* (Part Number T0106) for more information.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - VIRTUAL RETRY EXCEEDED, CALL CLEARED	215017	Medium	Minor	This alarm indicates that an X.25 call establishment, towards the host, has failed and it exceeded the configured retry limits. The value *PORT (n)* identifies the port number affected.		Perform these checks to find the cause of this problem and correct as necessary: • Check the X.25 connection. • Check the remote X.25 address. **Note** Refer to the *X.25 Basics Manual* in the *Vanguard Applications Ware Basic Protocols Manual* (Part Number T0106) for more information.
PORT (n) - X.28 SERVICE MESSAGE LOST	44005	Low	Minor	This alarm indicates that the X.28 message queue is full. The value *PORT (n)* indicates the port number.		Check if the Async connection between PAD port and the terminal is flow-controlled.
PORT (n) - X25 CONNECTION IS UP	227014	Medium	Normal	This report indicates that an X.25 link, between two TNPP PADs, is up.The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
PORT (n) BOOT FAILURE - *(cause)*	129001	High	Warning	This message indicates that a Port boot has failed. The value *PORT (n)* identifies the port affected while the *(cause)* is displayed at the end of the message.		Perform these actions until the port boots successfully: • Check if Port is disabled • Check if the Port type was changed before booting • Check to see if the port record exists or not. If it does not, create the required record.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) CPU - HA Communications Failure *(condition)*	141000	Low - for the 7300. Medium - all other platforms	Critical	This alarm indicates that the hardware accelerator is unable to communicate with the driver. The value *PORT (n)* identifies the port number, while *(condition)* indicates one of these events has taken place: • SET - Identifies when the failure occurred. • RST - Identifies when an attempt to restart the hardware is made. • CLR - Identifies when the failure condition has been cleared.		This problem is indicative of LAN card hardware failure; replace the LAN card.
PORT (n) DATA LOST FROM COMMAND QUEUE	218001	High	Major	This alarm indicates that the ATPAD could not transmit echoed commands or responses to commands. This is a result of the transmitting device's data queue having overflowed. The value *PORT (n)* identifies the ATPAD Port affected.	216000	Check that the ATPAD port has not been flow controlled by the terminal it is connected to. **■ Note** Refer to the *Configuring for APAD/ATPAD Manual* (Part Number T0110) for additional information.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) DATA LOST FROM DATA QUEUE	218000	High	Major	This alarm indicates that the ATPAD could not transmit data originally sent by a remote application. This is a result of the transmitting device's data queue having overflowed. The value *PORT (n)* identifies the ATPAD Port affected.	216000	If the ATPAD port has a data rate which is slower than the rate at which data is been sent by the remote application, data will back up in the ATPAD port's transmit queue. This could eventually lead to an overflow condition and loss of data. To prevent this from happening, it may be necessary to flow control the remote application. **■ Note** Refer to the *Configuring for APAD/ATPAD Manual* (Part Number T0110) for additional information.
PORT (n) FRAME RECEIVED FROM UNKNOWN DLCI: *(n)*	87000	Medium	Warning	This alarm indicates that a frame has been received from the link on a DLCI not associated with any FRI station or PVC management circuit. The value *PORT (n)* identifies the port number and the DLCI is given by *(n)*.		Check the DLCI numbers configured at both ends of the link.
PORT (n) FRAME RECEIVED INVALID ADDRESS *(dddd)*	87014	Medium	Warning	This alarm indicates that a frame with an unsupported address format (not 10 bit) has been received. The value *PORT (n)* identifies the port affected and the address value received in the frame is given by *(dddd)*.		Arrange for the network DLCI addressing to be in 10-bit format.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) FRAME RECEIVED INVALID ADDRESS *(dddd)*	187006	Medium	Warning	This alarm indicates that a frame with an unsupported address format (not 10 bit) has been received. The value *PORT (n)* identifies the port affected and the address value received in the frame is given by *(dddd)*.		Arrange for the network DLCI addressing to be in 10-bit format.
PORT (n) HA Warning:	141001	Low	Warning	This alarm indicates that the hardware accelerator tables are out of sync with the driver tables. The value *PORT (n)* identifies the port number.		Contact your customer service representative if this message is displayed.
PORT (n) LINE DOWN	177000	High	Major	This alarm indicates that all devices, on the HPAD side, are down, or that a poll was not received on the TPAD side. The value *PORT (n)* identifies the ALC port affected.	177001	To correct this problem: • Verify that the device addresses are correct. • Check power connections to the device.
PORT (n) LINE UP	177001	High	Normal	This message indicates that an ALC port is operational. The value *PORT (n)* identifies the ALC port affected.		This is an information message only. No corrective action is required.
PORT (n) LINK DOWN	87016	High	Major	This alarm indicates that the PVC management protocol has detected loss of the data link. The value *PORT (n)* identifies the port affected		To correct this problem: • Check connectors and cables. • Check the network status.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) LINK DOWN	187009	High	Major	This alarm indicates that the PVC management protocol has detected loss of the data link. The value *PORT (n)* identifies the port affected	187008	To correct this problem: a) Check connectors and cables. b) Check the network status.
PORT (n) LINK UP	87015	High	Normal	This alarm indicates that the PVC management protocol has established the data link. The value *PORT (n)* identifies the port affected		This is an information message only. No corrective action is required.
PORT (n) LINK UP	187008	High	Normal	This alarm indicates that the PVC management protocol has established the data link. The value *PORT (n)* identifies the port affected		This is an information message only. No corrective action is required.
PORT (n) PORT BOOT COMPLETE	88000	High	Normal	This message indicates that a FRI port boot has completed successfully. The value *PORT (n)* identifies the port affected.		This messages for information purposes only. No corrective actions are required.
PORT (n) PORT BOOT COMPLETE	139000	High	Normal	This message is for information purposes only and is displayed whenever a port boot is completed. The value *PORT (n)* identifies the port that has been booted.		This is an information message only. No corrective action is required.
PORT (n) PORT BOOT COMPLETE	193000	High	Normal	This message indicates that a port boot is completed. The value *PORT (n)* identifies the port number.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) PORT BOOT COMPLETE	196000	High	Normal	This message indicates that the port boot process has been completed. The value *PORT (n)* indicates the port number.		This is an information message only. No corrective action is required.
PORT (n) PORT BOOT COMPLETE	219000	High	Normal	This message indicates that the Port boot command has been successfully completed. The value *PORT (n)* identifies the port affected.	216000	This is an information message only. There are no corrective actions necessary.
PORT (n) PORT BOOT COMPLETE	300000	High	Normal	This message indicates that a Port Boot has been completed. The value *PORT (n)* identifies the port affected.		This is an information message only. There are no corrective actions necessary.
PORT (n) PORT BOOT COMPLETE	306000	High	Normal	This message indicates that a port boot operation is completed successfully. The value *PORT (n)* indicates the port that has been booted.		This is an information message only. There are no corrective actions necessary.
PORT (n) PORT BOOT FAILURE *(cause)*	196001	High	Normal	This alarm indicates that a boot command was sent to a specific port on your node but the boot process failed. The value *PORT (n)* indicates the port that has failed to boot, while *(cause)* identifies the reason for boot failure.		There are two possible corrective actions that you can perform: • If the maximum number of ports has been incorrectly configured, you should perform a Node Boot for the changed Port Record parameter to take affect. • If the Port is disabled, enable it and reboot the port.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) PORT BOOT FAILURE *(cause)*	219001	High	Normal	This message indicates that a Port boot command could not be successfully completed. The value *PORT (n)* identifies the port which has failed, while *(cause)* indicates one of the following reasons for the failure: • NO CONFIGURATION • PORT TYPE CHANGED • PORT DISABLED	216000	Perform the appropriate operation to correct this alarm condition: • If "NO CONFIGURATION" is displayed, a CMEM record does not exist for the port indicated. Configure a port record for the port identified in the alarm message. • If "PORT TYPE CHANGED" is displayed, a port change has been made on a node that does not support dynamic port type changes. Perform a node boot. • If "PORT DISABLED" is displayed, the identified ATPAD port did not come up. This is probably because the port has been disabled via the CTP port. Enable the port via the CTP port.
PORT (n) PORT BOOT FAILURE *(cause)*	306001	High	Normal	This alarm indicates that a boot command was sent to a specific port on your node but the boot process failed. The value *PORT (n)* indicates the port that has failed to boot, while *(cause)* identifies the reason for boot failure.		There are two possible corrective actions that you can perform: • If the maximum number of ports has been incorrectly configured, you should perform a Node Boot for the changed Port Record parameter to take affect. • If the Port is disabled, enable it and reboot the port.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) PORT BOOT FAILURE - *(cause)*	88001	High	Normal	This message indicates that a FRI port boot could not be performed for the indicated reason. The value *PORT (n)* identifies the port affected.		A node boot is required to correct this problem.
PORT (n) PORT DISABLE COMPLETE	139003	High	Warning	This message indicates completion of Port Disable command. The value *PORT (n)* identifies the disabled port.	139002	This is an information message only. No corrective action is required.
PORT (n) PORT DISABLE COMPLETE	193003	High	Warning	This message indicates the completion of a Port Disable command. The value *PORT (n)* identifies the port number.	193002	This is an information message only. No corrective action is required.
PORT (n) PORT DISABLE FAILURE *(cause)*	306003	High	Normal	This message indicates that you attempted to disable a port that a is already disabled. The value *PORT (n)* indicates the port that has not been disabled, while *(cause)* identifies the reason for the failure.		This is an information message only. There are no corrective actions necessary.
PORT (n) PORT DISABLED	69001	High	Warning	This message is displayed after the port has been disabled. The value *PORT (n)* indicates the port number.	69002	This is an information message only. No corrective action is required.
PORT (n) PORT DISABLED	88002	High	Warning	This message indicates that a FRI port has been disabled via the CTP. The value *PORT (n)* identifies the port affected.		This messages for information purposes only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) PORT DISABLED	129002	High	Normal	This message indicates that a port has been disabled via the CTP port. The value *PORT (n)* identifies the port affected.	129004	This is an information message only. There are no corrective actions necessary.
PORT (n) PORT DISABLED	196002	High	Warning	This message indicates that the port has been successfully disabled. The value *PORT (n)* indicates the port that has been disabled.	196003	This is an information message only. No corrective action is required.
PORT (n) PORT DISABLED	219002	High	Warning	This message indicates that a Port has been successfully disabled. The value *PORT (n)* identifies the disabled port.	219003	This is an information message only. There are no corrective actions necessary.
PORT (n) PORT DISABLED	300001	High	Warning	This message indicates that someone has disabled a port via the CTP port. The value *PORT (n)* indicates the port affected.	300002	This is an information message only. There are no corrective actions necessary.
PORT (n) PORT DISABLED	306002	High	Warning	This message indicates that the port has been successfully disabled. The value *PORT (n)* indicates the port that has been disabled.	306004	This is an information message only. There are no corrective actions necessary.
PORT (n) PORT ENABLED	69002	High	Normal	This message indicates that the port has been enabled. The value *PORT (n)* indicates the port number.		This is an information message only. No corrective action is required.
PORT (n) PORT ENABLED	88003	High	Normal	This message indicates that a FRI port has been enabled via the CTP. The value *PORT (n)* identifies the port affected.		This messages for information purposes only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) PORT ENABLED	196003	High	Normal	This message indicates that the port has been enabled. The value *PORT (n)* indicates the port affected.		This is an information message only. No corrective action is required.
PORT (n) PORT ENABLED	219003	High	Normal	This message indicates that a Port has been successfully enabled. The value *PORT (n)* identifies the enabled port.		This is an information message only. There are no corrective actions necessary.
PORT (n) PORT ENABLED COMPLETE	139002	High	Normal	This message indicates the completion of Port Enable command. The value *PORT (n)* identifies the enabled port.		This is an information message only. No corrective action is required.
PORT (n) PORT ENABLED COMPLETE	193002	High	Normal	This message indicates the completion of a Port Enable. The value *PORT (n)* identifies the port number.		This is an information message only. No corrective action is required.
PORT (n) PORT ERROR COUNT > THRESHOLD	107000	Medium	Warning	This message indicates that the total error count (equal to overrun errors plus underrun errors) is greater than that configured for the Node Error Threshold parameter. The value *PORT (n)* indicates the port affected.		This is most likely the result of a problem with your node hardware. Have this hardware serviced. There are no software related corrective actions applicable.
PORT (n) PORT ERROR COUNT > THRESHOLD	259000	Medium	Warning	This message indicates that the total error count (equal to overrun errors plus underrun errors) is greater than that configured for the Node Error Threshold parameter. The value *PORT (n)* indicates the port affected.		This is most likely the result of a problem with you node hardware. Have this hardware serviced when convenient. There are no software related corrective actions applicable.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) PORT INITIALIZATION FAILED - *(cause)*	88010	High	Critical	This message indicates that a FRI port could not be created for the indicated reason.	88000	To correct this problem: a) Install more RAM, or b) Reduce the number of ports, stations or channels configured on the node.
PORT (n) PORT INITIALIZATION FAILURE *(cause)*	139004	High	Critical	This alarm indicates that a port could not be initialized. The value *PORT (n)* identifies the port number while *(cause)* indicates the reason for the failure.	139002	Correct the cause of this alarm as indicated in the *(cause)* string and boot the port.
PORT (n) PORT INITIALIZATION FAILURE *(cause)*	193004	High	Critical	This alarm indicates that a port could not be initialized. The value *PORT (n)* identifies the port number and *(cause)* identifies the reason for the failure.	193000	Correct the cause of this alarm as indicated in the *(cause)* string and boot the port.
PORT (n) PORT STATUS WARNING *(cause)*	196005	Low	Warning	This message indicates that, during a node boot, the port is disabled. The value *PORT (n)* indicates the port affected while *(cause)* identifies the reason for the warning itself.	196000	To correct this situation, enable the port.
PORT (n) PORT STATUS WARNING - *(cause)*	88009	Low	Warning	This message indicates that an indicated port status condition is present. The value *PORT (n)* identifies the port affected.	88000	This messages for information purposes only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) PORT STATUS WARNING, LIMIT EXCEEDED PAGING TERMINAL IS IDENTIFIED AS *(t)*	300005	Medium	Warning	Each TFRI connection (to the TFR) is associated with a Paging Terminal Number that is configured in the TDLC port. When this alarm is displayed, a TFRI connection, registering the TDLC port with the configured Paging Terminal Number, does not exist. The value *PORT (n)* indicates the port affected, while *(t)* identifies the terminal to which the connection is being registered.	300000	To correct this problem: • Increase the 'Number of Paging Terminal' parameter value in TFR record. • Delete the extra TDLC port configuration.
PORT (n) PORT UTILIZATION > THRESHOLD	88004	Medium	Warning	This message indicates that the link utilization on the FRI port has exceeded the threshold configured in the Node Record. The value *PORT (n)* identifies the port affected.		This messages for information purposes only. No corrective actions are required.
PORT (n) PORT UTILIZATION > THRESHOLD	196004	Medium	Warning	This message indicates that the utilization of a Port has exceeded the limit configured for the Port Utilization Threshold parameter. The value *PORT (n)* identifies the port affected.	196000	Either off-load some of the traffic from this port or increase the line speed. **■ Note** Consider increasing the configured value of the “Port Utilization Threshold” if it is set unreasonably low.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) PROTOCOL ERROR THRESHOLD REACHED *(protocol)*	87017	Medium	Major	This alarm indicates that the link management protocol has detected too many errors (N392 errors our of the last N392 events). The value *PORT (n)* identifies the port affected and *(protocol)* identifies the control protocol operating on that port.		Contact your customer service representative if this alarm is displayed.
PORT (n) RETRIES *(r)* VIOLATIONS, NO ACTION	44011	Medium	Normal	This alarm indicates that the Port record "Call Option" parameter is configured as Mnemonic, and the Autocall establishment for the specified mnemonic has failed No action is taken on the port. The value *PORT (n)* indicates the port number while *(r)* identifies the maximum number of retries configured.		To correct this problem: • Check the Mnemonic Table configuration. • Check the X.25 link.
PORT (n) RETRIES *(r)* VIOLATIONS, PORT DEGRADED	44010	Medium	Warning	This alarm indicates that the Port record "Call Option" parameter is configured as Mnemonic, and the Autocall establishment for the specified mnemonic has failed. The Port is Busied out as configured in the Port record parameter "Action Type for MNEM Failure". The value *PORT (n)* indicates the port number while *(r)* identifies the maximum number of retries configured.		To correct this problem: • Check the Mnemonic Table configuration. • Check the X.25 link.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) RETRIES *(r)* VIOLATIONS, PORT DISCONNECTED	44008	Medium	Critical	This alarm indicates that the Port record "Call Option" parameter is configured as Mnemonic, and the Autocall establishment for the specified mnemonic has failed. The Port is disconnected as configured in the Port record parameter "Action Type for MNEM Failure". The value *PORT (n)* indicates the port number while *(r)* identifies the maximum number of retires configured.		To correct this problem: • Check the Mnemonic Table configuration. • Check the X.25 link.
PORT (n) RETRIES *(r)* VIOLATIONS, PORT LOCKED	44009	Medium	Critical	This alarm indicates that the Port record "Call Option" parameter is configured as Mnemonic, and the Autocall establishment for the specified mnemonic has failed. The Port is disabled as configured in the Port record parameter "Action Type for MNEM Failure". The value *PORT (n)* indicates the port number while *(r)* identifies the maximum number of retries configured.		To correct this problem: • Check the Mnemonic Table configuration. • Check the X.25 link.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT *(n) Station (s)* STATION Created	20021	Medium		This message indicates that the software has destroyed the old station and is in the process of creating the new station. Depending on Node loading this activity may take an extended amount of time. This delay is to minimize the data passing effect on other ports/devices/stations/ channels.		This is an information message only. No corrective action is required.
PORT (n) Station (s) STATION STARTED	20020	High		This message indicates that the software is in the process of destroying the current on-line station via the station update. Depending on Node loading this activity may take an extended amount of time. This delay is to minimize the data passing effect on other ports/devices/stations/ channels.		This is an information message only. No corrective action is required.
PORT (n) Station (s) STATION COMPLETE	20022	High		This message indicates that the software has completed a station update. This boot destroys and recreates the station data structure before initialization.		This is an information message only. No corrective action is required.
PORT (n) SW56K CALL FAILED - NO PHONE NUMBER	6011	High	Warning	This message indicates that an error was detected in the phone number configuration.	6007, 6008, 6010	Correct the phone number configuration and proceed.
PORT (n) SW56K CALL TO *(n)* FAILED	6009	High	Warning	This message indicates that an attempt by the given port (*PORT (n)*) to the phone number *(n)* failed.	6007, 6008, 6010	Make sure that the destination number is correct and is ready to accept calls.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) SW56K CALLING *(n)*	6007	Medium	Normal	This message indicates the port number (*PORT (n)*) and the called phone number *(n)*.		This is an information message only. No corrective action is required.
PORT (n) SW56K CONNECTED TO *(n)*	6008	Medium	Normal	This message indicates the port number (*PORT (n)*) and the called phone number *(n)*.		This is an information message only. No corrective action is required.
PORT (n) SW56K IN CHANNEL LOOPBACK	6017	High	Warning	This message indicates that a port was placed in Channel Loopback mode. The value *PORT (n)* identifies the port affected.	6008, 6010, 6015	This is an information message only. No corrective action is required.
PORT (n) SW56K IN DSU LOOPBACK	6018	High	Warning	This message indicates that a port was placed in the DSU loopback mode. The value *PORT (n)* identifies the port affected.	6007, 6008, 6010, 6015	This is an information message only. No corrective action is required.
PORT (n) SW56K INCOMING CALL ANSWERED	6010	Medium	Normal	This message indicates that the port just accepted an incoming call.		This is an information message only. No corrective action is required.
PORT (n) SW56K INCOMING CALL IGNORED	6012	High	Warning	This message indicates that an incoming call was ignored because Call Security is enabled.	6007, 6008, 6010	Reconfiguring the Call Security feature may correct this alarm. Generally, you can ignore this alarm.
PORT (n) UNSUPPORTED DATABITS: OPERATING WITH 8 DATABITS, NO PARITY	259001	Medium	Minor	This alarm indicates that the configured number of data bits is less than 7. This configuration is not supported and has been defaulted to 8 Data Bits with No Parity. The value *PORT (n)* indicates the port affected.		To correct this problem, check the configuration of the port indicated and modify the configuration as required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) UNSUPPORTED PARITY: OPERATING WITH 8 DATABITS, NO PARITY	107003	Medium	Minor	This message indicates that your node does not support a port configuration of 8 Data Bits, No Parity. The value *PORT (n)* indicates the port affected.		Recheck the port configuration and changes as required.
PORT (n) UNSUPPORTED BAUDRATE: OPERATING AT 9600 BPS	107002	Medium	Minor	This message indicates that AutoSpeed is not supported on SMC ports (i.e. port 4 of LCIF) 9600 baud. The value *PORT (n)* indicates the port affected.		Check the PAD port record configuration and modify it as required.
PORT (n) UNSUPPORTED DATABITS: OPERATING WITH 8 DATABITS, NO PARITY	107001	Medium	Minor	This alarm indicates that the configured number of data bits is less than 7. This configuration is not supported and has been defaulted to 8 Data Bits with No Parity. The value *PORT (n)* indicates the port affected.		To correct this problem, check the configuration of the port indicated and modify the configuration as required.
PORT (n) UNSUPPORTED FRAME SIZE: OPERATING WITH 1024 BYTES	196006	Medium	Minor	This message indicates that a port is booted, and the maximum configured frame size is 4K while the port driver (hardware) only supports 1K frame size. The value *PORT (n)* identifies the port affected.	196000	Adjusting the frame size will correct this problem.
PORT (n) UNSUPPORTED PARITY: OPERATING WITH 8 DATABITS, NO PARITY	259003	Medium	Minor	This message indicates that your node does not support a port configuration of 8 Data Bits, No Parity. The value *PORT (n)* identifies the port affected.		Recheck the port configuration and changes as required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT (n) UNSUPPORTED BAUDRATE: OPERATING AT 9600 BPS	259002	Medium	Minor	This message indicates that AutoSpeed is not supported on SMC ports (i.e. port 4 of LCIF) 9600 baud. The value *PORT (n)* identifies the port affected.		Check the PAD port record configuration and modify it as required.
PORT (n) VIRTUAL MAPPING ERROR, CAUSE: *(cause)*	282005	Low	Critical			Contact your customer service representative if this alarm appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n), FRAME DISCARDED - *(cause)*, *(SA)* - *(DA)*	227003	Low	Minor	This alarm indicates that data frames are being discarded. The value *PORT (n)* identifies the port affected, *(cause)* identifies one of the following causes for the problem, *(SA)* identifies the Source Address of the discarded frames, and *(DA)* identifies the destination address of the discarded frames: • CAN RECEIVED: No Route on the TNPP device for transmitting data frames. • RETRY EXCEEDED: The data frame has been retried more than six times. • QUEUE FULL: The outbound queue, to the remote TNPP PAD, is full. • BLOCKED BY NETWORK: The outbound connection to the remote TNPP PAD, is congested. • INCOMPLET FRAME: The data frame from the remote TNPP PAD is not complete. • HOLD RETRY EXCEEDED: The data frame for the TNPP device was held for more that six times. • HOLD QUEUE FULL: The data frame for the TNPP device can not be queued.		To correct this problem: • Verify that the TNPP routing device is properly configured. • Check to see if the TNPP device is congested. • Verify that the TNPP device is responding. • Determine whether the network link is congested.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n), LINK DOWN - *(cause)*, *(xx)* DATA FRAMES LOST	227000	Medium	Major	This alarm indicates that frames are lost and that the link is down. The value *PORT (n)* identifies the link affected while *(cause)* identifies one of these potential causes for the failure: • LINE DISCONNECTED • PORT BOOT/DISABLED • ENQ RETRY EXCEEDED The value *(xx)* identifies the number of frames that have been lost.	227001	To correct this problem: • Verify that the terminal is operating correctly and properly connected. • Verify that the X.25 connection is operational. • Check the X.25 configuration.
PORT (n), LINK UP	227001	Low	Minor	This alarm indicates that an EOT is received from the attached TNPP device. The value *PORT (n)* identifies the link affected.		This is an information message only. No corrective action is required.
PORT (n), PROTOCOL ERROR	227002	Medium	Warning	This alarm indicates that one of these conditions has occurred: • Unexpected control characters have been received during transmission of data frames from a PAD to a terminal. • One or more data frames have been received from the terminal before acknowledging earlier data. The value *PORT (n)* identifies the port affected.		To correct this problem, verify that the TNPP device is properly configured.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT - DYNAMIC PORT BEING CREATED	2007	Medium		This message indicates that the software has completely destroyed the old port type and is in the process of creating the new port type via the dynamic port. Depending on Node loading this activity may take an extended amount of time. This delay is to minimize the data passing effect on other ports/devices/stations/ channels.The value *PORT* identifies the port that has been reconfigured. This can be either SDLC or XDLC.		This is an information message only. No corrective action is required.
PORT - DYNAMIC PORT COMPLETED	2008	High		This message indicates that the software has completed a dynamic port. This destroys and recreates the port's data structures before initialization. The standard port simply re-initializes data structures.The value *PORT* identifies the port that has been reconfigured. This can be either SDLC or XDLC.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT - DYNAMIC PORT STARTED	2006	High		This message indicates that the SDLC software is in the process of destroying the current on-line port type via the dynamic port. Depending on Node loading this activity may take an extended amount of time. This delay is to minimize the data passing effect on other ports/devices/stations/ channels. The value *PORT* identifies the port that has been reconfigured. This can be either SDLC or XDLC.		This is an information message only. No corrective action is required.
PORT BOOT COMPLETE	129000	High	Normal	This message indicates that a Port boot has been completed successfully.		This is an information message only. There are no corrective actions necessary.
PORT DISABLED	51002	High	Warning	This alarm indicates that a port has been disabled by a CTP command.	51003	This is an information message only. No corrective action is required.
PORT ENABLED	51003	High	Normal	This alarm indicates that a port has been enabled by a CTP command.		This is an information message only. No corrective action is required.
PORT FAILURE	280001	High	Critical	This alarm indicates that a voice daughtercard has failed its power-up diagnostic routine.		Re-insert the voice card and try again. If this problem persists, you may have to replace the Voice daughtercard.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT FAILURE, CAUSE: MISSING BATTERY	281002	High	Critical	This message indicates that the DSPM-FXS or DSPM-E&M, if the E&M port is configured for Type II, III, or V, is not connected to the internal -48 volts supply or the internal -48v supply is not installed.		Verify that the -48v/Ringer supply is installed and is cabled to the DSPM card in question. If you check the above and the problem still persist try replacing the cable between the -48v/Ringer supply and the DSPM card.
PORT FAILURE, CAUSE: MISSING RINGER SUPPLY	281003	High	Critical	This message indicates that the DSPM-FXS is not connected to the internal ringer supply or the ringer supply is not installed.		Verify that the -48v/Ringer supply is installed and is cabled to the DSPM card in question. If you check the above and the problem still persist try replacing the cable between the -48v/Ringer supply and the DSPM card.
PORT STATUS WARNING - *(cause)*	51005	Low	Warning	This alarm indicates that a specific port status warning has been generated. The *(cause)* string identifies what has caused this alarm.	51000	Take the action necessary to correct the *(cause)*.
PORT UTILIZATION > THRESHOLD	51004	Medium	Warning	This alarm indicates that port utilization has exceeded the configured threshold.	51000	This is an information message only. No corrective action is required.
PORT UTILIZATION > THRESHOLD	130004	Medium	Warning	This message indicates that out/in utilization of the char/sec parameter exceeded the configured port threshold limit in the node record.		This is an information message only. There are no corrective actions necessary.
PORT_BOOT:SWITCHED TO Low BANDWIDTH	230010	Low	Normal	This is a special report generated under unique conditions. It implies that a Link has been switched to low bandwidth because the port has been booted.		This is an information message only. There are no corrective actions necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PORT_DISABLE:SWITCHED TO Low BANDWIDTH	230009	Low	Normal	This is a special report generated under unique conditions. It implies that a Link has been switched to low bandwidth because the port has been disabled.		This is an information message only. There are no corrective actions necessary.
PRI-**%d**B**%d** - OUTGOING CALL TO **%s** CONNECTED ON *PORT (n)*	283012	Medium	Normal	ISDN PRI Call is outgoing.		This is an information message only. There are no corrective actions necessary.
PRI-**%d** - **%s** CALL **%s** **%s** ON PORT **%d** DISCONNECTED BY 65xx	283013	Medium	Normal			Contact your customer service representative if this alarm is displayed.
PRI-**%d** - **%s** CALL **%s** **%s** ON PORT **%d** DISCONNECTED BY NETWORK	283014	Medium	Normal			Contact your customer service representative if this alarm is displayed.
PRI-**%d** - INCOMING CALL TO **%s** FROM **%s** FAILED ON PORT **%d**, **%s**	283015	Medium	Minor			Contact your customer service representative if this alarm is displayed.
PRI-**%d** - OUTGOING CALL TO **%s** FROM **%s** FAILED ON PORT **%d**, **%s**	283016	Medium		ISDN PRI call outgoing failed.		Contact your customer service representative if this alarm is displayed.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PRI-**%d** - INCOMING CALL TO **%s** FROM **%s** FAILED ON PORT **%d**, **%s**	283017	Medium		ISDN PRI call incoming failed.		Contact your customer service representative if this alarm is displayed.
SHDSL-**%d** *PORT (n)* - PORT BOOT COMPLETE	494000	High	Critical	This message is generated when a port boot is complete.		This message is for information only. No corrective actions are necessary.
SHDSL-**%d** *PORT (n)* - PORT BOOT FAILURE %s	494001	High	Critical	This alarm is generated when a port boot did not complete successfully. %s is the failure cause. Possible values for %s are: (CONFIG FAILED)-Invalid configuration, (CONFIG PCK TIMEOUT)- Communication to the daughtercard, (CONFIG FAILED 0xc)-Config failed due to invalid state, (CONFIG FAILED 0xd)-Config failed due to invalid state, (CONFIG FAILED 0xe)-Config failed due to invalid state.		For %s equal to (CONFIG FAILED), check the configuration parameters, then manually boot the port. For %s equal to (CONFIG PCK TIMEOUT), manually boot the port. For %s equal to (CONFIG FAILED 0xc), manually boot the port. For %s equal to (CONFIG FAILED 0xd), manually boot the port. For %s equal to (CONFIG FAILED 0xe), manually boot the port.
SHDSL-**%d** *PORT (n)* - PORT DISABLED COMPLETE	494003	High	Critical	This message is generated when a port disable has completed.		This message is for information only. No corrective actions are necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
SHDSL-**%d** *PORT (n)* - PORT INITIALIZATION FAILURE **%s**	494004	High	Critical	This message is generated when a port initialization did not complete successfully. %s is the failure cause. Possible values for %s are: (BOOT FAILED PLEASE RETRY)-An error occurred during booting. (CONFIG SEND FAILED)-An error occurred during port initialization. (CONFIG PCK TIMEOUT)-An error occurred during port initialization. (CONFIG FAILED)-An error occurred due to a bad configuration.		(BOOT FAILED PLEASE RETRY) - Manually boot the port. (CONFIG SEND FAILED)-Manually boot the port. (CONFIG PCK TIMEOUT)-Manually boot the port. (CONFIG FAILED)-Check the configuration parameters, then manually boot the port.
SHDSL-**%d** *PORT (n)* - PORT ENABLED COMPLETE	494002	High	Critical	This message is generated when a port enable has completed.		This message is for information only. No corrective actions are necessary.
SHDSL-**%d** *PORT (n)* - PORT STATUS WARNING - PORT DISABLED		High		This message is generated when the port running version has been created (node boot or power on events) and the port is in a disabled status.		This message is for information only. No corrective actions are necessary.
SHDSL-**%d** *PORT (n)* - PORT ACTIVE	494005	High	Critical	This message indicates the status of the G.SHDSL physical link is active and is now ready to achieve cell delineation.		This message is for information only. No corrective actions are necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
SHDSL-**%d** *PORT (n)* - PORT RETRYING	494006	Medium	Major	This alarm indicates the G.SHDSL physical link has timed-out in its current attempt to become active and is retrying to achieve active status.		Verify the configuration and physical connection.
SHDSL-**%d** *PORT (n)* - PORT INACTIVE (RETRAINING)	494007	High	Critical	This message indicates the G.SHDSL physical ink has become inactive due to a retrain condition.		The G.SHDSL Port statistics indicate the Last Retrain Reason. Using this statistic, adjust the port configuration accordingly.
SHDSL-**%d** *PORT (n)* - PORT INACTIVE (WATCHDOG TIMEOUT)	494008	High	Critical	This alarm indicates the G.SHDSL physical link has become inactive due to a Watchdog timeout error within the G.SHDSL Hardware.		This error may indicate a hardware problem.
SHDSL-**%d** *PORT (n)* - PORT INACTIVE (LOC)	494009	High	Critical	This alarm indicates the G.SHDSL physical link has become inactive due to detecting a Loss of Carrier Condition.		Verify configuration and physical connection.
SHDSL-**%d** *PORT (n)* - PORT CONFIG ERROR (%s)	494010	Medium	Major	This alarm indicates the G.SHDSL physical link has encountered a configuration error during activation or handshaking.		Verify configuration and physical connection.
SHDSL-**%d** CONFIGURATION INITIALIZATION FAILURE - **%<cause>**		High		This notification indicates that the bit setting for configInitFailure in the hdsl2ShdslEndpointCurrStatus object for this endpoint has changed. <cause> is a cause of the failure"ATM" - no AAM port configured		This message is for information only. No corrective actions are necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
T1/E1-**%d** VIRTUAL PORT **%d** - No T1/E1 memory available	283032	Medium				Contact your customer service representative if this alarm is displayed.
T1/E1-**%d** VIRTUAL PORT **%d** - T1/E1 CARD DOES NOT SUPPORT DATA or SWITCHED DATA PORTS	283030	High				Contact your customer service representative if this alarm is displayed.
T1/E1-**%d** VIRTUAL PORT **%d** - No T1/E1 memory available	283032	Medium				Contact your customer service representative if this alarm is displayed.
T14 TIMER EXPIRED	250011			This message indicates that the switched access path has been disconnected because no SVCs were active for the previous period of time (in seconds) configured for the T14 Timer parameter.	250000	This message is for information only. No corrective actions are necessary.
TPR-BOOT COMPLETE	317000	High	Normal	This message indicates that TPDU Router boot process has been completed successfully.		This is an information message only. There are no corrective actions necessary.
TR-**%d** PORT NOT DISABLED	138017	Medium	Normal			Contact your customer service representative if this alarm is displayed.
TR-**%d** TX HALTED	138012	Medium	Major		138003	Contact your customer service representative if this alarm is displayed.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TR-*(x)* BEACON CONDITION	138008	Medium	Critical	This message indicates that this alarm indicates that a Token Ring Port is receiving beacon MAC frames, or the Token Ring Port is transmitting beacon MAC frames. Data is unable to successfully traverse the Token Ring Network. The value *(x)* identifies the Token Ring Port affected.	138008	To correct this problem: • Verify that the Token Ring Port configuration, and the configuration of the other stations on the ring is consistent. • Verify that there are no disconnected cables in the Token Ring network.
TR-*(x)* COMMAND REJECT **%x** (**%x***)*	138013	Medium	Major	This alarm indicates that n internal error has occurred in the Vanguard device. The value *(x)* identifies the Token Ring Port affected.	138003	Contact your customer service representative if this alarm is displayed.
TR-*(x)* AUTO REMOVE ERROR	138015	Medium	Major	This message indicates that the Token Ring Port has determined that it is the cause of the Beacon condition, so it has detached itself from the Token Ring Network.The value *(x)* identifies the Token Ring Port affected.	138003	Resolve the cause of the Beacon condition and reboot the Token Ring port.
TR-*(x)* DIAGNOSTIC CHECK	138026	High	Critical	This message indicates that the Token Ring port software has encountered an error condition. Under normal operating conditions, this alarm should never be displayed. It indicates a hardware or software problem. The Token Ring port automatically attempts to recover from the anomalous condition. The value *(x)* identifies the Token Ring Port affected.	138003	If this alarm occurs constantly, run diagnostics or contact your customer service representative.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TR-*(x)* FATAL ERROR	138019	High	Critical	This alarm indicates that an internal error has occurred in the Vanguard device. The value *(x)* identifies the Token Ring Port affected.	138003	Contact your customer service representative if this alarm is displayed.
TR-*(x)* LOBE WIRE FAULT	138014	Medium	Critical	This message indicates that the Token Ring Port lobe wire current is either too low or too high to allow data transmission or reception on the Token Ring Port. The value *(x)* identifies the Token Ring Port affected.	138003	Check for a faulty connection from the Token Ring Card to Token Ring network.
TR-*(x)* LOSS OF SIGNAL	138006	Medium	Major	This alarm indicates that the signal, on the receive side of the Token Ring Port, is either nonexistent or is not powerful enough for the Token Ring Port to interpret receive data. The value *(x)* identifies the Token Ring Port affected.		To correct this problem, check for a faulty connection from the Token Ring card to the Token Ring network.
TR-*(x)* LOSS OF SIGNAL CLEARED	138007	Medium	Normal	This message indicates that the "Loss of Signal" condition has been cleared. The value *(x)* identifies the Token Ring Port affected.		To correct this problem, check for a faulty connection from the Token Ring card to the Token Ring network.
TR-*(x)* PORT CMD TIMEOUT **%x**	138018	High	Major	This alarm indicates that the TMS380 adapter has been requested to issue a command failed; the command code is included in the event. The value *(x)* identifies the Token Ring Port affected.		This alarm indicates that a hardware or software problem; run diagnostics or call your customer service representative.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TR-*(x)* PORT DOWN	138022	High	Major	This alarm indicates that a Token Ring Port is down. This is due to: a) The Token Ring Port having been disabled via the CTP, b) A Lobe Wire Fault, Auto-Remove, or Remove received condition existing. The value *(x)* identifies the Token Ring Port affected. The value *(x)* identifies the Token Ring port affected.	138003, 138021	Determine cause of Token Ring port going down and correct those faults.
TR-*(x)* PORT INITIALIZATION FAILURE TMS380 OPEN FAILED	138002	High	Critical	This alarm indicates that the TMS380 experienced an error condition when attaching to the ring. The value *(x)* identifies the Token Ring card affected.		To correct this problem, check the Token Ring port configuration and the connection from the Token Ring card to the Token Ring network.
TR-*(x)* PORT INITIALIZATION FAILURE TMS380 RESET FAILED	138000	High	Critical	This alarm indicates that an error has occurred in the TMS380 power-up diagnostics, or during the TMS380 initial software download. The value *(x)* identifies the Token Ring card affected.	138003	To correct this problem, replace the Token Ring card identified in the alarm description.
TR-*(x)* PORT INITIALIZATION FAILURE TMS380 INIT FAILED	138001	High	Critical	This alarm indicates that an error in TMS380 initialization sequence has occurred. The value *(x)* identifies the Token Ring card affected.	138003	To correct this problem, replace the Token Ring card identified in the alarm description.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TR-*(x)* PORT INITIALIZATION SUCCESSFUL	138003	High	Normal	This message indicates that the Token Ring Port has successfully run through the reset, initialization, and open phases of initialization, and is ready to transmit and receive data. The value *(x)* identifies the Token Ring port affected.		This is an information message only. There are no corrective actions necessary.
TR-*(x)* PORT UP	138021	High	Normal	This message indicates that the Token Ring Port is up and functional. The port has been re-enabled, or the Lobe Wire Fault condition has been resolved. The value *(x)* identifies the Token Ring port affected.		This is an information message only. There are no corrective actions necessary.
TR-*(x)* REMOVE RECEIVED	138016	Medium	Warning	This message indicates that the Token Ring Port has received a "Remove Ring Station" MAC Frame from another station on the ring, and removed itself from the ring. The value *(x)* identifies the Token Ring Port affected.	138003	Determine if removing the Ring Station was done by the LAN Manager intentionally. The Token Ring port can be rebooted to get it to reattach to the ring.
TR-*(x)* RX COMMAND TIMed OUT	138004	High	Major	This alarm indicates that the TMS380 adapter has failed to receive frames sent to it. This is an indication of a hardware or software problem. The value *(x)* identifies the adapter affected.		Contact your customer service representative if this alarm is displayed.
TR-*(x)* SINGLE STATION ERROR	138020	Medium	Major		138003	Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TR-*(x)* TRANSMIT DIAG	138025	High	Critical	This message indicates that the Token Ring port software has encountered an error condition. Under normal operating conditions, this alarm should never be displayed. It indicates a hardware or software problem. The Token Ring port automatically attempts to recover from the anomalous condition. The value *(x)* identifies the Token Ring Port affected.	138003	If this alarm occurs constantly, run diagnostics or contact your customer service representative.
TR-*(x)* TRANSMIT ERROR	138023	High	Major	This message indicates that the Token Ring software has encountered an error condition. Under normal operating conditions, this alarm should never be displayed. It indicates a hardware or software problem. The Token Ring port automatically attempts to recover from the anomalous condition. The value *(x)* identifies the Token Ring port affected.	138003	If this alarm occurs constantly, run diagnostics or contact your customer service representative.
TR-*(x)* TRANSMIT ERROR 2	138024	High	Major	This message indicates that the Token Ring software has encountered an error condition. Under normal operating conditions, this alarm should never be displayed. It indicates a hardware or software problem. The Token Ring port automatically attempts to recover from the anomalous condition. The value *(x)* identifies the Token Ring port affected.	138003	If this alarm occurs constantly, run diagnostics or contact your customer service representative.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TR-*(x)* TRANSMIT TIMEOUT				This message indicates that the Token Ring software failed to transmit data frames.		Contact your customer service representative if displayed.
TR-*(x)* TX BEACON CONDITION	138010	Medium	Critical	This alarm indicates that a Token Ring Port is transmitting Beacon MAC frames. This indicates that data is unable to successfully traverse the Token Ring network. The value *(x)* identifies the Token Ring Port affected.	138003	To correct this problem: • Verify that the Token Ring Port configuration, and the configuration of the other stations on the ring is consistent. • Verify that there are no disconnected cables in the Token Ring network.
TR-*(x)* TX BEACON CONDITION CLEARED	138011	Medium	Normal	This message indicates that the Beacon condition cleared and the unit is no longer transmitting the beacon signal. The value *(x)* identifies the Token Ring Port affected.		This is an information message only. No correct action is require.
TR-*(x)* TX COMMAND TIMed OUT	138005	High	Major	This alarm indicates that the TMS380 adapter has failed to transmit data frames. This is an indication of a hardware or software problem. The value *(x)* identifies the adapter affected.	138003	Contact your customer service representative if this alarm is displayed.
UNSUCCESSFUL CALL THRESHOLD EXCEEDED	250010			This message indicates that the number of unsuccessful calls, since the switched access path was established for this dial-in port, has exceeded the configured value. No further calls will be permitted on this port and the switched access path will be disconnected once all the existing calls are cleared.	250000	This message is for information only. No corrective actions are necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
V.25 BIS UNKNOWN ERROR	6006	High	Minor	An unexpected block of data was received from the attached device during V.25 bis protocol handshaking.		Verify that the device connected to the physical port is properly configured for V.25 bis.
VOICE CALL: CALLING *(cnum)*, CALLED *(cdnum)*, SRC *(source)*, DEST *(destination)*, CLR *(reason)*, TIME *(t)* sec	281012	CONN	Normal	This report is generated by the voice calling port. • CALLING - The value *(cnum)* identifies the Calling Number. This is either the CALLING PARTY NUMBER, as defined in the QSIG/ISDN setup message, or as configured in the voice port record (“Local Subscriber Address”). • CALLED - The value *(cdnum)* identifies the Called Party Number. This is either the CALLED PARTY NUMBER, as defined in the QSIG/ISDN (and INFO) message*(s)*, or the number the user has dialled. • SRC - The value *(source) identifies the* source node and port of the calling voice port. • DEST - The value *(destination)* identifies the destination node and port number; the CALLED port.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
VOICE CALL: CALLING *(cnum)*, CALLED *(cdnum)*, SRC *(source)*, DEST *(destination)*, CLR *(reason)*, TIME *(t)* sec (Cont'd)	281012	CONN	Normal	CLR - The two digit value *(reason)* identifies the reason the call was cleared. The reasons include: • 0 - Normal clearing. • 1 - Call collision or remote end busy. • 3 - Successful CVS lookup, entry found. • 5 - No logical channel available (All circuits are in use). • 9 - Remote port disabled, remote T1/E1 port in alarm, no power on interface; FXO analog, remote port in loopback, or called end OOS. • 11 - PBX handshake error, called PBX clears before answered, software error or protocol violation, or called PBX clears before completion. • 13 - Caller disconnected before answered. • 17 - CCS clear other than normal or default. • 21 - RPOA Out of Order (Incompatible Destination) • 33 - Unsuccessful CVS lookup entry not found. • TIME - The value *(t)* identifies, in seconds, the duration of the call.		This is an information message only. No corrective action is required.
VOICE-*(x)* VSM RESPONSE: EID *(x)*, OPCODE *(x)*, PAYLOAD *(x)*	281015	Medium	Normal	This report is enabled via the voice port configuration and is used to aid in debugging a voice signaling protocol issue.		This is an information message only. No corrective action is required.

Chapter 3
Station Alarms and Reports

Introduction

This chapter describes those alarms and reports that are generated due to station activity on a Vanguard node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
%s - DYNAMIC ALL STATIONS BOOT STARTED	226009			All the stations are being de-allocated.		This is an information message only. No corrective action is required.
%s - DYNAMIC ALL STATIONS BEING CREATED	226010			All the stations are being allocated.		This is an information message only. No corrective action is required.
%s - DYNAMIC ALL STATIONS BOOT CREATED	226011			Completed creation of the stations.		This is an information message only. No corrective action is required.
%s - DYNAMIC ALL STATION BOOT STARTED	226012			Specified station is being de-allocated.		This is an information message only. No corrective action is required.
%s - DYNAMIC ALL STATION BOOT BEING CREATED	226013			Specified station is being re-allocated.		This is an information message only. No corrective action is required.
%s - DYNAMIC ALL STATION BOOT COMPLETED	226014			Completed creation of a specified station.		This is an information message only. No corrective action is required.
%s - END-TO-END SEGMENTATION LINK DOWN (or) %s - FRAME SEGMENTER LINK DOWN	87011	Medium	Normal	This alarm indicates that a peer's End-to-End segmentation is not configured properly.	87012	Configure the peer's segmentation properly.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
%s - END-TO-END SEGMENTATION LINK UP	87012	Medium	Warning	This alarm indicates that a peer's segmentation is configured properly.		None.
INSUFFICIENT DYNAMIC MEMORY TO SUPPORT %S CONFIGURATION	226015			Not enough dynamic port creation heap to complete the boot.		Increase dynamic port creation heap and/or delete some stations.
%s - NO STATION CREATED	226016			There is no station configured for creation.		This is an information message only. No corrective action is required.
%s - ALL STATIONS BOOT COMPLETE	226017			obsolete		This is an information message only.
%s - WILL REQUIRE FRI BOOT OF %d or/r/n	226018			New station requires associated FRI to be booted or the station will not connect.		Boot the associated FRI station
%s - ERR: SLAC DYNAMIC BOOT IN PROGRESS, TRY AGAIN WHEN COMPLETED	226019			Boot cannot be performed because all stations boot is still in progress.		Wait for current boot to complete, then re-issue the boot.
%s - UNI SEGMENTATION LINK DOWN	87018	Medium		This alarm indicates that the peer's UNI segmentation is not configured properly.		Configure the peer's segmentation properly.
%s - UNI SEGMENTATION LINK UP	87019	Medium		This alarm indicates that the peer's segmentation is configured properly.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
CHAIN portion of the TRANSPARENT BRIDGE FORWARDING TABLE is full	192000	High	Major	This alarm indicates that the number of stations stored in the table of learned stations has exceeded its maximum number.		You can perform two corrective actions: a) Decrease the Aging Timer parameter value. b) Implement Filtering.
DLCI CHANNEL DISCONNECTED BY FRI	225001	Medium	Normal	This message indicates that a Frame Relay PVC, and the associated FRI station is no longer available for use by LLC.		To correct this alarm, look at the FRI Station Status and determine why the PVC is down. **■ Note** Refer to the *Frame Relay Interface/Access Manual* (Part Number T0106-02) for additional information.
DYNAMIC STATION BEING CREATED	74022	Medium		This message indicates that the SDLC software has destroyed the old station and is in the process of creating the new station. Depending on node loading this activity may take an extended amount of time. This delay is to minimize the data passing effect on other ports/devices/stations/ channels.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DYNAMIC STATION BEING CREATED	112021	Medium		This message indicates that the XDLC software has destroyed the old station and is in the process of creating the new station. Depending on node loading this activity may take an extended amount of time. This delay is to minimize the data passing effect on other ports/devices/stations/ channels.		This is an information message only. No corrective action is required.
DYNAMIC STATION BOOT COMPLETED	112022	High		This message indicates that the XDLC software has completed a dynamic station. This destroys and recreates the station's data structures before initialization. The station simply re-initializes data structures.		This is an information message only. No corrective action is required.
DYNAMIC STATION BOOT COMPLETED	74023	High		This message indicates that the SDLC software has completed a dynamic station. This destroys and recreates the station's data structures before initialization. The station simply re-initializes data structures.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DYNAMIC STATION BOOT STARTED	74021	High		This message indicates that the SDLC software is in the process of destroying the current on-line station via the station update. Depending on node loading this activity may take an extended amount of time. This delay is to minimize the data passing effect on other ports/devices/stations/ channels.		This is an information message only. No corrective action is required.
DYNAMIC STATION BOOT STARTED	112020	High		This message indicates that the XDLC software is in the process of destroying the current on-line station via the station update. Depending on node loading this activity may take an extended amount of time. This delay is to minimize the data passing effect on other ports/devices/stations/ channels.		This is an information message only. No corrective action is required.
FRAME RECEIVED WITH BAD LENGTH: DLCI *(n)*	87002	Medium	Minor	This message indicates that this alarm indicates that a frame larger than the allowed maximum size has been received from the link. The DLCI is given by *(n)*.		Correct the configuration of the remote equipment so that it will not send frames larger than allowed locally.
INSUFFICIENT MEMORY TO PROTECT STATION	112019	High	Critical	This alarm indicates that Data Connection Protection has been configured although there is insufficient system memory to support this function.	112000	To correct this situation: • Add more system memory. • Delete any unused configurations, ports, or stations to free system memory. • Disable Data Connection Protection.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
INVALID DEVICE RESPONDING	308036	Medium	Minor	This alarm indicates that an invalid device is responding.	308000	Check the station configuration.
LSC - *(app)* *STATION (n)* - 5494 CONTROLLER DOWN	385010	Medium		This alarm indicates that an LLC-SDLC Station has brought down a LU6.2 Session and Conversation. This is the session/conversation used for Controller specific Data. The value *STATION (n)* identifies the LLC-SDLC station number affected, while *(app)* identifies one of these applications: • TR - Token Ring • ETH - Ethernet • FR - Frame Relay		Confirm that Test Frames and XID frames are being received by this LLC-SDLC Station. If they are not, check the state of the LAN/Frame Relay Port and Station. On the Host System, confirm that the APPC Controller for the LLC-SDLC Station controller is Varied On.
LSC - *(app)* *STATION (n)* - 5494 REMOTE CONNECTION ESTABLISHED	385029	Connect		This message indicates that an LLC-SDLC Station has successfully received a QLLC UA from the 5394-type Controller, through the network. The value *STATION (n)* identifies the LLC-SDLC station number affected, while *(app)* identifies one of these applications: • TR - Token Ring • ETH - Ethernet • FR - Frame Relay		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
LSC - *(app)* *STATION (n)* - 5494 WORKSTATION DOWN, LU ID : *(ID)*	385016	Medium		This alarm indicates that the LLC-SDLC Station has brought down a LU6.2 Session and Conversation. This is the session/ conversation used for Display specific Data. The value *STATION (n)* identifies the LLC-SDLC station number affected, while *(app)* identifies one of these applications: • TR - Token Ring • ETH - Ethernet • FR - Frame Relay		Confirm that the remote 5394-Type display/printer is attached, powered-up, and has a unique LU ID matching that in the AS/400 Display/Printer definition. On the Host System, confirm that the Display and Remote Work Station Controller for this Display is Varied On.
LSC - *(app)* *STATION (n)* - 5494 CONTROLLER UP	385009	Medium		This message indicates that an LLC-SDLC Station has successfully established a LU6.2 Session and Conversation with the AS/400 for Controller specific Data. The value *STATION (n)* identifies the LLC-SDLC station number affected, while *(app)* identifies one of these applications: • TR - Token Ring • ETH - Ethernet • FR - Frame Relay		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
LSC - *(app)* *STATION (n)* - 5494 REMOTE CALL ESTABLISHED	385030	Connect		This message indicates that an LLC-SDLC Station has successfully established a Call with the Remote SDLC TPAD station adjacent to the 5394-type Controller. The value *STATION (n)* identifies the LLC-SDLC station number affected, while *(app)* identifies one of these applications: • TR - Token Ring • ETH - Ethernet • FR - Frame Relay		This is an information message only. No corrective action is required.
LSC - *(app)* *STATION (n)* - 5494 STATION RECEIVED A REMOTE DISC	385028	Connect		This message indicates that the LLC-SDLC Station Received a Call Disconnect from the Remote SDLC TPAD station adjacent to the 5394-type Controller. The value *STATION (n)* identifies the LLC-SDLC station number affected, while *(app)* identifies one of these applications: • TR - Token Ring • ETH - Ethernet • FR - Frame Relay		To correct this problem: • Check the state of the Remote SDLC TPAD. • Check the power and state of the remote 5394-type controller.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
LSC - *(app)* *STATION (n)* - 5494 WORKSTATION UP, LU ID : *(ID)*	385017	Medium		This message indicates that an LLC-SDLC Station has successfully established a LU6.2 Session and Conversation with the AS/400 for Display specific Data for Remote Display/Printer. The value *STATION (n)* identifies the LLC-SDLC station number affected, while *(app)* identifies one of these applications: • TR - Token Ring • ETH - Ethernet • FR - Frame Relay		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
LSC-*(app) STATION (n)* - 5494 *(counter)* RETRY LIMIT REACHED	385001	Medium		This alarm indicates that a retry counter has reached it's configured limit. The value *(app)* identifies the application (TR - Token Ring, ETH - Ethernet, or FR - Frame Relay) involved, *STATION (n)* identifies the LLC-SDLC station number affected, and *(counter)* indicates one of these retry counters: • QLLC_C • QLLC_XID_C • QLLC_SM_C • ALLOCATE AND RECEIVE_AND_WAIT		Perform the necessary actions as listed below: • If the counter indicates: – QLLC_C, QLLC_XID_C – QLLC_SM_C: Check if the call to the remote TPAD is connected. If it is not, check the state of the network interface. If the network interface is OK, check configuration of the Route Selection Table or Mnemonic Table. • If the counter indicates: ALLOCATE AND RECEIVE_AND_ WAIT RETRY LIMIT REACHED – Check the state of the LLC-SDLC Station. If it is down, determine why and correct the problem as needed. • If XIDs are exchanging, and a SABME has not been received from the AS/400, check the settings of External PU Type, XID, and Control Point Name in the AS/400 and LLC-SDLC Station record.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
MASTER POLLED EARLY	75004	High	Minor	This alarm indicates that an MX25 slave station has detected that the master has polled another slave prior to it going off line.		To correct this problem, reconfigure the poll timer to a larger value. **■Note** Refer to the *Multipoint X.25 Protocol Manual* (Part Number T0103-03) for more information.
NETWORK DLCI UNASSIGNED: DLCI *(n)*	87008	Medium	Normal	This alarm indicates that a DLCI number not assigned to any station appears in a status message from the network. The DLCI is given by *(n)*.		Check that the DLCI numbers configured in the FRI stations match those provisioned by the network.
NO CONFIG FOR STN	295004	High	Critical			Contact your customer service representative if this alarm is displayed.
NO STATION FOR SMDS DESTINATION	290002	Medium	Minor			Contact your customer service representative if this alarm is displayed.
SDLC *STATION (n)* - INSUFFICIENT MEMORY TO PROTECT STATION	74019	High	Critical	This alarm indicates that an SDLC station has not received sufficient allocation of memory to enable Data Connection Protection on the station. The value *STATION (n)* identifies the SDLC station affected.	74000	The only solution to this problem is to add more memory to your Vanguard device. **■Note** Refer to the S*DLC Protocol Manual* (Part Number T0101-05) for additional information.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
SDLC-*(n) STATION (n)* - BAD FRAME LENGTH *(b)*	75001	Medium	Minor	This alarm indicates that a frame has been received with an incorrect frame length. The value *(n)* identifies the SDLC port number, *STATION (n)* identifies the station number on that port, and *(b)* indicates the length of the received frame.		To correct this problem, configure the device to send smaller frames.
SDLC-*(n) STATION (n)* - BAD FRAME TYPE *(h)*	75002	Low	Minor	This alarm indicates that a frame has been received with an unrecognizable receive control byte. The value *(n)* identifies the SDLC port number, *STATION (n)* identifies the station number on that port, and *(h)* is the hexadecimal value of that byte.		To correct this problem, check the link configuration, and ensure that the Frame Sequence is the same at both ends of that link.
SDLC-*(n) STATION (n)* - BAD N(R) *(r)(e)*	75003	Low	Minor	This alarm indicates that a frame has been received with a bad last received sequence number, or N(R). The value *(n)* identifies the SDLC port number, *STATION (n)* identifies the station number on that port, *(r)* identifies the received N(R), and *(e)* identifies the expected sequence number.		Check the K Frame Window Size Parameter, in the Port and/or Station records, to confirm that the window sizes of the Vanguard match those of the attached device. **■ Note** Refer to the *SDLC Protocol Manual* (Part Number T0101-05) for additional information.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
SDLC-*(p) STATION (n)* - FRMR *(cc)(nn)(wxyz)*	75005	Low	Minor	This message indicates that a SDLC Station has received a Frame Reject (FRMR) from an attached device. Frame rejection can be for any of these reasons: • The command field is not recognized • The data field is too long • An invalid frame sequence number is used. The value *(p)* identifies the SDLC port number, *STATION (n)* identifies the station number on that port, *(cc)* identifies the command field, *(nn)* identifies preset sequence numbers, and the *(wxyz)* field is used to identify the following: • w = an invalid command from the TPAD. • x = an invalid information field was received. • y = a received information field that was too long. • z = incorrect sequence number received.		When this alarm is displayed, you must check these SDLC parameters to ensure that they are compatible between the device and Station: • Window Size • Max. BTU Size • Device Types
STATION (n) - ADDRESS ERROR **(%02X)**	75009	Medium	Warning	This alarm indicates that an unconfigured, or unsupported, address was received by the SDLC station. The value *STATION (n)* indicates the station affected.		To correct this problem, check the address configured into the attached SDLC device.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) - CAN NOT FORWARD - STATION DISABLED	308043	Medium	Critical	This alarm indicates that a station is disabled and cannot forward the packet. The value *STATION (n)* indicates the station affected.	308000	Enable the station.
STATION (n) - CLEARING CALL, REMOTE STATION DOWN RECEIVED	344003	High	Warning	This alarm indicates that the DLCI connected to the TPA is down due to some reason. The value *STATION (n)* identifies the TPA Slot number associated with this TPA.	344000	Contact your customer service representative for additional information.
STATION (n) - CONFIGURATION ERROR:	110013	Medium	Critical	This alarm indicates that the TPAD Group Poll and Contention modes have been simultaneously enabled. The value *STATION (n)* identifies the station affected.	110000	If Contention has been enabled, the TPAD Group Poll is automatically disabled. Therefore, to correct this problem, either: • Disable the Group Poll Mode in the device record via the Device Options parameter. • Disable the Contention Mode in the Port Record.
STATION (n) - CONFIGURATION ERROR:	110014	Medium	Critical	This alarm indicates that an HPAD device has been configured with the Group Poll option. The value *STATION (n)* identifies the station affected.	110000	The Group Poll option can be configured for TPAD only. To correct this problem, disable the Group Poll option in the device record, via the Device Options parameter.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) - FRAME RECEIVED FOR DISABLED STATION: DLCI *(dddd)*	187001	Low	Minor	This alarm indicates that a frame was received for a station that has been disabled. The DLCI number in the frame is dddd. The value *STATION (n)* identifies the FRA station affected, while *(dddd)* identifies the disabled DLCI.		If the control protocol is configured to None, notify the administrator of the remote equipment that the DLCI is unavailable.
STATION (n) - HPAD STATION ACTIVE	75012	Low	Normal	This alarm indicates that the SDLC HPAD is being polled successfully. The value *STATION (n)* indicates the station affected.		This is an information message only. No corrective action is required.
STATION (n) - HPAD STATION DOWN	75010	High	Major	This alarm indicates that an SDLC HPAD is no longer in the Normal Response Mode. The value *STATION (n)* indicates the station affected.	75011	When this alarm is displayed, you should check the condition of the attached device to ensure that it is operating correctly.
STATION (n) - HPAD STATION INACTIVE	75013	Low	Minor	This alarm indicates that the SDLC HPAD is no longer being polled. The value *STATION (n)* indicates the station affected.	75012	When this alarm is displayed, you should check the condition of the attached device to ensure that it is operating correctly.
STATION (n) - HPAD STATION UP	75011	High	Normal	This alarm indicates that an SDLC HPAD is in the Normal Response Mode. The value *STATION (n)* indicates the station affected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) - INHIBITED - *(controller address) (station address)* - NO DSP CONNECTION AVAILABLE	110015	High	Critical	This alarm indicates that the number of DSP devices used character oriented serial protocols, configured on the node, exceeds the number of available DSP devices configured in the Node Record. These protocols use DSP devices: • BSTD • BSC3270 • IBM2260 • TPA_BSC3270 The value *STATION (n)* identifies the station affected while *(controller address) (station address)* identify the hexadecimal addresses.	110000	To correct this problem, increase the number of available DSP devices configured in the Node Record. This can be done via the Quantity of DSP Devices parameter.
STATION (n) - LINE	306020	High	Normal	This message indicates that the line status is UP or DOWN. The value *(cause)* identifies what the change in status involved. The value *STATION (n)* identifies the station affected.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) - LOCAL ERROR *(message)*	306019	Medium	Minor	This message informs you that a Protocol Error has occurred. In this case, the message indicates that a received packet has some sort of error associated with it. This is most likely a formatting error and, therefore, it is being discarded. The message is generated to alert you to the fact that you are receiving such packets. The message also displays an explanatory message that may include: • Retries of a particular message have been exhausted. • A message is too long. • A Receive Timeout has been detected for a particular type of packet. The value *STATION (n)* identifies the station affected.		This is an information message only. There are no corrective actions necessary.
STATION (n) - OVERSIZE FRAME FROM REMOTE	75016	Medium	Minor	This alarm indicates that a frame has been received, on an SDLC port that was longer than the frame size configured in the SDLC Port record. The value *STATION (n)* indicates the station affected.		Confirm that the attached device is configured with a frame size that is compatible with the frame size configured in the SDLC port record.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) - STATION BOOT FAILURE *(cause)*	74007	High	Normal	This alarm is displayed when one of these conditions exist: • CMEM records do not exist. • The port type is mismatch. • The port sub-type is changed. • The number of stations have been changed. • The port/station is in the disabled state. The value *STATION (n)* indicates the station that has failed to boot while *(cause)* identifies the reason for that failure.		To correct this problem, enable the port station or boot the node.
STATION (n) - STATION DISABLED	186005	High	Warning	This message indicates that a FRA Station has been disabled by a user. The value *STATION (n)* identifies the port affected.	186006	This is an information message only. No corrective action is required.
STATION (n) - STATION DOWN	306025	High	Minor	This message indicates that a station has gone down because the number of connection attempts specified has been exceeded. The value *STATION (n)* identifies the station affected.	306007	To correct this situation, check the cables, clocking, and availability of equipment.
STATION (n) - STATION DOWN	110009	High	Minor	This alarm indicates that a station has not responded to a poll. The value *STATION (n)* identifies the station number affected.	110000, 110011	Verify that the links are all intact and operational, and check the configuration for errors.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) - STATION DOWN - *(address)*	125009	High	Minor	This alarm indicates that a station has not responded to a poll. The value *STATION (n)* identifies the station number affected. The value *(address)* identifies the station address and is presented as two hexadecimal numbers representing the .	125010	Verify that the links are all intact and operational, and check the configuration for errors.
STATION (n) - STATION ENABLE FAILURE	112011	High	Normal	This message indicates that you have attempted to enable a station that is already enabled or has not been properly initialized. The value *STATION (n)* identifies the station number affected.		This is an information message only. No corrective action is required.
STATION (n) - STATION ADDRESS DUPLICATED	112014	High	Critical	This alarm indicates that more than one station, on a specific port, has the same address. The value *STATION (n)* identifies the station number affected.	112000	Change the address of one of the stations that are in conflict.
STATION (n) - STATION BOOT COMPLETE	74006	High	Normal	This message is displayed whenever a station boot operation is completed successfully. The value *station STATION (n)* indicates the station that has been booted.		This is an information message only. There are no corrective actions necessary.
STATION (n) - STATION BOOT COMPLETE	112006	High	Normal	This message indicates that a station has been successfully booted and is now ready for use. The value *STATION (n)* identifies the port number affected.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
STATION (n) - STATION BOOT COMPLETE	186007	High	Normal	This message indicates that a Frame Relay station failed to boot. The value *STATION (n)* identifies the port affected		This is an information message only. No corrective action is required.
STATION (n) - STATION BOOT FAILED	69009	High	Normal	This alarm indicates that one of these conditions exist: • CMEM records do not exist. • Port type mismatch. • Port subtype changed. • Number of stations changed. • Port or station disabled. The value *STATION (n)* indicates the station number.		To correct this problem: a) Enable the port or station. b) Remove any duplicated station addresses. c) Boot the node when complete.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) - STATION BOOT FAILURE - *(cause)*	112007	High	Normal	This alarm indicates that a user initiated station boot has failed. The value *STATION (n)* identifies the station number affected while *(cause)* indicates one of the following reasons for the failure: • There is no port record configured for the port/station that you are attempting to boot. • There is no station record present for the station that you are attempting to boot. • The station that you are attempting to boot is not fully initialized. • The station type that you are attempting to boot, does not match a station type for the specified port. • The port record for the station that you are attempting to boot has changed. • The port for the station that you are attempting to boot is disabled. • The number of stations for the specified port has changed. • The DCP level has changed.		Resolve the conflicts identified in the alarm message to correct this problem.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) - STATION BOOT FAILURE - *(cause) (Cont'd)*	112007	High	Normal	• There is a duplicate address for the station that you are attempting to boot. • Then number of PVCs or the starting PVC number for the specified MX25 station has changed. • The number of SVCs of the starting SVC number for the specified MX25 station has changed.		Resolve the conflicts identified in the alarm message to correct this problem.
STATION (n) - STATION BOOT FAILURE - *(cause)*	186008	High	Normal	This alarm indicates that a station could not be booted. The value *STATION (n)* identifies the station affected, while *(cause)* indentifies the reason for the failure.		Correct the cause of this problem. A node boot may be necessary to correct this problem.
STATION (n) - STATION BOOT FAILURE - *(cause)*	308007	High	Normal	This message indicates that there has been a failure in booting the station. The value *STATION (n)* indicates the station affected while the *(cause)* string identifies the reason for the failure.		Determine reason for failure via explanation. Correct the problem and then reboot the port.
STATION (n) - STATION BUSY-OUT COMPLETE	69017	High	Warning	This message indicates a the station has busied-out. The value *STATION (n)* indicates the station number.		Contact your customer service representative for additional information.
STATION (n) - STATION BUSY-OUT FAILURE	74017	High	Normal	This message indicates that a station has not been busied-out via the Port/Station Control Menu. The value *STATION (n)* identifies the Station affected		This is an information message only. No corrective action is required.

Alarm Text	**Trap No.**	**Priority**	**Severity**	**Description**	**Cleared By:**	**Corrective Action** *(continued)*
STATION (n) - STATION DISABLED	112008	High	Warning	This message indicates that a station has successfully been disabled. The value *STATION (n)* identifies the station number affected.	112010	This is an information message only. No corrective action is required.
STATION (n) - STATION DISABLE FAILURE	112009	High	Normal	This message indicates that you have attempted to disable a station that is already disabled or has not been properly initialized. The value *STATION (n)* identifies the station number affected.		This is an information message only. No corrective action is required.
STATION (n) - STATION DISABLE FAILURE	318007	High	Normal	This message indicates that an SPP port could not be disabled. The reason may be that the station has not been initialized, or that it is already disabled. The value *STATION (n)* indicates the station number.		If the station has not been initialized, verify the station number to be disabled.
STATION (n) - STATION DISABLE FAILURE - ALREADY DISABLED	74009	High	Normal	This message indicates that the station disable operation has failed. The value *STATION (n)* identifies the station affected.		This is an information message only. There are no corrective actions necessary.
STATION (n) - STATION DISABLED	318006	High	Warning	This message indicates that an SPP station has been successfully disabled. The value *STATION (n)* indicates the station number.	318008	This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) - STATION DOWN	68010	High	Minor	This alarm indicates that a station has gone down because the number of attempts to connect has been exceeded. The value *STATION (n)* indicates the station number.	68001	Check cables, clocking, and availability of equipment.
STATION (n) - STATION DOWN	75007	High	Minor	This message indicates that the specified station has gone down because the number of attempts to connect has been exceeded. The value *STATION (n)* indicates the station affected.	75008	To determine why this station has gone down: • Check all hardware and cables. • Verify that node clocking is correct. • Verify that all connected equipment is available and operating properly.
STATION (n) - STATION ENABLE FAILURE	318009	High	Normal	This message indicates that an SPP port could not be enabled. The reason may be that the station has not been initialized, or that it is already enabled. The value *STATION (n)* indicates the station number.		If the station has not been initialized, verify the station number to be enabled.
STATION (n) - STATION ENABLED	74010	High	Normal	This message indicates that a station is successfully disabled. The value *STATION (n)* indicates the station affected.		This is an information message only. There are no corrective actions necessary.
STATION (n) - STATION ENABLED	112010	High	Normal	This message indicates a response to a user command to enable a station. The value *STATION (n)* identifies the station number affected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) - STATION ENABLED	186006	High	Normal	This message indicates that a FRA Station has been enabled by a user. The value *STATION (n)* identifies the port affected.		This is an information message only. No corrective action is required.
STATION (n) - STATION ENABLED	318008	High	Normal	This message indicates that an SPP station has been successfully enabled. The value *STATION (n)* indicates the station number.		This is an information message only. No corrective action is required.
STATION (n) - STATION INHIBITED ADDR CONFLICT	306014	High	Critical	This is a warning message indicating that a station will not be polled because the Controller Address (ADDR CONFLICT) of that station is same as that of some other station configured on the port. The value *STATION (n)* indicates the station affected.	306000, 306007	Correct the station's Controller Address and then boot the station.
STATION (n) - STATION NOT CONFIGURED	308042	Low	Critical	This alarm indicates that a host is polling a station that is not configured on the HPAD. The value *STATION (n)* indicates the station affected.	308000	Check station address in station's configuration.
STATION (n) - STATION OPERATIONAL	110010	High	Normal	This message indicates that a station is up and operational. The value *STATION (n)* identifies the station number affected.		This messages for information purposes only. No corrective actions are required.
STATION (n) - STATION OPERATIONAL	125010	High	Normal	This message indicates that a station is up and operational. The value *STATION (n)* identifies the station number affected.		This messages for information purposes only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) - STATION REQUESTED DISCONNECT	75006	High	Minor	An SDLC controller has sent a Request to Disconnect to the TPAD. The value *STATION (n)* indicates the controller affected.		Verify that the attached SDLC equipment is available and operating properly.
STATION (n) - Station Requested Disconnect	111006	High	Minor		111008	Contact your customer service representative if this alarm is displayed.
STATION (n) - STATION STAT OVERFLow	112016	High	Warning	This message indicates that a statistic parameter has looped over the maximum counter value and started over from zero. The value *STATION (n)* identifies the station number affected.	112000	This is an information message only. No corrective action is required.
STATION (n) - STATION STATUS WARNING	318014	Medium	Warning	This SPP station was in disabled state when the node initialized. The value STATION *(n)* indicates the station number.	318000	Enable the station if it is to be used.
STATION (n) - STATION UP	75008	High	Normal	This message indicates that an MX25/SDLC station that was disconnected is now in Data Transfer state. The value *STATION (n)* indicates the station affected.		This is an information message only. No corrective action is required.
STATION (n) - STATION DISABLED	74008	High	Warning	This message indicates that a station is successfully disabled. The value *STATION (n)* indicates the station affected.	74010	This is an information message only. There are no corrective actions necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
STATION (n) - STN BOOT COMPLETE	295000	High	Normal	This message indicates that a station boot operation is completed successfully. The value *STATION (n)* indicates the station that has been booted.		This is an information message only. There are no corrective actions necessary.
STATION (n) - STN BOOT FAILURE - **%s**	295001	High	Normal			Contact your customer service representative if this alarm is displayed.
STATION (n) - STN DISABLED	295002	High	Warning	This message indicates that a station has been disabled. The value *STATION (n)* indicates the station affected.	295003	This is an information message only. No corrective action is required.
STATION (n) - STN ENABLED	295003	High	Normal	This message indicates that a station has been enabled. The value *STATION (n)* indicates the station affected.		This is an information message only. No corrective action is required.
STATION (n) - TPAD STATION ACTIVE	75014	Low	Normal	This alarm indicates that the SDLC TPAD is successfully polling an attached device. The value *STATION (n)* indicates the station affected.		This is an information message only. No corrective action is required.
STATION (n) - TPAD STATION INACTIVE	75015	Low	Minor	This alarm indicates that the SDLC HPAD is no longer successfully polling an attached device.The value *STATION (n)* indicates the station affected.	75014	When this alarm is displayed, you should check the condition of the attached device to ensure that it is operating correctly.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) - UNSUPPORTED FRAME SIZE: OPERATING WITH 1024 BYTES	74020	Medium	Minor	This message indicates that a port is booted, and the maximum configured frame size is 4K while the port driver (hardware) only supports 1K frame size. The value *STATION (n)* identifies the Station affected.	74000	Adjusting the frame size will correct this problem.
STATION (n) AUTOCALL ATTEMPTS EXHAUSTED	306018	High	Minor	This alarm indicates that the number of attempts to establish a connection using the configured Autocall mnemonic has been exceeded. The value *STATION (n)* indicates the station affected.	306000, 306007	Check the Autocall Mnemonic string for this station against the string configured in the Mnemonic Table. If there is an error in this station's Autocall mnemonic, correct it and boot the station. If the error is in the Mnemonic Table, correct it and perform a Tables Boot.
STATION (n) BYPASS STATION DOWN	87006	Medium	Warning	This alarm indicates that a FRI Bypass station is unable to pass data. The value *STATION (n)* identifies the station number affected.		To correct this problem: • Check the network connection, network status, and the status of the remote equipment for possible failure. • Check the status of the LCON, or of the onward links and equipment for possible failure, as appropriate.
STATION (n) BYPASS STATION UP	87005	Medium	Warning	This message indicates that a FRI Bypass station is able to pass data. The value *STATION (n)* identifies the station number affected.		This message is fort information purposes only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
STATION (n) DATA ERROR *(message)*	306022	Medium	Minor	This alarm indicates that a received data message is not in the correct format. The value *STATION (n)*indicates the station affected while *(message)* identifies the error message that will be sent to the Host.		This is an information message only. There are no corrective actions necessary.
STATION (n) DQ ERROR *(message)*	306021	Medium	Warning	The received message is: • Out of context. • Too short. • As an invalid format. • Contains an unknown UCN. • Has an unrecognized message code. • Has an invalid read reference number. An error indication message is built and sent to the Host with this error. The value *STATION (n)* indicates the station affected while *(message)* identifies the error message that will be sent to the Host.	306000, 306007	This is an information message only. There are no corrective actions necessary.
STATION (n) FRAME RECEIVED FOR DISABLED STATION: DLCI *(n)*	87001	Low	Major	This alarm indicates that a frame has been received from the link for a FRI station that is disabled. The value *STATION (n)* identifies the station number affected and the DLCI is given by *(n)*.		If no PVC management protocol is in use, inform the administrator for the remote node that the DLCI is not available.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) INSUFFICIENT MEMORY TO PROTECT STATION	226007	High	Warning	This alarm indicates that an LLC station did not receive enough memory allocation in order to enable Data Connection Protection at the station. The value *STATION (n)* indicates the station affected.	226000	The only solution to this problem is to add additional memory to your Vanguard device. Refer to your Vanguard Installation Guide for additional information.
STATION (n) NETWORK LINK DOWN	76007	Medium	Major	This message indicates that the QLLC station is inactive. The value *STATION (n)* identifies the station affected.	76004	Check the status of the network port to determine the cause of this alarm.
STATION (n) NETWORK LINK UP	76006	Medium	Normal	This message indicates that the QLLC station is active. The value *STATION (n)* identifies the station affected.		This is an information message only. No corrective action is required.
STATION (n) RECEIVED ERROR MSG *(message)*	306023	High	Normal	This alarm indicates that an error message has been received. The value *STATION (n)* indicates the station affected while *(message)* identifies the error message that will be sent to the Host.		This is an information message only. There are no corrective actions necessary.
STATION (n) REMOTE CALL ESTABLISHED	222005	CONN	Normal	This message indicates that a call has been established. The value *STATION (n)* indicates the station affected.		This is an information message only. There are no corrective actions necessary.
STATION (n) STATION BOOT COMPLETE	306007	High	Normal	This message indicates that a station boot operation is completed successfully. The value *STATION (n)* indicates the station that has been booted.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) STATION BUSY-OUT FAILED	69012	High	Normal	This alarm indicates that the station has been disabled or already busied-out. The value *STATION (n)* indicates the station number.		To correct this problem, enable the port first and then busy-out the port.
STATION (n) STATION DOWN	222001	Medium	Minor	This message indicates that the specified station has gone down because the number of attempts to connect has been exceeded. The value *STATION (n)* indicates the station affected.	222000	To correct this problem: • Check all hardware and cabling. • Verify that the system clocking is accurate and that all attached equipment is available and operating correctly.
STATION (n) STATION ENABLED	226004	High	Normal	This message indicates that a station has been enabled. The value *STATION (n)* indicates the station affected.		This is an information message only. No corrective action is required.
STATION (n) STATION INHIBITED - ADDRESS CONFLICT	110011	High	Critical	This alarm indicates that at least two BSTD stations have been configured with the same address. The value *STATION (n)* identifies the BSTD station affected.		To correct this problem, simply change the address of one of the configured stations in the BSTD Station Table.
STATION (n) STATION POLL RESUMED	306016	Low	Normal	This message indicates that the polling of this controller has been resumed. The value *STATION (n)* indicates the station affected.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) STATION RECEIVED A REMOTE DISCONNECT	222003	CONN	Normal	This message indicates that a remote TPAD/HPAD received an "SDLC DISCONNECT" LPDU. The host or terminal on the remote HPAD/TPAD terminated the Logical Link Session. The value *STATION (n)* identifies the affected station.		This is an information message only. There are no corrective actions necessary.
STATION (n) STATION STATUS WARNING *(cause)*	306013	High	Warning	This alarm indicates that a station is disabled during a node boot. The value *STATION (n)* indicates the station affected while *(cause)* identifies the reason for the alarm.	306000, 306007	Enable the station if required.
STATION (n) STATION UP	187011		Major	This message indicates that the FRA station is now able to pass data. The value *STATION (n)* identifies the station number affected.		This is an information message only. No corrective action is required.
STATION (n) STATION BOOT COMPLETE	88007	High	Normal	This message indicates that a FRI station boot has completed successfully. The value *STATION (n)* identifies the station number affected.		This messages for information purposes only. No corrective actions are required.
STATION (n) STATION BOOT COMPLETE	226000	High	Normal	This message indicates that a station has successfully restarted. The value *STATION (n)* indicates the station affected.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
STATION (n) STATION BOOT FAILURE *(cause)*	226001	High	Normal	This alarm indicates that one of these conditions exist: • CMEM records do not exist. • The port type is mismatch. • The port sub-type is changed. • The number of stations have been changed. • The port/station is in the disabled state. The value *STATION (n)* identifies the station that failed to boot while *(cause)* identifies the reason for that failure.		To correct this alarm, enable the port station the node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) STATION BOOT FAILURE *(cause)*	306008	High	Normal	This alarm indicates failure of the boot operation for a 3201 station. The *(cause)* of the failure is one of the following : • NO PORT RECORD - The port corresponding to the affected station has been deleted. • NO STATION RECORD - The station record corresponding to this station number has been deleted or is not configured. • PORT TYPE MISMATCH or PORT RECORD CHANGED - The configured port record is not a 3201 port. • PORT DISABLED • STATION DISABLED • # CONTROLLERS HAS CHANGED The value *STATION (n)* indicates the station affected.		Depending on the *(cause)* of the failure, these corrective actions can be taken : • NO PORT RECORD - Reconfigure the port record and retry. • NO STATION RECORD - Reconfigure the station record and retry. • PORT TYPE MISMATCH or PORT RECORD CHANGED - Reconfigure the port record and retry. • PORT DISABLED - Enable the corresponding 3201 port and retry. • STATION DISABLED -Enable this 3201 station and retry. • # CONTROLLERS HAS CHANGED - If the number of controllers changed, then this requires a node boot to take effect. If this change is not immediately desired, reconfigure the port record to the original setting for this parameter and retry.
STATION (n) STATION BOOT FAILURE - *(cause)*	88008	High	Normal	This message indicates that a FRI port boot could not be performed for the *(cause)* indicated. The value *STATION (n)* identifies the station number affected.		You must perform a node boot to correct this problem.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
STATION (n) STATION DISABLE FAILURE - ALREADY DISABLED	226003	High	Normal	This alarm indicates that the station disable operation has failed. The value *STATION (n)* indicates the station affected.		This is an information message only. No corrective action is required.
STATION (n) STATION DISABLED	69004	High	Warning	This alarm indicates that the station has been disabled. The value *STATION (n)* indicates the station number.	69005	This is an information message only. No corrective action is required.
STATION (n) STATION DISABLED	226002	High	Warning	This message indicates that a station has been disabled. The value *STATION (n)* indicates the station affected.	226004	This is an information message only. No corrective action is required.
STATION (n) STATION DISABLE FAILED	69011	High	Normal	This alarm indicates that the station has either: not been initialized or has already been disabled. The value *STATION (n)* indicates the station number.		To correct this problem, enable the station and then boot the node.
STATION (n) STATION DISABLE FAILURE *(cause)*	306010	High	Normal	This alarm is displayed when you fail in an attempt to disable a Station that is already disabled, i.e, the station has not been initialized. The value *STATION (n)* indicates the station that has failed to boot while *(cause)* identifies the reason for that failure.		To correct this alarm, enable the station and, if necessary, boot the node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) STATION DISABLED	88005	High	Warning	This message indicates that a FRI station has been disabled via the CTP. The value *STATION (n)* identifies the station number affected.		This messages for information purposes only. No corrective actions are required.
STATION (n) STATION DISABLED	306009	High	Warning	This message is displayed after a station is successfully disabled. The value *STATION (n)* indicates the station affected.	306011	This is an information message only. There are no corrective actions necessary.
STATION (n) STATION DOWN	187012		Major	This alarm indicates that the FRA station is now unable to pass data. The value *STATION (n)* identifies the station number affected.		Check the status of the remote equipment and the onward circuit (or LCON) for outages, to correct this problem.
STATION (n) STATION ENABLE COMPLETE	69005	High	Normal	This alarm indicates that the station has been enabled. The value *STATION (n)* indicates the station number.		This is an information message only. No corrective action is required.
STATION (n) STATION ENABLE FAILED	69010	High	Normal	This alarm indicates that one of these conditions exist: • The station has already been enabled. • The port is busied-out. • The station address has been duplicated. The value *STATION (n)* indicates the station number.		To correct this problem, enable port and remove any duplicated station address.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
STATION (n) STATION ENABLE FAILURE *(cause)*	74011	High	Normal	This alarm indicates that a station is already in the enabled state or is not yet initialized. The value *STATION (n)* indicates the station affected while *(cause)* identifies the reason for the failure.		If the station is not yet initialized, boot the node.
STATION (n) STATION ENABLE FAILURE *(cause)*	306012	High	Normal	This alarm indicates that the station is already in the enabled state or is not yet initialized. The value *STATION (n)* indicates the station affected while *(cause)* identifies the reason for the failure.		Boot the node if the station is not yet initialized
STATION (n) STATION ENABLE FAILURE - ALREADY ENABLED	226005	High	Normal	This message indicates that a station enable operation has failed. The value *STATION (n)* indicates the station affected.		This is an information message only. No corrective action is required.
STATION (n) STATION ENABLED	88006	High	Normal	This message indicates that a FRI station has been enabled via the CTP. The value *STATION (n)* identifies the station number affected.		This messages for information purposes only. No corrective actions are required.
STATION (n) STATION ENABLED	306011	High	Normal	This message is displayed after a station is successfully disabled. The value *STATION (n)* indicates the station affected.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) STATION MNEMONIC ERROR	306017	Low	Critical	This alarm indicates that an error occurred while parsing the Host mnemonic string. The value *STATION (n)* indicates the station affected.	306000, 306007	To correct this alarm, check the station's Autocall Mnemonic against the string configured in the Mnemonic Table, and perform the required action: a) If there is an error in the station's Autocall Mnemonic, correct it and boot the station. b) If the error is in the Mnemonic Table, correct it and perform a Table Boot.
STATION (n) STATION POLL SUSPENDED *(cause)*	306015	Low	Warning	This message indicates that the polling of this controller has been suspended. The value *STATION (n)* indicates the station affected while *(cause)* will identify: • BLOCKED - Polling has been suspended because of flow control. • INTR - Polling has been suspended because an interrupt packet was received from the host. • CONN - Polling has been suspended until the connection to the host has been established. • ITC - An Invitation To Clear message has been received.	306016	This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) STATION TIMed OUT	222002	CONN	Minor	This message indicates that a SLAC station has not received any data from the station it is logically linked to for a period of time equal to T1 multiplied by N2. This time is configured in the Profile table for this station. The value *STATION (n)* indicates the station affected.		Check the Profile table for this station.
STATION (n) STATION UP	222000	Medium	Normal	This message indicates that an MX25/SDLC station, that was disconnected, is now in the Data Transfer state. The value *STATION (n)* indicates the station affected.		This is an information message only. There are no corrective actions necessary.
STATION (n) STATION UP	306024	High	Warning	This message indicates that a station has been successfully restarted. The value *STATION (n)* identifies the restarted station.		This is an information message only. There are no corrective actions necessary.
STATION (n) SUSPICIOUS CONFIGURATION - ZERO VOICE BANDWIDTH AND VOICE RELAY CIRCUITS PRESENT	88011	Medium	Minor	This message indicates that the configuration of the indicated Voice-related parameters may be inconsistent. The value *STATION (n)* identifies the station number affected.	88000	Correctly configure the Voice-related parameters.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
STATION (n) SUSPICIOUS CONFIGURATION - FRAME SEGMENTER ENABLE AND VOICE BANDWIDTH IS ZERO	88014	Medium	Minor	This alarm indicates that the configuration of the indicated Voice-related parameters may be inconsistent. The value *STATION (n)* identifies the station number affected.		Correctly configure the Voice-related parameters.
STATION (n) TPAD STATION DOWN	76005	High	Minor	This message indicates that the TPAD station is not in the Normal Response Mode. The value *STATION (n)* identifies the station affected.	76004	Check the condition of all attached controllers or devices to determine the cause of this alarm.
STATION (n) TPAD STATION UP	76004	High	Minor	This message indicates that the TPAD station is in the Normal Response Mode. The value *STATION (n)* identifies the station affected.		This is an information message only. No corrective action is required.
STATION (n)- STATION BOOT COMPLETE	308006	High	Normal	This message indicates that a station has been booted. The value *STATION (n)* indicates the station affected.		This is an information message only. There are no corrective actions necessary.
STATION (n)- STATION BUSY-OUT	308016	High	Normal	This message indicates that a station has been busied out from the CTP. The value *STATION (n)* indicates the station affected.		This is an information message only. There are no corrective actions necessary.
STATION (n)- STATION DISABLED	308008	High	Warning	This message indicates that a station has been disabled. The value *STATION (n)* indicates the station affected.	308010	This is an information message only. There are no corrective actions necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
STATION (n)- STATION ENABLE FAILURE - *(cause)*	308011	High	Normal	This message indicates that there has been a failure while enabling the station. The value *STATION (n)* indicates the station affected while the *(cause)* string identifies the reason for the failure.		Determine reason for failure via explanation. Correct the problem and then reboot the port.
STATION (n)- STATION ENABLED	308010	High	Normal	This message indicates that a station is enabled. The value *STATION (n)* indicates the station affected .		This is an information message only. There are no corrective actions necessary.
STATION (n)- STATION DISABLE FAILURE - *(cause)*	308009	High	Normal	This message indicates that there has been a failure while disabling the station. The value *STATION (n)* indicates the station affected while the *(cause)* string identifies the reason for the failure.		Determine reason for failure via explanation. Correct the problem and then reboot the port.
STATION ADDRESS DUPLICATED	69008	High	Critical	This alarm indicates that an MX25 port has been duplicated following a port or node boot.	69000	Remove duplicated station addresses, enable and boot the port.
STATION BUSY-OUT	74016	High	Warning	This message indicates that a station has been successfully busied-out via the Port/Station Control Menu.		This is an information message only. No corrective action is required.
STATION INHIBITED - *(s1) (s2)* - ADDRESS CONFLICT	125011	High	Critical	This alarm indicates that at least two stations have the same address. The two stations involved are identified by the values *(s1)* and *(s2)*.	125000	To correct this problem, change the configuration.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TWO MASTERS ON MULTIPOINT LINK	68002	High	Critical	This alarm indicates that two masters stations have been configured for a single multipoint link.		Reconfigure one end to be a Slave Link. **■Note** Refer to the *Multipoint X.25 Protocol Manual* (Part Number T0103-03) for additional information.
TWO MASTERS ON MULTIPOINT LINK - *STATION (n)*	68001	High	Normal	This alarm indicates that an MX25/SDLC station that was disconnected is now in the Data Transfer state. The value *STATION (n)* indicates the station number.		This is an information message only. No corrective action is required. **■Note** Refer to either the *Multipoint X.25 Protocol Manual* (Part Number T0103-03) or *SDLC Protocol Manual* (Part Number T0101-05) for additional information.
WRONG MESSAGE ADDRESS	308039	Medium	Minor	This alarm indicates that the Terminal ID, on the received message from an HPAD port, does not match the configured remote Terminal ID.	308000	Check the Remote address parameter in the GSC station configuration.
XDLC - *(p) (n)* - ADDRESS ERROR (a)	111004	Medium	Warning	This alarm indicates that, for a specific port and station, a frame was received with an incorrect address field. The values *(p)* and *(n)* identify the port and station (respectively) affected by this alarm, while (a) identifies the incorrect address.		To correct this problem: a) Verify that the attached device is configured correctly. b) Boot the attached device. c) Boot the affected station and/or port.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
XDLC - *(p) (n)* - BAD FRAME LENGTH *(id)*	111001	Medium	Minor	This alarm indicates a frame was received with a frame length that is either larger than the configured maximum, or less than the minimum frame size. The values *(p)* and *(n)* identify the port and station (respectively) affected by this alarm, while *(id)* identifies the frame type ID.		To correct this problem: • Verify that the port parameter "Maximum Frame Size" is configured to the appropriate value. Note that this parameter is effective for SDLC station types only. • Verify that the attached device is configured correctly
XDLC - *(p) (n)* - BAD FRAME TYPE *(id)*	111002	Low	Minor	This alarm indicates that, for a specific port and station, a frame was received that is invalid for the given protocol state, or a frame was received that is unrecognizable. The values *(p)* and *(n)* identify the port and station (respectively) affected by this alarm, while *(id)* identifies the frame type ID.		To correct this problem: a) Verify that the attached device is configured correctly. b) Boot the attached device. c) Boot the affected station and/or port.
XDLC - *(p) (n)* - BAD N(R) *(n)*	111003	Low	Minor	This alarm indicates that, for a specific port and station, a frame was received out of sequence. The values *(p)* and *(n)* identify the port and station (respectively) affected by this alarm, while *(n)* identifies the frame sequence number.		To correct this problem: a) Boot the attached device. b) Boot the affected station and/or port.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
XDLC - *(p) (n)* - FRMR *(f) (ps) (d)*	111005	Low	Minor	This alarm indicates that, for a specific port and station, a frame reject was generated. The values *(p)* and *(n)* identify the port and station (respectively) affected by this alarm, while *(f) (ps) (d)* identifies the frame type, protocol state, and debug information respectively.		To correct this problem: a) Verify that the attached device is configured correctly. b) Boot the attached device. c) Boot the affected station and/or port.
XDLC - *(p) (n)* - MX25 STATION DOWN	111007	High	Major	This alarm indicates that, for a specific port and station, the station has been declared Down. This is generally due to protocol reasons. The values *(p)* and *(n)* identify the port and station (respectively) affected by this alarm.	111008	To correct this problem: a) Verify that the attached device is configured correctly. b) Boot the attached device. c) Boot the affected station and/or port.
XDLC - *(p) (n)* - MX25 STATION UP	111008	High	Normal	This message indicates that, for a specific port and station, the MX25 station has been declared Up and is active. Values *(p)* and *(n)* identify the port and station (respectively).		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
XDLC - *(p) (n)* - OVERSIZE FRAME FROM REMOTE	111013	Medium	Minor	This message indicates that, for a specific port and station, a Network Frame was received with a frame length that is either larger or smaller than the configured maximum. The values *(p)* and *(n)* identify the port and station (respectively) affected by this alarm. **■Note** This parameter is effective for SDLC station types only.		Verify that the port parameter Maximum Frame Size is configured to the appropriate value.
XDLC - *(p) (n)* - STAT OVERFLow	111010	High	Warning	This message indicates that, for a specific port and station, a statistic parameter has looped over the maximum counter value and started over from zero. The values *(p)* and *(n)* identify the port and station (respectively) affected by this alarm.		This is an information message only. No corrective action is required.
XDLC - *(p) (n)* - TPAD STATION ACTIVE	111011	Low	Normal	This message indicates that, for a specific port and station, a station has become active. The values *(p)* and *(n)* identify the port and station (respectively) affected by this alarm.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
XDLC - *(p) (n)* - TWO MASTERS ON MULTIPOINT LINK	111009	High	Critical	This alarm indicates that, for a specific port and station, there are two "master" stations polling on the same physical link. The values *(p)* and *(n)* identify the port and station (respectively) affected by this alarm.	111008	Verify that there is only one "master" station polling on the link.
XDLC - *(p) (n)* - TPAD STATION INACTIVE	111012	Low	Minor	This message indicates that, for a specific port and station, a station has become inactive. The values *(p)* and *(n)* identify the port and station (respectively) affected by this alarm.	111011	This is an information message only. No corrective action is required.

Chapter 4
Channel Alarms and Reports

Introduction

This chapter describes those alarms and reports that are generated due to channel activity on a port on a Vanguard node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
%s CONNECTED TO MAIN CHANNEL	115005	High	Normal			Contact your customer service representative if this alarm is displayed.
%s FAILED MAIN CHANNEL CONNECT	115004	High	Major		115005	Contact your customer service representative if this alarm is displayed.
%s - NCI CHANNEL UTILIZATION >100%%	255002	Medium	Warning		255000	Contact your customer service representative if this alarm is displayed.
%s CONNECTED TO MAIN CHANNEL	116004	High	Normal			Contact your customer service representative if this alarm is displayed.
%s FAILED MAIN CHANNEL CONNECT	116003	High	Major		116004	Contact your customer service representative if this alarm is displayed.
%s LOST MAIN CHANNEL CONNECTION	115006	High	Major		115005	Contact your customer service representative if this alarm is displayed.
BAD P(K)	46003	Low	Minor	This alarm indicates that the packet level window has been exceeded on the link and the far end channel.	46000	Check the configuration to be sure the Packet Window sizes match at both ends.
BRI - X.25 OVER D CHANNEL ERROR:	241012	High	Warning	This alarm indicates that a Packet D channel error has occurred.		Evaluate the code to determine the type of error.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
BROADCAST OVERRUN	46010	Low	Major	This alarm indicates that broadcast data sent to this channel, or port, has been lost.	46000	Decrease the amount of broadcast data.
CHANNEL (c) - CHANNEL BOOT COMPLETE	245000	High	Normal	This message indicates that a BRI channel has been booted. The value *CHANNEL (c)* identifies the channel number.		This is an information message only. There are no corrective actions necessary.
CHANNEL (c) - CHANNEL BOOT FAILURE - *(cause)*	245001	High	Normal	This message indicates that an internal error occurred when booting a BRI channel. The value *CHANNEL (c)* identifies the channel number while *(cause)* identifies the reason for the failure.		Evaluate the *(cause)* string to determine why the channel boot failed.
CHANNEL (c) - CHANNEL DISABLED	245004	High	Warning	This message indicates that a channel is disabled. The value *CHANNEL (c)* identifies the channel number.	245009	This is an information message only. There are no corrective actions necessary.
CHANNEL (n) - CHANNEL ENABLED,	245009	High	Normal	This message indicates that a channel enable command was successful. The value *CHANNEL (n)* identifies the channel number.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
CHANNEL *(n)* - CHANNEL RESET RECEIVED	46002	Low	Minor	This alarm indicates that a RESET packet was received. All data within the node on this channel was discarded. The value *CHANNEL (n)* indicates the channel number.	46000	Take corrective action based on the cause and diagnostic codes in the Reset packet. These can be obtained either from the end device (APAD port, etc.) or by monitoring the X.25 link. **■ Note** Refer to the X.25 Configuration Basics Manual, in the *Vanguard Basic Protocols Manual* (Part Number T0106), for additional information.
CHANNEL (n) - CHANNEL STATUS WARNING - *(cause)*	245008	Low	Warning	This warning message is displayed during channel initialization. The value *CHANNEL (n)* identifies the channel number while *(cause)* identifies the reason for the warning.	245000	Evaluate the (cause) to determine what the best solution to this problem.
CHANNEL (n) - CHANNEL UTILIZATION > THRESHOLD	245011	Medium	Warning	This message indicates that data flowing through a channel has exceeded the warning threshold. The value *CHANNEL (n)* identifies the channel number.	245000	This is an information message only. There are no corrective actions necessary.
CHANNEL *(n)* - NO RESPONSE	46001	CONN	Warning	This alarm indicates that a channel has not received a call accept packet from the destination, in response to its call request packet, within the prescribed time limit. The value *CHANNEL (n)* indicates the channel number.	46000	Check to see if the destination site is down.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
CHANNEL *(n)* FRAME SEQUENCING OVERRIDE	275000	Low	Normal	This alarm indicates that the frame sequencing, at an X.25 port which is connected to the D channel on an ISDN line, is not set to EXT. The value *CHANNEL (n)* identifies the channel affected.		Reconfigure the Frame Sequence Counting parameter from NOMR to EXT.
CONFIGURED PKT SIZE > MAX ALLOWED ISDN D-CHANNEL	51006	Low	Critical	This message indicates that the packet size configured in the X.25 port record, is larger than the maximum packet size allowed on an ISDN D channel. The packet size is internally being set to the largest size supported by the D channel.	51000	This is an information message only. No corrective action is required.
DC - **%s** CONFIGURATION IS INCORRECT	248015	High	Critical	This alarm indicates that Data Configuration has been enabled for a connection where the network port is not configured as "NP".		To correct this problem, configure the network port as "NP".
DC - ABNORMAL CLEAR FLUSH FROM NS: Event=**%d**, State=**%d**, Chan_ID=**%d**	248007	High	Warning	This alarm indicates that a clear has been issued to DC in wrong state.		Contact your customer service representative if this alarm is displayed.
DC - ABNORMAL COMMAND ID FROM NS: Command_ID = *(id)*	248013	High	Warning	This alarm indicates that an invalid Data Compression command has been received. The value *(id)* identifies the command involved.		Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DC - CALL REQUEST ORIGINATOR IS NOT CONFIGURED FOR DATA COMPRESSION - *CHANNEL (n)*	248011	High	Warning	This alarm indicates that either a call originator is not configured for data compression or the network could not pass facilities. If this occurs, the call is cleared by the destination node.The value *CHANNEL (n)* identifies the channel affected.		To correct this problem, configure both ends of the connection for same data compression value.
DC - *CHANNEL (n)* CLEARED THE CALL DURING SRC NEGOTIATION, SAVED FACILITY WAS *(b)* CORRUPTED CONTROL BLOCK	248012	High	Major	This alarm indicates that the negotiate facility, that is saved in the control block at the source node, has been corrupted for the specified end point. The value CHANNEL (n) identifies the channel/end point affected while (b) identifies the facility saved.		Contact your customer service representative if this alarm is displayed.
DC - *CHANNEL (n)* IS CONNECTED TO ANOTHER AP, COMPRESSION IS NOT ALLOWED	248009	High	Warning	This message indicates that both source and destination channels are configured as “AP”, a configuration not supported by Data Compression. When Data Compression is configured, the network port must be configured as “NP”. The value *CHANNEL (n)* identifies the channel affected.		To correct this problem perform either of these: • Disable Data Compression on both end points. • Configure the network port as “NP”.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DC - *CHANNEL (n)* RECEIVED NEGOTIATE FACILITY IN CALL REQUEST AND IS CONFIGURED AS FORCE ON	248005	High	Warning	This alarm indicates that a call request has been received by a channel for a destination to which Data Compression is configured for "Force On". The value *CHANNEL (n)* identifies the channel affected, for example LCON-1 or X25-1(1).		Change the configuration for data compression level such that both end points are configured the same.
DC - CHANNEL UNAVAILABLE, CALL REJECTED FOR *(cause)*	248004	High	Minor	This alarm indicates that a data compression channel was unavailable when a call was received. The call has been rejected for the reason indicated by the value *(cause)*.		Correct the problem, as indicated in the *(cause)*, and place the call again.
DC - CHANNEL UNAVAILABLE, PVC *CHANNEL (n)* DID NOT GET CONNECTED WITH DATA COMPRESSION	248010	High	Warning	This alarm indicates that a PVC connection that is configured for Data Compression came up without Data Compression due to unavailable Data Compression resources. The value *CHANNEL (n)* identifies the channel affected.		To correct this problem: • Verify that the number of end points configured for Data Compression do not exceed the number of DC channels available. • Check that the Data Compression hardware is operational. **■ Note** If the Data Compression hardware has failed, consult your customer service representative.
DC - DATA COMPRESSION HEADER ERROR, AP=**%s**, NP=**%s**	248016	High	Minor	This alarm indicates that Data Compression is not configured properly. Data Compression is enabled only at one end of the connection.		To correct this problem, configure both ends of the connection for same data compression value.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
DC - DATA COMPRESSION DISABLED, DSP DOWNLOAD FAILURE, STATUS = **%d**	248014	High	Critical	This alarm indicates that a failure was detected while downloading DSP; Data Compression is disabled.		Contact your customer service representative if this alarm is displayed.
DC - DC HANDLER GENERAL INIT FAILURE	248018	High	Critical	This alarm indicates that the initialization of Data Compression handler software has failed.		Contact your customer service representative if this message is displayed.
DC - LOST/ PENDING CALL CLEAR IN EP Q: Event=**%d**, State=**%d**, Chan_ID=**%d**	248008	High	Warning	This message indicates that a clear request is lost or pending in the EP queue. Could be as a result of queue overflow.		Contact your customer service representative if this alarm is displayed.
DC - NODE CONFIGURATION FOR DATA COMPRESSION CHANNELS DIFFERS CMEM. MAX DC CHANNELS=*(n)*	248017	High	Warning	This alarm indicates that the number of DC Channels, configured in CMEM, is greater than the number of channels supported by the Data Compression hardware, i.e., the default number of channels have been allocated. The value *(n)* identifies the maximum number of compression channels that can be configured.		To correct this problem: a) Reconfigure the parameter number of Data Compression Channels to match the Data Compression Hardware. b) Boot the node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DC - PVC MISCONFIGURED, *CHANNEL (n)* IS AN AP CONNECTING TO ANOTHER AP	248006	High	Critical	This alarm indicates that both a nodes source and destination channels are configured as “AP” for PVC. Data Compression does not support this type of configuration. When Data Compression is configured, the network port must be configured as “NP”. Call is up without Data Compression. The value *CHANNEL (n)* identifies the channel affected.		To correct this problem, disable Data Compression for this connection or configure the network port as “NP”.
ERROR ON CHANNEL *(n)* - *(cause)*	281008	High	Critical	The report indicates that either: • A communication error has occurred between the motherboard and the DSPM card. • The node is running low on data buffers.		This is an information message only. No corrective action is required.
ISDN SIGNALING MESSAGE RECEIVED FOR CHANNEL **%d**	283022	High				Contact your customer service representative if this alarm is displayed.
ISDN SIGNALING MESSAGE RECEIVED FOR CHANNEL **%d**	283023	High				Contact your customer service representative if this alarm is displayed.
LOST MAIN CHANNEL CONNECTION	116005	High	Major		116004	Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
MUX,**%s** DIALING TO **%s** ON BRI INT. **%d** **%s** CHANNEL	278012	Conn	Normal			Contact your customer service representative if this alarm is displayed.
MUX,INCOMING CALL **%s** ON BRI INT. **%d** B%1d CHANNEL	278013	Conn	Normal			Contact your customer service representative if this alarm is displayed.
NO CHANNELS CONFIGURED	245012	High	Critical	This message indicates that during port initialization no channel records were found in CMEM.	245000	Create channel records.
NS RUN-TIME ERROR - CHANNEL OR FEATURE REGISTERED TWICE	229004	High	Critical			Contact your customer service representative if this alarm is displayed.
NS RUN-TIME ERROR - NO AVAILABLE NS CHANNELS	229003	High	Critical			Contact your customer service representative if this alarm is displayed.
PRI-**%d** - D CHANNEL ESTABLISHING	283024	High				Contact your customer service representative if this alarm is displayed.
PRI-**%d** - D CHANNEL UP	283018	High				Contact your customer service representative if this alarm is displayed.
PRI-**%d** - D CHANNEL DOWN	283019	High				Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PRI-**%d** - D CHANNEL RESTARTED, ALL CALLS DROPPED	283028	High				Contact your customer service representative if this alarm is displayed.
PRI-**%d**B**%d** - B CHANNEL DOWN	283021	High				Contact your customer service representative if this alarm is displayed.
PRI-**%d**B**%d** - B CHANNEL UP	283020	High				Contact your customer service representative if this alarm is displayed.
PVC DUPLICATED IN PVC TABLE	16002	Medium	Critical	This alarm indicates that a PVC channel is configured in more than one PVC Table entry. All PVC channel entries, except the first entry, are ignored.		Check the PVC Table and remove or change any duplicated table entries. **■ Note** Refer to the Vanguard Applications Ware Documentation Set for additional information.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PVC NOT CONNECTED TO *(des)* - *(cause)*	16003	Medium	Critical	This alarm indicates one of two possible problems: • SOURCE UNAVAILABLE - This alarm indicates that the source PVC channel is already connected and therefore unavailable to be connected to this destination. • DEST UNAVAILABLE - This alarm indicates that the destination PVC channel is already connected or is not named correctly. The string *(des)* indicates the destination to which the call was made.		Complete these steps to correct this problem: a) Configure the PVC channel (which is either a port or a station) and perform the appropriate boot procedure. b) Check the name of the PVC channel and correct if necessary.
SOURCE *(c)* - PVC NOT CONNECTED TO *(des)* - *(cause)* SOURCE UNAVAILABLE *(Continued)*	16003	Medium		The value *(c)* identifies the source address, *(des)* identifies the destination address, and *(cause)* indicates one of these problems: a) SOURCE UNAVAILABLE - This alarm indicates that the source PVC channel is already connected and therefore unavailable to be connected to this destination. b) DEST UNAVAILABLE - This alarm indicates that the destination PVC channel is already connected or is not named correctly.		Perform the appropriate corrective action based on the displayed cause: a) Check the channel statistics to ensure that the source is not already connected to another channel. b) Verify that the PVC channel is properly named and then check that the destination PVC channel is not already connected.

Chapter 5
Session Alarms and Reports

Introduction

This chapter describes those alarms and reports that are generated due to session activity on a Vanguard node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
SESSION (s) (p) - NON-RECOVERABLE INBOUND ERROR	57005	High	Major	This alarm indicates that a session has been disconnected due to a non-recoverable inbound error. The value *SESSION (s)* indicates which session has failed while *(p)* indicates which protocol was responsible for the error.	57000	Check the protocol sequence, as indicated in the message. **■ Note** Refer to the Vanguard Applications Ware Documentation Set for additional information.
SESSION (s) (p) - NON-RECOVERABLE OUTBOUND ERROR	57006	High	Major	This alarm indicates that a session has been disconnected due to a non-recoverable inbound error. The value *SESSION (s)* indicates which session has failed while *(p)* indicates which protocol was responsible for the error.	57000	Check the protocol sequence, as indicated in the message. **■ Note** Refer to the Vanguard Applications Ware Documentation Set for additional information.
LLC LT: SESSION NOT STARTED - *(cause)* LOC MAC/ SAP *(a)(p)*, REM MAC/SAP *(a)(p)*	155001	Medium	Minor	This message indicates that the LLC session failed to start due to the *(cause)* number listed in the report message. The value *(a)* identifies the MAC Address, and *(p)* identifies the Service Access Point.	155002	Refer to the IP Routing manual, in the *IP and LAN Feature Protocols Manual* (Part Number T0100) for cause code information.
LLC LT: SESSION *(n)* STARTED -LOC MAC/SAP *(a)(p)*, REM MAC/SAP *(a)(p)*	155002	Medium	Normal	This message indicates that an LLC session has started. The value *(n)* identifies the session number, *(a)* identifies the MAC Address, and *(p)* identifies the Service Access Point.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
LLC LT: SESSION *(n)* TERMINATED *(cause)* LOC MAC/ SAP *(a)(p)*, REM MAC/SAP *(a)(p)*	155003	Medium	Normal	This message indicates that an LLC session has been terminated. The value *(n)* identifies the session number, *(cause)* indicates the cause of the termination, *(a)* identifies the MAC Address, and *(p)* identifies the Service Access Point.		Refer to the IP Routing manual, in the *IP and LAN Feature Protocols Manual* (Part Number T0100) for cause code information.
(s) LU-LU SESSION CLEARED, CLEARING SVC	315009	Low	Normal	This alarm indicates the session between the primary and secondary LU has been cleared. The value *(s)* identifies the TPA-SDLC slot number affected.		The session may have been cleared because either: • The connection between TPA-SDLC and SDLC TPAD is cleared. • Data transfer did not take place during the configured period causing the Idle Timer to expire.
(s) PU SESSION CLEARED, CLEARING SVC	315010	Low	Normal	This message indicates the session between the TPA-SDLC and the terminal has been disconnected. The value *(s)* identifies the TPA-SDLC slot number affected.		The session may have been cleared because either: • The connection between TPA-SDLC and SDLC TPAD is cleared. • Data transfer did not take place during the configured period causing the Idle Timer to expire.
(s) PU SESSION ACTIVATED	315011	Low	Normal	This message indicates that the PU-PU session, between the TPA-SDLC and the attached terminal, is up. The value *(s)* identifies the TPA-SDLC slot number affected.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
(s) LU SESSION ACTIVATED	315012	Low	Normal	This message indicates that the session between primary and secondary LU is up. The value *(s)* identifies the TPA-SDLC slot number affected.		This is an information message only. There are no corrective actions necessary.
SESSION IS IN PROGRESS WITH SLOT *(s)*	317010	Medium	Normal	This message indicates that the destination TPDU Router slot session is in progress. The value *(s)* indicates the destination TPDU slot address.		This is an information message only. There are no corrective actions necessary.
INVALID SESSION MESSAGE IN IDLE STATE FROM SLOT *(s)*	317011	Medium	Minor	This message indicates that out-of-sequence Session messages have been received in IDLE state (Internal State Machine error). The value *(s)* indicates the slot affected.		This is an information message only. There are no corrective actions necessary.
SESSION ABORTED - INVALID SESSION MESSAGE	317012	Medium	Major	This report indicates that an invalid message was received while the Session setup was in progress (for example, Session Open.		This is an information message only. There are no corrective actions necessary.
SESSION ABORTED *(s)* - GOT SESSION CLOSE	317013	Medium	Normal	This message indicates that the originator TPDU Router slot has closed the Session. The value *(s)* indicates the slot affected.		Check the link to the originating TPDU Router slot. **■ Note** Refer to the TPDU Protocol Manual in the *Vanguard Applications Ware Basic Protocols Manual* (Part Number T0106) for additional information.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
SESSION ABORTED *(s)* - GOT INVITATION TO CLR	317014	Medium	Normal	This report indicates that the Originator Slot (the identification sting is displayed in the report) requested the destination Slot to Clear the Session. The value *(s)* indicates the slot affected.		This is an information message only. There are no corrective actions necessary.
TPA (type)-(s1) - SESSION ABORTED *(s2)* - GOT ILLEGAL MESSAGE	317015	Medium	Normal	This alarm indicates that a TPA received an unsupported or an illegal message. The value *(type)* identifies which type of TPA is involved, (*s1)* indicates the initiating TPA slot, and (s2) indicates that TPA slot that received the message.		This is an information message only. There are no corrective actions necessary.
TPA (type)-(s1) - SESSION ABORTED *(s2)* - DATA WHEN OPENING SLOT	317016	Medium	Normal	This message indicates that a TPA received data packets while it was opening a session with the adjacent TPA. The session will be aborted. The value *(type)* identifies which type of TPA is involved, (*s1)* indicates the initiating TPA slot, and (s2) indicates that TPA slot that received the message.		This is an information message only. There are no corrective actions necessary.
SESSION ABORTED *(s)* - GOT CALL CLEAR	317017	Medium	Major	This message indicates that a Call Clear was received, while the Session was being established between the TPDU Router slots. The value *(s)* indicates the slot affected.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
SESSION ABORTED *(s)* - GOT CALL REQUEST	317018	Medium	Major	This message indicates that a Call Request was received, from the Destination Slot, while the session was being established. The value *(s)* indicates the slot affected.		This is an information message only. There are no corrective actions necessary.
SESSION ABORTED *(s)* - GOT CALL ACCEPT	317019	Medium	Major	This message indicates that a Call Accept packet was received when the Session was being established with the adjacent TPDU Router slot. The value *(s)* indicates the slot affected.		This is an information message only. There are no corrective actions necessary.
SESSION ABORTED *(s)* - GOT DATA FROM DEVICE WHILE NOT CONNECTED	317020	Medium	Normal	This message indicates that the TPDU destination address is configured incorrectly and that data is being received while the session is being established. The value *(s)* indicates the slot affected.		Correct the configured Destination Address in the TPDU Router slot Configuration. **■ Note** Refer to the TPDU Feature Protocol Manual in the *Vanguard Applications Ware Basic Protocols Manual* (Part Number T0106) for additional information.
SESSION CLOSED *(s)*	317021	Medium	Normal	This message indicates that a Session is closed between the TPDU Router slots. The value *(s)* indicates the slot affected.		This is an information message only. There are no corrective actions necessary.
SESSION ESTABLISHED WITH SLOT *(s)*	317022	Medium	Major	This message indicates that a Session has been established with the Destination Slot. The value *(s)* indicates the slot affected.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DATA IN IDLE STATE FROM SLOT *(s)*	317023	Medium	Major	This message indicates that the TPDU destination address is configured incorrectly and that a data packet is received from the adjacent PAD before the session is established. The value *(s)* indicates the slot affected.		Correct the configured Destination Address in the TPDU Router slot Configuration. **Note** Refer to the TPDU Feature Protocol Manual in the *Vanguard Applications Ware Basic Protocols Manual* (Part Number T0106) for additional information.
SESSION CLOSED *(s)* - GOT CALL REQUEST	317024	Medium	Normal	This message indicates that a Call Request packet was received from an adjacent PAD that is connected to a TPDU slot that is in the data transfer state. The value *(s)* indicates the slot affected.		This is an information message only. There are no corrective actions necessary.
SESSION CLOSED *(s)* - GOT CALL ACCEPT	317025	Medium	Normal	This message indicates that a Call Accept packet was received from an adjacent PAD that is in the data transfer state. The value *(s)* indicates the slot affected.		This is an information message only. There are no corrective actions necessary.
TPA (type)-(s1) - SESSION CLOSED *(s2)* - GOT ILLEGAL MESSAGE	317026	Medium	Normal	This alarm indicates that the TPA received an unsupported/illegal message. The session will be closed. The value *(type)* identifies which type of TPA is involved, (*s1)* indicates the initiating TPA slot, and (s2) indicates that TPA slot that received the message.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TPA (type)-(s) - PACKET ALLOCATION FAILED	317027			This alarm indicates that the internal buffer pool is empty. The value *(type)* identifies which type of TPA is involved while *(s)* identifies the slot affected.		To correct this problem, increase the DRAM size to have more buffer pool.
SESSION CLOSED *(s)* - GOT INVALID SESSION MESSAGE	317029	Medium	Major	This message indicates that Session Control messages are received in Session Data transfer state. The value *(s)* indicates the slot affected.		This is an information message only. There are no corrective actions necessary.
DISCARDED - SESSION MESSAGE FROM SLOT *(s)*	317030	Medium	Minor	This message indicates that session control messages are being received from the TPDU Router slot for which the session is not established. The value *(s)* indicates the slot affected.		Check the TPDU Router Slot configuration. **■ Note** Refer to the TPDU Protocol Manual in the *Vanguard Applications Ware Basic Protocols Manual* (Part Number T0106) for additional information.
TPA (type)-(s) - SESSION STATUS MESSAGE COULDN'T SEND TO DEVICE	317031	Medium	Major	This message, which should not normally be generated, indicates that the internal queue is full. The value *(type)* identifies which type of TPA is involved while *(s)* identifies the slot affected.		This is an information message only. There are no corrective actions necessary. **■ Note** Contact your customer service representative if this message is displayed.
ESTABLISHED ENCRYPTION SESSION	379002	Medium		This message indicates that a data encryption session now exists between nodes		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
CANNOT CREATE ENCRYPTION SESSION *(cause)*	379003	High		This alarm indicates, via the *(cause)* field, that one of these problems exists: • ENCRYPTION IS DISABLED: encryption hardware is present in the node but that the encryption feature has not been enabled. • NO FREE CHANNEL: Data encryption resources are unavailable and, as a result, a the current call has been cleared. This is usually an indication that you have attempted to use more encryption channels than what is currently available. • CANNOT FIND BASE KEY IN PROFILE: Indicates that the Base Key specified in an Encryption Profile is not configured.		Complete the following actions for the cause indicated: **Note** Refer to the *Data Encryption Feature Protocol Manual* (Part Number T0103-09) for additional configuration information when correcting this problem. • You must ENABLE the 'Encryption Parameters' record, via the CTP, and then boot the node. • Try to increase the number of data encryption channels in the "Encryption Parameters" record. Consult your customer service representative to determine if you need to purchase a licence for additional number of channels • Configure the required Base Key or change the Base Key specified in the encryption profile

Chapter 6
DEBUG Alarms and Reports

Introduction

This chapter describes those alarms and reports that are generated by the Vanguard Applications Ware when the DEBUG mode of operation is used.

It is not normally recommended that Vanguard products be run in the DEBUG mode although some very large network habitually run in DEBUG for extended periods of time.

Note

Only those users of Vanguard products who have been instructed by Customer Service should attempt to run their network with DEBUG turned on.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
0 ERROR DETECTED AT 0x0 bit(s) 0x0 CORRECTED	1005	Medium		Bad DRAM in the unit is being corrected by the software.		Swap the DRAM SIMMs to correct this problem.
(s) - TIMEOUT FROM TCP	329011	Medium	Minor	This message indicates that the TCP internal retries have been exhausted because of network congestion. The value *(s)* indicates the slot affected.		This is an information message only. There are no corrective actions necessary.
DC - ABNORMAL FSM EVENT: Event=%d, State=%d, Chan_ID=%d	248025	High	Warning	This is a debug message.		Contact your customer service representative if this message appears.
DC - BAD COMPRESSED PACKET	248031	High	Minor	This is a debug message.		Contact your customer service representative if this message appears.
DC - DC HANDLER CHANNEL NUMBER FAILURE	248033	High	Warning	This is a debug message.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
DC - DC HANDLER CHANNEL STATISTICS FAILURE, STATUS = %d	248034	High	Warning	This is a debug message.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DC - DC HANDLER CHANNEL STATS RESET FAILURE, STATUS = %d	248039	High	Warning	This is a debug message.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
DC - DC HANDLER FUNC TYPE FAILURE	248032	High	Minor	This is a debug message.		Contact your customer service representative if this message appears.
DC - DC HANDLER VOCABULARY RESET FAILURE	248035	High	Warning	This is a debug message.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
DC - DC WAS CALLED TO PROCESS CALL ACCEPT WITHOUT A SAVED CALL REQUEST FOR **%s**	248020	High	Warning	This is a debug message.		Contact your customer service representative if this message appears.
DC - dca_channel_flush(): PACKET COUNT ON THE QUEUE IS NON-ZERO	248037	High	Warning	This is a debug message.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DC - dca_deallocate_resources() WAS CALLED WITH A NULL DCCB PTR	248022	High	Minor	This is a debug message.		Contact your customer service representative if this message appears.
DC - dca_get_config_value() WAS CALLED WHEN CONFIG AS DISABLED FOR **%s**	248021	High	Critical	This is a debug message.		Contact your customer service representative if this message appears.
DC - dch_api_dho_provide_new_buf() RETURNED DCH FAILURE	248038	High	Warning	This is a debug message.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
DRAM CODE CHECKSUM ERROR - REPAIRED	1006	Medium		This alarm indicates that part of the code in DRAM is corrupted. It was detected an automatically repaired by reloading the image from FLASH to DRAM.		Go to DEBUG menu, option Display DRAM Code Errors. Record the screen and send the information to customer service. Contact your customer service representative if this message appears.
DRAM CODE CHECKSUM ERROR - UNABLE TO REPAIR - WRONG or NO FLASH	1007	High		This alarm indicates that part of code in DRAM is corrupted. It was detected but was not automatically repaired.		If the image in FLASH is new and good, reboot the node. If the image in FLASH is bad, load a good image and boot the node. Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DRAM IDATA CHECKSUM ERROR - RELOADING IDATA	1008	Medium		The IDATA area of RAM has been corrupted and the software is repairing it. The node should continued to operate correctly.		If reoccurring replace the MB.
DRAM IDATA ARRAY BITS[0 - 3]: 0x80d508 0x80d500 0x80d50c 0x80d510	1011	Medium		The IDATA area of RAM has been corrupted and the software is repairing it. The node should continued to operate correctly.		If reoccurring replace the MB.
DRAM IDATA Was reloaded correctly, contact customer service with above information	1009	Medium		The IDATA area of RAM has been corrupted and the software is repairing it. The node should continued to operate correctly.		If reoccurring replace the MB. Contact your customer service representative if this message appears.
EPx task rescued from possible deadlock	9001	Debug		This message indicates that the software detected a rare situation of a possible deadlock. The condition was automatically corrected.		This is an information message only. No corrective action is required. Contact your customer service representative if this message appears.
Process Msg: PID: *(n)* Event: *(n)* x25cause: *(n)* x25diag: *(n)* Stat	242015			This is a DEBUG report and only appears when the DEBUG option is enabled. Used for tracing call events through software modules.		This is an information message only. No corrective action is required.
ROUT MAIN: Command: *(event)* from *(n)*	16019			This is a DEBUG report and only appears when the DEBUG option is enabled. Used for tracing call events through software modules.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
RUIHC-Compressed Pkt CID # does not exist on LCON *(n)* Decompressor	404011	LOW	Warning	This message indicates the Context Identifier (CID) of the compressed packet is not valid because corresponding context is not valid in the decompressor context. This report appears only when RTP/UDP/IP Header compression DEBUG option is enabled.		Ensure that the number of sessions configured on both nodes of a link are the same. For each node, check the "Number of Session to be Compressed" parameter in the LAN Connection Table record.
RUIHC-Compressed pkt rcvd but comp typ is TRANSMIT on LCON *(n)*	404010	LOW	Warning	This message indicates that the receiver received a compressed packet on LCON # but the compression type configured is TRANSMIT only. This report appears only when RTP/UDP/IP Header compression DEBUG option is enabled.		If decompression is required change the "RTP/UDP/IP Header Compression" parameter to DUPLEX or AUTODETECT.
RUIHC-Compression started, LCON *(n)*, srcadd *(n)*, dstadd *(n)*, srcport *(n)*, dstport *(n)*, ssrc *(n)*	404003	LOW	Warning	This message indicates that compression is started on the LCON # with this flow: srcadd *(n)* is the IP Source Address dstadd *(n)* is the destination address srcport *(n)* is the source UDP port dstport *(n)* is the destination UDP port ssrc *(n)* is the RTP SSRC This report appears only when RTP/UDP/IP Header compression DEBUG option is enabled.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
RUIHC-Compressor Ctxt Overflow, LCON *(n)*	404001	LOW	Warning	This message indicates that a compressor (transmitter) context overflow on LCON #. This report appears only when RTP/UDP/IP Header compression DEBUG option is enabled.		Increase the value for the "Number of Session to be Compressed" parameter.
RUIHC-Ctxt Ent in NegCache, LCON *(n)*, srcadd *(n)*, dstadd *(n)*, srcport *(n)*, dstport *(n)*, ssrc *(n)*	404005	LOW	Warning	This message indicates that the context entry on LCON # with the following flow has been moved to negative cache where: srcadd *(n)* is the IP Source Address dstadd *(n)* is the destination address srcport *(n)* is the source UDP port dstport *(n)* is the destination UDP port ssrc *(n)* is the RTP SSRC This report appears only when RTP/UDP/IP Header compression DEBUG option is enabled.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
RUIHC-Ctxt Ent Tmout, LCON *(n)*, srcadd *(n)*, dstadd *(n)*, srcport *(n)*, dstport *(n)*, ssrc *(n)*	404004	LOW	Warning	This message indicates a context entry on LCON # with this flow times out: srcadd *(n)* is the IP Source Address dstadd *(n)* is the destination address srcport *(n)* is the source UDP port dstport *(n)* is the destination UDP port ssrc *(n)* is the RTP SSRC This report appears only when RTP/UDP/IP Header compression DEBUG option is enabled.		This is an information message only. No corrective action is required.
RUIHC-Ctxt St Packet Received, LCON *(n)*	404006	LOW	Warning	This message indicates that the CONTEXT_STATE packet is received on LCON #. This report appears only when RTP/UDP/IP Header compression DEBUG option is enabled.		This is an information message only. No corrective action is required.
RUIHC-Ctxt State packet CID *(n)*	404007	LOW	Warning	This message indicates that the context entry with Context Identifier # in the CONTEXT_STATE packet is rejected because that context is not valid in the transmitter (Compressor) context. This report appears only when RTP/UDP/IP Header compression DEBUG option is enabled.		Ensure that the number of sessions configured on both nodes of a link are the same. For each node, check the "Number of Session to be Compressed" parameter in the LAN Connection Table record.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
RUIHC-Ctxt State Pkt CID size mismatch on LCON *(n)*	404008	LOW	Warning	This message indicates that the there is a mismatch in CONTEXT_STATE packet entry CID size for this LCON.This report appears only when RTP/ UDP/IP Header compression DEBUG option is enabled.		Ensure that the number of sessions configured on both nodes of a link are the same. For each node, check the "Number of Session to be Compressed" parameter in the LAN Connection Table record.
RUIHC-New CtxtEnt Added, LCON *(n)*, srcadd *(n)*, dstadd *(n)*, srcport *(n)*, dstport *(n)*, ssrc *(n)*	404002	LOW	Warning	This message indicates that a new context entry is added to the compressor (transmitter) context on LCON # where: • srcadd *(n)* is the IP Source Address • dstadd *(n)* is the destination address • srcport *(n)* is the source UDP port • dstport *(n)* is the destination UDP port • ssrc *(n)* is the RTP SSRC This report appears only when RTP/UDP/IP Header compression DEBUG option is enabled.		This is an information message only. No corrective action is required.
RUIHC-No MEM to send Ctxt State packet on LCON *(n)*	404009	LOW	Warning	This message indicates that there is no memory available to generate a CONTEXT_STATE packet on LCON #. This report appears only when RTP/UDP/IP Header compression DEBUG option is enabled.		Increase the memory in the packet buffer pool.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
RUIHC-NO Memory LCON *(n)*	404000	LOW	Warning	This message indicates that there is no memory available. This report appears only when RTP/ UDP/IP Header compression DEBUG option is enabled.		Increase the memory by adding additional DRAM to your Vanguard unit.
Select Condition: Chain: *(n)* PID: *(n)* TbleAddr: *(n)* SETUP: *(n)*	242014			This is a DEBUG report, which appears when the DEBUG option is enabled, and is used to trace call events through software modules.		This is an information message only. No corrective action is required.
Select Destination: *(n)*	242013			This is a DEBUG report, which appears when the DEBUG option is enabled, and is used to trace call events through software modules.		This is an information message only. No corrective action is required.
SOTCP *(n)* - Invalid packet *(cause)*	331005			This alarm indicates that a remote node receives an SOTCP packet with an invalid packet format. The value *(n)* identifies the SOTCP session number, while (cause) identifies one of these causes for the alarm: • Vers = x. • Type = y. • Incorrect length of header extension. • Header extension = z.		To correct this problem, check the version of SOTCP running on the remote node. There may be a mismatch between the versions running on the source and destination. This mismatch could cause packets sent by one node to be unrecognizable by another.
SOTCP Data loss due to queue overflow	331019	Medium	Major	This message indicates that a packet has been dropped on this SOTCP connection since the queue toward TCP is full.	331007, 331013	Reduce the rate at which data is pumped into SOTCP from the serial protocol.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
SOTCP Init failed - IDCM init failed	331022			This alarm indicates that the ICDM module is not present in the software image that has been loaded into the node. This results in the SOTCP module failing to initialize.		The solution to this problem is to create a new image containing the ICDM and SOTCP modules and then reload it into the affected node.
IDCM Invalid Packet Type*(n)*		High		This alarm indicates an SoTCP error and voice calls not passing.		Contact Customer Service, customer might need an upgrade.
SOTCP Init failed Insufficient memory	331000	High	Critical	This alarm indicates that there is insufficient memory available to support the current SOTCP configuration.		To correct this problem, either: • Add more DRAM to the node. • Default the CMEM and reconfigure the node with lower values.
SOTCP Memory allocation failed	331008	High	Critical	This alarm indicates that SOTCP was unable to allocate memory for a particular operation such as allocating buffers to read data for a particular connection/session).		Retry the call later. **Note** Refer to the *Voice over IP Manual* in the *IP and LAN Feature Protocols Manual* (Part Number T0100) for additional information.
SOTCP New connection with connection id *(n)*	331013	CONN	Normal	This message indicates that a new connection has been established. The value *(n)* identifies the connection ID number.		This is an information message only. There are no corrective actions necessary.
SOTCP No matching IP peer for *(address)*	331016	Medium	Major	This message indicates that the X.25 address, indicated by *(address)* has no associated IP destination configured in the SOTCP mapping table.	331007, 331013	Configure the X.25 address and its corresponding destination IP address in the SOTCP mapping table.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
SOTCP No more connections	331009	High	Minor	This alarm indicates that SOTCP cannot accept/create a new connection because the number of active connections has reached the configured limit - either on this session (Max SVCs per session parameter) or overall (Total number of SVCs).	331007, 331013	Increase the value of the appropriate parameter, or retry the call after one of the active connections has closed. **Note** Refer to the *Voice over IP Manual* in the *IP and LAN Feature Protocols Manual* (Part Number T0100) for additional information.
SOTCP No more TCP sessions	331002	High	Major	This alarm indicates that SOTCP is unable to open a new TCP session because the number of active sessions has reached the limit configured for the Max TCP Sessions parameter.	331007, 331013	To correct this problem, either increase the configured number of Max TCP sessions or close one of the active sessions in order to accommodate a new one.
SOTCP Packet allocation failed	331014	Low	Minor	This message indicates that SOTCP has failed to allocate a packet due to an insufficient number of packets in the buffer pool.	331007, 331013	This is an information message only. There are no corrective actions necessary.
SOTCP Queue toward TCP blocked	331017	Medium	Minor	This message indicates that the session's queue of packets bound toward TCP has exceeded the blocking threshold, and all connections on this session have been blocked. This message is generated only on SOTCP sessions running Version 0 of the SOTCP protocol, where flow control per TCP session is performed.	331007, 331013	This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
SOTCP Queue toward TCP unblocked	331018	Medium	Normal	This message indicates that the session's queue of packets bound toward TCP fell below the unblocking threshold, and all connections on this session were unblocked. This report is generated only on SOTCP sessions running Version 0 of the SOTCP protocol, where flow control per TCP session is performed.		This is an information message only. There are no corrective actions necessary.
SOTCP Remote does not support pkt type	331021	High		This message indicates that the specified packet type is not recognized by the version of SOTCP running at the remote end. The packet is not being transmitted to the remote end.		This is an information message only. There are no corrective actions necessary.
SOTCP Session closed	331012	CONN	Normal	This message indicates that SOTCP has successfully closed the TCP session.		This is an information message only. There are no corrective actions necessary.
SOTCP TCP Active open failed with *(remote address)*	331006	High	Major	This alarm indicates that SOTCP was unable to create a TCP session to place a call to the remote end, due to insufficient memory. The string *(remote address)* identifies the end being called.		Either add more DRAM to the node or reduce the configuration in the node to create more available memory.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
SOTCP TCP Listen failed, trying after a while	331003	Medium	Warning	This alarm indicates that SOTCP was unable to create a TCP session to listen on the configured TCP port number. This alarm is the result of insufficient memory in the node.	331007, 331013	To correct this problem, either add more DRAM to the node or reduce the configuration in the node to free more available memory.
SOTCP TCP receive failed, session aborted	331004	High	Minor	This alarm indicates that SOTCP was unable to post a read to TCP for the next segment and has closed the TCP session.	331007, 331013	This is an information message only. There are no corrective actions necessary.
SOTCP TCP session closed by the remote end	331011	CONN	Normal	This alarm indicates that a remote IP node has closed the TCP session.		Check if the remote node is down, or if some router in the network has gone down.
SOTCP TCP session established with destination *(address)*	331007	CONN	Normal	This alarm indicates that SOTCP has established a TCP session with the IP destination identified by *(address)*.		This is an information message only. There are no corrective actions necessary.
SOTCP TCP session timed out with *(address)*	331010	CONN	Minor	This alarm indicates that TCP has detected that the link is inactive and has closed the session with the IP destination specified by the string *(address)*.	331007, 331013	Check if the remote IP destination is accessible (try to ping that destination).
TCP: *(high)*	256056	High	Major	This is a general alarm/report that is generated with a High priority level. This should never be displayed.		Contact your customer service representative if This message appears.
TCP: *(low)*	256058	Low	Warning	This is a general alarm/report that is generated with a Low priority level. This should never be displayed.		Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TCP: *(sn1)* to *(sn2)* given to app.	256030	Low	Normal	This alarm indicates that a segment has been given to an application. The value *(sn1)* is the starting sequence number and *(sn2)* is the ending sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: Act opn sccfl *PORT (n)*	256002	CONN	Normal	This message indicates the TCP connection has been opened successfully. The value *PORT (n)* identifies the destination port.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: app rcv tmout	256025	Low	Warning	This alarm indicates that the application receiver has timed out.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: drop seg *PORT (n) (sn)* ack num *(n)* rcv invld ACK	256012	Low	Warning	Received segment with invalid ACK, drop ping the segment. The value *PORT (n)* identifies the destination port, *(sn)* identifies the sequence number, and *(n)* is the ACK number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: drop seg *PORT (n) (sn)* no ACK present	256011	Low	Warning	This alarm indicates that a segment, with no ACK, has been received and that the segment is being dropped. The value *PORT (n)* identifies the destination port while *(sn)* identifies the sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TCP: drp seg *(sip)* -> *(desip) PORT (n)* rsn *(cause)* snd ACK	256006	Low	Warning	This alarm indicates that a segment was dropped and that an ACK is being sent. The value *(sip)* identifies the source IP address, *(desip)* identifies the destination IP address, *PORT (n)* identifies the destination port, and *(cause)* gives you an indication of why the segment was dropped.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: drp seg *PORT (n) (sn)*, too big for rcv buff	256022	Low	Warning	This alarm indicates that the length of a received segment exceeds the length of the receiver buffer. The value *PORT (n)* identifies the destination port and *(sn)* is the sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: ESTAB: rcvd FIN *PORT (n) (sn)*	256013	Low	Normal	This alarm indicates that a FIN was received in the ESTAB state. The value *PORT (n)* identifies the destination port and *(sn)* is the sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: excssv num rtries	256031	Low	Warning	This alarm indicates that an excessive number of retries has occurred.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TCP: frgn prt illgl close of wndw frgn hst *(fip)* lcl hst *(lip)* *PORT (n) PORT (s)*	256026	Low	Minor	This alarm indicates that a foreign host has illegitimately closed a window. The value *(fip)* is the foreign IP address, *(lip)* is the local IP address, *PORT (n)* is the destination port, and *PORT (s)* is the source port.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: Frng TCB for frgn hst *(fip)* lcl hst *(lip)*	256041	Low	Normal	This alarm indicates the TCD is being freed. The value *(fip)* identifies the foreign IP address while *(lip)* is the local IP address.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: Frng TCB for frgn hst *(fip)* lcl hst *(lip)*	256042	Low	Normal	This alarm indicates the TCD is being freed. The value *(fip)* identifies the foreign IP address while *(lip)* is the local IP address.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: get buf fld - cannot snd pkt\r\n	256052	High	Minor	This alarm indicates that the getting buffer failed, cannot send packet.		Try making the connection again and, if it still fails, contact your customer service representative.
TCP: Idle tmr fires frgn hst *(fip)* lcl hst *(lip)*	256043	Low	Warning	This alarm indicates that the idle timer has fired. The value *(fip)* identifies the foreign IP address while *(lip)* is the local IP address.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TCP: illgl optn rcvd in SYN seg	256035	Low	Warning	This alarm indicates that an illegal option was received in the SYN segment.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: Lcl wndw zero	256050	Low	Warning	This alarm indicates that the local window size has shrunk to zero.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: LISTEN: rcvd RST *PORT (n)* (*sn*)	256008	Low	Normal	This alarm indicates that the node is ignoring an RST packet in LISTEN state. The value *PORT (n)* identifies the destination port while *(sn)* identifies the sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: pkt cksum fld pkt = *(packet checksum*) calc = *(calculated checksum)*	256000	Low	Warning	This alarm indicates that a received packet has bad checksum.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: prcss FIN in ESTAB|SYN RCVD state frgn hst *(fip)* lcl hst *(lip) PORT (n) PORT (s)*	256024	Low	Normal	This alarm indicates that a FIN is being processed in the ESTAB or SYNRCVD state. The value *(fip)* is the foreign IP address, *(lip)* is the local IP address, *PORT (n)* is the destination port, and *PORT (s)* is the source port.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TCP: prcss FIN in invld state	256023	Low	Warning	This alarm indicates that a FIN is being processed in an invalid state.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: Rcvd ACK for Keep Alive	256049	Low	Normal	This alarm indicates that an ACK for the Keep Alive segment has been received.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: rcvd ACK seg with *PORT (n) (sn)* in LISTEN, snd RST	256038	Low	Warning	This alarm indicates that an ACK has been received in the LISTEN state and that an RST is being sent. The value *(PORT (n)* identifies the destination port and *(sn)* identifies the sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: Rcvd data after close, snd RST *(fip)* -> *(lip) PORT (n) PORT (s)*	256047	Low	Warning	Received data after close, sending RST. The value *(fip)* identifies the foreign IP address, *(lip)* is the local IP address, *PORT (n)* is the destination port, and *PORT (s)* is the source port.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: rcvd FIN while in LISTEN *PORT (n) (sn)*, snd RST	256016	Low	Warning	This alarm indicates that a FIN was received in the LISTEN state, and that an RST is being sent. The value *PORT (n)* identifies the destination port and *(sn)* is the sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TCP: rcvd invld SYN in wndw *(sip) -> (desip) PORT (n)* kill cnn	256003	High	Minor	This alarm indicates that an invalid SYN has been received and the connection is therefore being killed. The value *(sip)* identifies the source IP address, *(desip)* identifies the destination IP address, and *PORT (n)* identifies the destination port.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: Rcvd NACK	256048	Low	Warning	This alarm indicates that an NACK has been received.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: rcvd old seg *PORT (n)* (*sn*) snd ACK	256007	Low	Normal	This alarm indicates that an old segment has been received and that an ACK is being sent. The value *PORT (n)* identifies the destination port while *(sn)* identifies the sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: rcvd old SYN *(sip) -> (desip) PORT (n)* snd ACK	256004	Low	Normal	This alarm indicates that an old SYN has been received and that the connection is sending an ACK. The value *(sip)* identifies the source IP address, *(desip)* identifies the destination IP address, and *PORT (n)* identifies the destination port.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TCP: rcvd out of order seg *PORT (n) (sn)*, add hole at end (*hb*) to (*he*)	256017	Low	Warning	This alarm indicates that an out of order segment was received and a hole is being added. The value *PORT (n)* identifies the destination port, *(sn)* is the sequence number, (*hb*) is the hole beginning, and (*he*) is the hole end.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: rcvd out of order seg *PORT (n) (sn)*, add hole at end (*hb*) to (*he*)	256018	Low	Warning	This alarm indicates that an out of order segment was received and a hole is being added. The value *PORT (n)* identifies the destination port, *(sn)* is the sequence number, (*hb*) is the hole beginning, and (*he*) is the hole end.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: rcvd out of wndow seg *(sip)* -> *(desip) PORT (n)* snd ACK	256005	Low	Warning	This alarm indicates that a received segment is out of it's window and that an ACK is being sent. The value *(sip)* identifies the source IP address, *(desip)* identifies the destination IP address, and *PORT (n)* identifies the destination port.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: rcvd pkt (*sip*) -> (*desip*) *PORT (n)* no cnn	256001	Low	Minor	The packet does not belong to any connection. The value *(sip)* identifies the source IP address, *(desip)* identifies the destination IP address, and *PORT (n)* identifies the destination port.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TCP: rcvd PSH *PORT (n) (sn)*	256014	Low	Normal	This indicates that a PSH has been received. The value *PORT (n)* identifies the destination port and *(sn)* is the sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: rcvd RST *PORT (n) (sn)*, abort	256010	High	Minor	This alarm indicates that an RST has been received and that the connection is being aborted. The value *PORT (n)* identifies the destination port while *(sn)* identifies the sequence number.		Try making the connection again and, if it still fails, contact your customer service representative.
TCP: rcvd seg *PORT (n) (sn)*, fill beg hole (*hb*) to (*he)*	256019	Low	Warning	This alarm indicates that a new segment partially fills the beginning of a hole. The value *PORT (n)* identifies the destination port, *(sn)* is the sequence number, (*hb*) is the hole beginning, and (*he*) is the hole end.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: rcvd seg *PORT (n) (sn)*, fill end hole (*hb*) to (*he)*	256020	Low	Normal	This alarm indicates that a new segment partially fills the end of a hole. The value *PORT (n)* identifies the destination port, *(sn)* is the sequence number, (*hb*) is the hole beginning, and (*he*) is the hole end.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TCP: rcvd seg *PORT (n) (sn)*, rmv hole **%d** (*hb*) to (*he)*	256021	Low	Normal	This alarm indicates that a new segment completely fills a hole. The hole is being removed from the hole queue. The value *PORT (n)* identifies the destination port, *(sn)* is the sequence number, (*hb*) is the hole beginning, and (*he*) is the hole end.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: rcvd TCP pkt *(sip) -> (desip) PORT (n)*	256029	Low	Normal	This alarm indicates that a TCP packet has been received. The value *(sip)* is the source IP address, *(desip)* is the destination IP address, and *PORT (n)* is the destination port.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: recv buf too large *(rbs)*, clipped to *(cvrbs)*	256054	Low	Warning	This alarm indicates that the receiver buffer is too large; it is being clipped. The value *(rbs)* identifies the receiver buffer size and *(crbs)* is the clipped receiver buffer size.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: rjct seg *PORT (n) (sn)* bad ACK in SYNRCVD, snd RST	256037	Low	Warning	This alarm indicates that a segment is being rejected in the SYNRCVD state because a bad ACK was received. An RST is being sent. The value *(PORT (n)* identifies the destination port and *(sn)* identifies the sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TCP: rxmt *(sn1)* to *(sn2)*	256033	Low	Normal	This alarm indicates that a segment is being retransmitted. The value *(sn1)* is the starting sequence number and *(sn2)* is the ending sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: Rxmt tmr fires frgn hst *(fip)* lcl hst *(lip)*	256044	Low	Normal	This alarm indicates that the retransmission timer has fired. The value *(fip)* identifies the foreign IP address while *(lip)* is the local IP address.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: snd ctrl seg *(sn)* ack num *(n)* wndw *(s)*	256032	Low	Normal	This alarm indicates that a control segment is being sent. The value *(sn)* is the sequence number, *(n)* is the ACK number, and *(s)* is the window size.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: snd FIN *(sn)*, ack *(n)*	256051	Low	Normal	This alarm indicates that a FIN is being sent. The value *(sn)* identifies the sequence number and *(n)* identifies the ACK number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: State trnstn frm ESTAB to FIN WAIT *(fip) -> (lip) PORT (n) PORT (s)*	256045	Low	Normal	Transiting from ESTAB to FINWAIT state. The value *(fip)* identifies the foreign IP address, *(lip)* is the local IP address, *PORT (n)* is the destination port, and *PORT (s)* is the source port.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TCP: State trnstn to CLOSED *(fip)* -> *(lip) PORT (n) PORT (s)*	256046	CONN	Normal	Transiting to CLOSED state.The value *(fip)* identifies the foreign IP address, *(lip)* is the local IP address, *PORT (n)* is the destination port, and *PORT (s)* is the source port.		TCP connection has been successfully closed. If this was not a result of normal connection closure, contact your customer service representative.
TCP: state trnstn to ESTAB	256028	Low	Normal	Transiting to ESTAB state.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: state trnstn to SYNRCVD	256027	Low	Normal	Transiting to SYNRCVD state.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: SYN_RCVD SYN_SNT: rcvd RST *PORT (n)* (*sn*), rtrn->LISTEN	256009	Low	Normal	This alarm indicates that an RST has been received RST in the SYNRCVD or SYNSENT state, and that it is being transitioned to the LISTEN state. The value *PORT (n)* identifies the destination port while *(sn)* identifies the sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TCP: SYNRCVD: rcvd vld seg *PORT (n) (sn)*, enter ESTAB	256015	Low	Normal	This alarm indicates that a valid segment was received in the SYNRCVD state, and is entering the ESTAB state. The value *PORT (n)* identifies the destination port and *(sn)* is the sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: TCP cnn clsd frgn hst *(fip)* lcl hst *(lip)*	256040	Low	Normal	This alarm indicates that the TCP connection has been closed. The value *(fip)* identifies the foreign IP address while *(lip)* is the local IP address.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: TCP is Restarting	256055	Low	Warning	This alarm indicates that TCP is restarting.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: TCP snd rst to hst *(rip)*	256039	Low	Normal	This alarm indicates that an RST is being sent. The value *(rip)* identifies the remote IP address.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: xmit buf too large *(tbs)*, clipped to *(cvtbs)*	256053	Low	Warning	This alarm indicates that the transmit buffer is too large; it is being clipped. The value *(tbs)* identifies the transmit buffer size and *(ctbs)* is the clipped transmit buffer size.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TCP: xmt seq num *(sn1)* to *(sn2)*	256034	Low	Normal	This alarm indicates that segment is being transmitted. The value *(sn1)* is the starting sequence number and *(sn2)* is the ending sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP: zero wndw probe *(sn)*	256036	Low	Normal	This alarm indicates that there is Zero window probing. The value *(sn)* identifies the sequence number.		This message appears only when the DEBUG function is turned on, and is used for advanced system diagnosis. Contact your customer service representative if this message appears.
TCP:*(medium)*	256057	Medium	Minor	This is a general alarm/report that is generated with a Medium priority level. This should never be displayed.		Contact your customer service representative if this message appears.
TPA_TCP, TCP TIMEOUT, DISREGARDING PACKETS	329012	CONN		This alarm indicates that an infinite number of retries have been configured. TCP has timed out and packets are being discarded.		To correct this problem, verify that the link is alive and retry making the connection.
TPA_TCP,QUEUE FULL,PACKET DROPPED	329003	Medium	Major	This indicates that outbound queue (towards the remote host) is full.		To correct this problem, enable Flow Control on the node.
TPA_TCP,TCP ACTIVE OPEN FAILED	329008	CONN	Warning	This message indicates that a TCP open request has failed.		To correct this problem you can do one of two things: a) Increase the amount of RAM currently installed in the Vanguard device. b) Reboot the TPA

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TPA_TCP,TCP LISTEN FAILED	329007	CONN	Warning	The initial listen for the configured port is failed (internal error).		Reboot the TPA. **■ Note** Refer to the *TPDU Feature Protocol Manual* in the *Vanguard Applications Ware Basic Protocols Manual* (Part Number T0106) for additional information.
TPA_TCP,TCP-SEND FAILEDCONNECTION DROPPED	329004	High	Warning	The Writing into TCP byte stream is failed, the connection will be released immediately.		This is an internal error and there is no corrective action required.
VAN JACOBSON COMPRESSION FAILED ON INBOUND PACKET	270001	Medium	Major	This alarm indicates that Van Jacobson header decompression on a TCP/IP frame was attempted and failed.		Verify that the correct equipment and port is connected at the remote end of the link.

Chapter 7
Hardware Generated Alarms and Reports

Introduction

This chapter describes those alarms and reports that are generated as a result of Vanguard hardware problems, or failures, and link errors. The entries found in this chapter are those where the primary corrective actions involve making modifications to existing Vanguard hardware or the links that connect one node to another.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
%s - I.430 DIM IN SYNC	341001	High	Normal			Contact your customer service representative if this alarm is displayed.
%s - I.430 DIM OUT OF SYNC	341002	High	Major		341001	Contact your customer service representative if this alarm is displayed.
%s DETECTED DEVICE %d (%x hex) %s	115000	High	Normal			Contact your customer service representative if this alarm is displayed.
%s-<%d> - BOARD BOOT: CAUSE WATCHDOG TIMER EXPIRED	283008	High	Critical			Contact your customer service representative if this alarm is displayed.
%s-<%d> - HW BOARD FAILURE, CAUSE: BACKGROUND DIAGNOSTIC	283007	High	Critical			Contact your customer service representative if this alarm is displayed.
(s) CLEARING CALL, BAD OR NO RESPONSE FOR QSM	315006	High	Warning	This message indicates that the QLLC handshake process that takes place between the TPA-SDLC and the SDLC TPAD failed. The value *(s)* indicates the TPA-SDLC slot number affected.		Check the connection between SDLC TPAD and TPA-SDLC.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
(s) RETRY EXCEEDED, FOR SNA MESSAGE	315008	Low	Minor	This alarm indicates that an initial SNA ACTIVATE message has failed, and that no response was received from the attached terminal through SDLC TPAD. The value *(s)* identifies the TPA-SDLC slot number affected.		To correct this problem, you can do one of two things: • Check whether the terminal is up • Check whether the SDLC TPAD is running.
(x) BYTES LOADED FROM EXTENDED FLASH MEMORY	211000	High				Contact your customer service representative if this alarm is displayed.
<%s>-<%d>: BOARD BOOT: CAUSE SOFTWARE DOWNLOAD FAILED	283003	High	Critical			Contact your customer service representative if this alarm is displayed.
BACKUP LINK ACTIVATED	195010	High	Warning	This alarm indicates that the backup link is active and that all alternate links are down.		Check that the alternate links are properly configured.
BOD FEATURE DISABLED BY TIME OF WEEK	230005	Low	Warning	This message indicates that the BOD feature on a link is disabled by the Time Of Week feature.		This is an information message only. There are no corrective actions necessary.
BOD FEATURE ENABLED BY TIME OF WEEK	230006	Low	Warning	This message indicates that the BOD feature on a link is enabled by the Time Of Week feature.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
CANNOT ERASE FLASH MEMORY	105011	High	Critical	This alarm indicates that a failure occurred while erasing FLASH memory.	105002, 105005, 105014	To correct this problem: • Check all hardware for possible failure. • Verify the accuracy of all input parameters.
CANNOT ERASE FLASH MEMORY, *SLOT (s)*	105008	High	Critical	This alarm indicates that a failure occurred while erasing FLASH memory on one the configured slots. The value *SLOT (s)* identifies the slot number on which the error occurred.		To correct this problem: • Check all hardware to ensure it is operating correctly. Where necessary, refer to the appropriate hardware Installation Guide and relevant Applications Ware documentation. • Verify the accuracy of all input parameters.
CANNOT READ FROM FLASH MEMORY, *SLOT (s)*	104000	High	Critical	This alarm indicates a “Read” error occurred while reading FLASH memory. The value *SLOT (s)* identifies the slot number on which the error occurred.		To correct this problem: • Ensure that the specified slot has flash memory installed. • Install additional FLASH memory to you Vanguard device. • Check your Vanguard device to determine if there are any other mechanical problems. • Ensure that the specified slot has flash memory installed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
CANNOT WRITE TO FLASH MEMORY	105012	High	Critical	This alarm indicates that a failure occurred while writing to FLASH memory.		Check all hardware components for possible failure. **■ Note** If a hardware failure is not the cause of this problem, contact your customer service representative.
CANNOT WRITE TO FLASH MEMORY, *SLOT (s)*	105009	High	Critical	This alarm indicates that a failure occurred while writing to FLASH memory. The value *SLOT (s)* identifies the slot number on which the error occurred.	105002, 105005	To correct this problem: • Check all hardware to ensure it is operating correctly. Where necessary, refer to the appropriate hardware Installation Guide and relevant Applications Ware documentation. • Verify the accuracy of all input parameters.
CMEM BATTERY BAD	19015	High	Critical			Contact your customer service representative if this alarm is displayed.
CMEM CORRUPTION DETECTED ON BOARD *(n)*	4000	High	Critical	This alarm indicates that a CMEM checksum mismatch has occurred on a slave CPU and that the CMEM has been rebooted from a master CPU. The value *(n)* identifies the board's slot number.	4001	Reboot the slave CPU from the master CPU. **■ Note** If this alarm repeats itself contact your customer service representative.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
CMEM RECOVERED FROM BOARD *(n)*	4001	High	Normal	This message indicates that the alarm described for Trap 4000 occurred and corrected itself. The value *(n)* identifies the board number.		This is an information message only. No corrective action is required **■ Note** If the original alarm repeats itself, contact your customer service representative.
CVS - Module failed initialization	373001	High		This alarm indicates that Centralize Voice Switching Table software has failed to initialize because either the Voice Switching Table software has not been installed or there is insufficient DRAM.		There are two ways to deal with this situation: • Obtain an Applications Ware image that contains the Voice Switching Table software, or • Install additional DRAM in your Vanguard device.
DATA ENCRYPTION NOT ENABLED, H/W IS O.K	379020	High		This alarm indicates that the Data Encryption feature is not operational, that is, Data Encryption has not been enabled on a node equipped with the Data Encryption SIMM		You must ENABLE the 'Enable Encryption' parameter, in the in "Encryption Parameters" record. **■ Note** Refer to the *Data Encryption Feature Protocol Manual* (Part Number T0103-09) for additional configuration information.
DC - DATA COMPRESSION DISABLED, DC HARDWARE FAILURE	248001	High	Critical	This alarm indicates that data compression has been disabled in your Vanguard product. The reason for data compression being disabled is most likely a component failure in the data compression circuitry.		Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DC - DATA COMPRESSION DISABLED, DSP RAM NOT FOUND	248002	High	Critical	This alarm indicates that data compression has been disabled in your Vanguard product. The reason for this problem is a failure in the DSP SIMM.		Refer to the hardware Installation Guide that shipped with the Vanguard product for an indication of what the problem might be.
DC - DATA COMPRESSION DISABLED, POWER-UP DIAGNOSTICS FAILURE	248000	High	Critical	This alarm indicates that the Vanguard product has failed specific diagnostic tests that are automatically performed during power-up.		Refer to the hardware Installation Guide that shipped with the Vanguard product for an indication of what the problem might be. **■ Note** Contact customer service if this problem repeats itself.
DC - INSUFFICIENT RAM FOR DATA COMPRESSION	248003	High	Warning	This alarm indicates that your Vanguard product does not have sufficient on-board RAM to support the data compression feature.		Increase the amount of RAM installed in your device.
DEVICE ACTIVE	308034	Medium	Normal	This message indicates that a device is active.		This is an information message only. There are no corrective actions necessary.
DEVICE BOOT COMPLETE	57016	High		This message indicates that the Device Record was successfully booted.		This is an information message only. No corrective action is required.
DEVICE BOOT FAILURE	57017	High		This message indicates that the Device Record boot failed.		Save the device record.
DEVICE DISABLED	57013	High	Warning	This message indicates that a device is now disabled.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DEVICE DISABLE FAILURE	57015	High	Normal	This message indicates that a device has failed to be disabled.		This is an information message only. No corrective action is required.
DEVICE DOWN	57009	High	Major	This alarm indicates that a device has gone down, can not be addressed.	57000, 57008, 57010	Check the attached device.
DEVICE ENABLE FAILURE	57014	High	Normal	This message indicates that a device has failed to be enabled.		This is an information message only. No corrective action is required.
DEVICE ENABLED	57012	High	Normal	This message indicates that a device is enabled now.		This is an information message only. No corrective action is required.
DEVICE OPERATIONAL	57010	High	Normal	This message indicates that a device is operational.		This is an information message only. No corrective action is required.
DIAGNOSTIC FAILURE ON BOARD ##	19008	High	Critical	This message indicates that at the last node reset, the board specified was detected as inoperative.		Contact your customer service representative for additional information.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DIAGNOSTIC FAILURE ON BOARD 0, (x) SECTION	19007	High	Critical	This message indicates an error message that results from diagnostic tests that are run on the motherboard. The value (x) indicates one of these sections: • Main • DSP • PAD • Slave • Global Memory • DMA • Port (n)		Contact your customer service representative for additional information.
DOWNLOAD FAILED: INSUF. MEMORY FOR %s	339000	High		This alarm indicates that a DSP image file, in FLASH memory, is larger than the ports allocated download buffer.		This alarm should never be displayed. However, if you encounter it, you should contact customer service.
DOWNLOAD FAILED: VSMIO OPERATION FAILED	339001	High		This alarm indicates that communication with the DSP assigned to the port has failed during port initialization		To correct this Voice feature problem: • Check the results of the power-up diagnostics for a specific failure report. • Return voice card for repair/ replacement

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DVMRP.2 DVMRP Module Aborted; not enough RAM\r\n,	328002	High	Critical	This message indicates that the DVMRP module does not have enough memory to initialize.		Perform one of these activities to correct this problem: • Increase the amount of memory in your node. • Reduce existing memory usage by: – Reducing table sizes – Removing unwanted features in the image
ENCRYPTION SIMM IS DEFECTIVE	379000	High		This message indicates that either a failure has occurred in the Data Encryption SIMM or the SIMM itself has not been installed in the node.		Verify that an Encryption SIMM is installed and replace if necessary. **■ Note** Refer to the *Vanguard Daughtercard Installation Guide* (Part Number T0020) for additional information.
EXTENDED CHECKSUM ERROR: SLOT *(s)* DISABLED	211004	High	Critical	This message indicates that a slave CPU has encountered a fatal error.		Verify that slave CPU is not defective. Replace the CPU if necessary.
EXTENDED SOFTWARE LOAD FAILS IN *SLOT (s)*	211002	Medium	Critical	This message indicates that an error has been detected when trying to load the extended memory from slot indicated by the value *SLOT (x)*.		System will continue running in 'Economy'. You should verify that FLASH memory is loaded with the proper extended image

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
FAN FAILED	1002	High	Critical	This alarm is generated whenever the fan stops running.		Check and repair/replace the defective fan. **■ Note** Refer to your Vanguard Installation Guide for additional information.
HW BOARD FAILURE	280000	High	Critical	This alarm indicates that a voice daughtercard has failed its power-up diagnostic routine.		Re-insert the voice card and try again. **■ Note** If this problem persists, you may have to replace the Voice daughtercard.
IGMP.15 IGMP Membership Query on %d IGMP Circuit	327015	LOW	Low	This message indicates the arrival of an IGMP query on particular interface.		This is an information message. No corrective action is required.
IGMP.16 IGMP Membership Report(VER_1) on %d IGMP Circuit for %s Multicast Address	327016	LOW	Low	This alarm indicates some host is registering to particular group address.		This is an information message. No corrective action is required.
IGMP.18 IGMP Membership Leave message on %d IGMP Circuit for %s Multicast Address	327017	LOW	Low	This alarm indicates that the specified interface wants to leave the group to which it has registered.		This is an information message. No corrective action is required.
IGMP.19 IGMP Leave for Unknown grp member %s on ckt %d	327018	LOW	Low	This message indicates an alarm error condition. A leave request has been received on an interface, for which the same host is not registered.		This is an information message. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IGMP.2 IGMP Module Aborted; not enough RAM	327002	High	High	This alarm is generated during memory allocation for the IGMP control block.		To correct this problem: • Add memory to the router, or • Reduce existing memory usage by reducing table sizes or removing unwanted modules from the image.
IGMP.20 IGMP Unknown Packet type %d on ckt %d	327019	LOW	Low	This alarm indicates the Type field, in the IGMP header, is unknown. The router cannot handle the type received		This is an information message. No corrective action is required.
IGMP.21 IGMP Group Membership Timeout	327020	LOW	Low	This message indicates that there are no reports received from host for a particular group till the configured expiry time.		This is an information message. No corrective action is required.
IN-SUFFICIENT MEMORY FOR X25 CALL TRANSLATION TABLES	46014	High	Critical	This alarm indicates that your Vanguard device has insufficient memory to create the X.25 Incoming Call Translation Table.		Reduce the number of entries in the Incoming Call Translation Table, configured in the node record. **Note** Refer to the X.25 Basic Configuration Manual for additional information.
INBOUND LINK BLOCKED	308045	Low	Minor	This alarm indicates that the frame queue, to the terminal, is blocked and that a frame has been dropped.	308046	Check the queue size and the port speed.
INBOUND LINK UNBLOCKED	308046	Low	Normal	This alarm indicates that the frame queue to the terminal is no longer blocked.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
INSUFFICIENT MEMORY TO INITIALIZE ENCRYPTION	379001	High		This message indicates that the node running encryption does not have sufficient DRAM to support the application.		Contact your customer service representative for information on upgrading your nodes DRAM.
INSUFFICIENT RAM FOR CONFIGURATION	19012	High	Critical			Contact your customer service representative if this alarm is displayed.
IPX tables boot failed : No memory for IPX context block.	210000	High		This alarm indicates that an IPX Tables boot failed due to the lack of memory for the IPX module.		To correct this problem: a) Add additional DRAM to your Vanguard router (increasing shared heap, adding DRAM). b) Boot the node.
IPX tables boot failed : No memory for IPX_CTP context block	210000	High		This alarm indicates that an IPX Tables boot has failed due to the lack of memory for the IPX_CTP module.		To correct this problem: a) Add additional DRAM to your Vanguard router (increasing shared heap, adding DRAM). b) Boot the node.
ISDN LINE DOWN:SWITCHED TO Low BANDWIDTH	230007	Low	Normal	This is a special report generated under unique conditions. It implies that a Link has been switched to low bandwidth because the ISDN link is down.		Check the ISDN connection to determine why the failure occurred. **■ Note** Refer to the *Multi-Service Feature Protocols Manual* (Part Number T0103) for additional information.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
LEASED LINE DOWN:SWITCHED TO High BANDWIDTH	230002	High	Normal	This is a special report generated under unique conditions. It implies that a Link has been switched to high bandwidth because the normally used leased line is down.		Investigate the cause of the leased line failure.
LEASED LINE UP:SWITCHED TO Low BANDWIDTH	230003	High	Normal	This is a special report generated under unique conditions. It implies that a Link has been switched to low bandwidth because the normally used leased line is up.		This is an information message only. There are no corrective actions necessary.
LINE DOWN	57007	High	Major	This alarm indicates that a line has gone down, and that no attached devices can be addressed.	57000, 57008	Check the attached host/devices.
LINE DOWN	125007	High	Major	This alarm indicates that none of the devices on the line are responding to to TPAD polling.	125008	Verify that the links are all intact and operational, and check the configuration for errors.
LINE OPERATIONAL	57008	High	Normal	This message indicates that a line is up.		This is an information message only. No corrective action is required.
LINE OPERATIONAL	110008	High	Normal	This alarm indicates that at least one device responded to a TPAD poll and that at least one device was polled or selected (HPAD).		This is an information message only. No corrective action is required.
LINE OPERATIONAL	125008	High	Normal	This alarm indicates that at least one device responded to a TPAD poll and that at least one device was polled or selected (HPAD).		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
LINK DOWN	68011	High	Major	This alarm indicates that the link is inoperative. Occurs when the number of attempts to connect (as set during configuration) is exceeded.	68007	Check cables and hardware for possible failure. If OK, check the transmission media.
LINK DOWN	195000	High	Major	This alarm indicates that a link is inoperative. This alarm occurs when the number of attempts to connect (as set during configuration) is exceeded.	195007	Check cables and hardware for possible failure. If these are OK, check the transmission media.
LINK UP	68007	High	Normal	This message indicates that the link has gone from link setup state to data transfer state.		This is an information message only. No corrective action is required.
LINK UP	308035	High	Normal	This message indicates that a connection between PAD (HPAD and TPAD) is up.		This is an information message only. There are no corrective actions necessary.
LOCAL DRAM EXHAUSTED	19014	Low	Critical	This message indicates that a sufficiently complex configuration is stored and the node runs out of DRAM.		Add the expansion DRAM SIMMs to your node to alleviate memory space
MASTER FAILED TO COPY EXTENDED S/W	211003	Medium	Critical	This message indicates that an error was detected while copying an image into the Master CPU.		Swap the slave CPU (that has the image) to be the master
MEMORY ALLOCATION FAILED	308020	Low		This alarm indicates that there is insufficient memory in the node.		Add additional DRAM to your Vanguard device or contact your customer service representative for assistance.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
MODEM FAULTY OR NOT CONNECTED	6021	Medium	Warning	This message indicates that the modem is faulty or not connected. When this occurs, the node will use shared memory for storage, but this is slower to access than local memory.		Ensure that the modem is properly connected.
MOTHERBOARD LAB STRAP INSTALLED	106003	High	Normal			Contact your customer service representative if this alarm is displayed.
No memory for (type) table	202006	High		This alarm indicates that the IPX protocol could not obtain memory for the table (type) listed below: • XNS Routing Tables • Access Tables • SAP Filter Tables		To correct each of these problems you must add additional DRAM to your Vanguard router.
No memory for Access Control Cache	202003	High		This alarm indicates that the IPX protocol could not obtain memory for Access Control Cache.		To correct this problem you must add additional DRAM to your Vanguard router.
No memory for outbound interfaces list of Access control filter	202008	Low		IPX Could not allocate memory for outbound interface list in the access control table		To correct this problem you must add additional DRAM to your Vanguard device.
No memory for outbound LCONs list of Access control filter: Attempt to add duplicate record	202008	Low		This alarm indicates that duplicate records have been configured in the outbound LCON List and, therefore, IPX can not allocate memory for the outbound LCON list in the access control table.		To correct this problem you must add additional DRAM to your Vanguard product.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
No memory for *TABLE (x)* record	202007	Medium		This alarm indicates that IPX cannot obtain memory for an entry. The value TABLE (x) specifies the table in which the record can not be created.		To correct this problem you must add additional DRAM to your Vanguard product.
NODE RESET DUE TO POWER-UP OR RESET SWITCH	19000	High	Normal	This alarm indicates that a node reset occurs as a result of a power-up event being received or the RESET switch being pressed.		This is an information message only. No corrective action is required.
NOT ENOUGH MEMORY	317028	Medium	Critical	This message indicates that memory, for allocating the context for Session and Flow Control, is not available.		To correct this problem you can do one of two things: • Reduce the Image Size. • Increase the DRAM of the Node.G22
NS RUN-TIME ERROR - NO FEATURES	229001	Low	Critical			Contact your customer service representative if this alarm is displayed.
Out of Memory	236001	High	Critical	This alarm indicates that there is insufficient memory available for the specified AppleTalk data structure to startup.		Add additional RAM to your Vanguard device and reboot the node.
PORT (n) OUT OF MEMORY - SOME STATIONS NOT CREATED	186011	High		This alarm indicates that the memory available in the node has been exhausted while setting up FRA stations on the port. Consequently one or more of the configured stations are not operational. The value *PORT (n)* identifies the port affected.		To correct this problem: • Increase the amount of RAM in your Vanguard product. • Reduce the number of configured FRA stations on the port.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
POWER SUPPLY *(n)* DOWN	1000	High	Critical	This alarm indicates that a failure has been detected in the power supply. The value *(n)* indicates which power supply is affected.	1001	Repair or replace the faulty power supply as soon as possible. **■ Note** Refer to your Vanguard Installation Guide for additional information.
POWER SUPPLY *(n)* UP	1001	High	Normal	This message indicates that the power supply has returned to it's normal (ON) status. The value *(n)* indicates which power supply, in multi-supply products, is affected.		This is an information message only. No corrective action is required.
QOS: INITIALIZATION FAILURE - NOT ENOUGH MEMORY	400000	High		This message indicates that a failure was logged during node initialization because there was not enough memory to bring up the QoS features for the node.		To correct this problem: a) Add more memory or configure the QoS General parameters. b) Boot the node.
SLOT (n) - HW BOARD FAILURE, CAUSE: BACKGROUND DIAGNOSTIC	281000	High	Critical	This alarm indicates that a DSPM in *Slot (n)* has failed its background diagnostic routine.		This problem is caused by either a hardware failure or a problem with the software. If the problem does not repeat itself, there are no corrective actions required. However, if the problem does repeat replace the DSPM card. Contact customer service if this does not solve the problem.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
SLOT (n) BOARD BOOT, CAUSE: WATCHDOG TIMER EXPIRED	281001	High	Critical	This alarm is related to Trap No 281000, which indicates the type of background diagnostic that failed.		This problem is caused by either a hardware failure or a problem with the software. If the problem does not repeat itself, there are no corrective actions required. However, if the problem does repeat replace the DSPM card. Contact customer service if this does not solve the problem.
SS: ENTRY (x) IS INVALID	242002	High	Critical	This alarm indicates that a link has been configured as a backup and as a monitored link. The value (x) identifies the link.		Backup links cannot be configured as monitor.
T1E1VG_REPT ALARM	371003			This alarm is used to report various T1E1 alarms.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - Hardware Failed (OS Memory)	371003	High	Critical	This message indicates that a node does not have enough memory to accommodate the T1E1VG module. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - Hardware Failed (DRV Memory)	371003	High	Critical	This message indicates that a node failed to create the T1E1VG_DRIVER. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - Hardware Failed (ME Memory)	371003	High	Critical	This message indicates that a node failed to allocate memory for T1E1VG_ME context. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
T1E1 Int. *(i/f)* - Hardware Failed (DSL Memory)	371003	High	Critical	This message indicates that a node failed to allocate memory for T1/E1 interface control block. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - Configuration Mismatch	371003	High	Critical	This message indicates that the Interface type configured in the CMEM record is different from the H/W DIM type. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - CMEM Error *(code)*	371003	High	Critical	This alarm indicates that a CMEM record has an invalid setting for some parameters. The value *(code)* identifies these error codes: • Code 1; Some parameters are out of range. • Code 4, The 1st channel port is 0 for FRACTIONAL • Code 5; FDL is selected for SF format • Code 6; Time slot is overlap • Code 7; The 1st channel port has 0 time slot • Code 8; The B channel range is 0 • Code 9; The D channel is configured for B channel usage		To correct this problem, clear CMEM and re-configure the product.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
T1E1 Int. *(i/f)* - Remote loopback in progress	371001	High	Normal	This message indicates that the T1/E1 interface is currently in Remote Loopback. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - Remote loopback ended	371002	High	Normal	This message indicates that the T1/E1 interface is out of Remote Loopback and has returned to normal operation. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - REMOTE ALARM INDICATION: CLEARED	371003	High	Normal	This message indicates that the E1 interface indicates that an alarm condition has been cleared. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - LOSS OF FRAME: CLEARED	371003	High	Normal	This message indicates that the E1 interface indicates that an alarm condition has been cleared. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - LOSS OF SIGNAL: CLEARED	371003	High	Normal	This message indicates that the E1 interface indicates that an alarm condition has been cleared. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - ALARM INDICATION SIGNAL: CLEARED	371003	High	Normal	This message indicates that an alarm condition on the E1 interface has been cleared. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
T1E1 Int. *(i/f)* - REMOTE ALARM INDICATION	371003	High	Normal	This message indicates that an alarm condition on the E1 interface has occurred. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - LOSS OF FRAME	371003	High	Normal	This message indicates that an alarm condition on the E1 interface has occurred. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - LOSS OF SIGNAL	371003	High	Normal	This message indicates that an alarm condition on the E1 interface has occurred. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - ALARM INDICATION SIGNAL	371003	High	Normal	This message indicates that an alarm condition on the E1 interface has occurred. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - YELLOW ALARM: CLEARED	371003	High	Normal	This message indicates that the T1 interface indicates that an alarm condition has been cleared. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int.*(i/f)* - RED ALARM: CLEARED	371003	High	Normal	This message indicates that the T1 interface indicates that an alarm condition has been cleared. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - BLUE ALARM: CLEARED	371003	High	Normal	This message indicates that the T1 interface indicates that an alarm condition has been cleared. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
T1E1 Int. *(i/f)* - YELLOW ALARM	371003	High	Normal	This message indicates that the T1 interface indicates that an alarm condition has occurred. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int. *(i/f)* - RED ALARM	371003	High	Normal	This message indicates that the T1 interface indicates that an alarm condition has occurred. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1E1 Int *(i/f)* - BLUE ALARM	371003	High	Normal	This message indicates that the T1 interface indicates that an alarm condition has occurred. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1/E1 Int. *(i/f)*-LES THRESHOLD EXCEEDED	371004	Medium	Normal	This message indicates that the thresholds configured in the T1/E1 interface CMEM record have been exceeded. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1/E1 Int. *(i/f)* -LCV THRESHOLD EXCEEDED	371004	Medium	Normal	This message indicates that the thresholds configured in the T1/E1 interface CMEM record have been exceeded. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1/E1 Int. *(i/f)* -PCV THRESHOLD EXCEEDED	371004	Medium	Normal	This message indicates that the thresholds configured in the T1/E1 interface CMEM record have been exceeded. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
T1/E1 Int. *(i/f)* -CSS THRESHOLD EXCEEDED	371004	Medium	Normal	This message indicates that the thresholds configured in the T1/E1 interface CMEM record have been exceeded. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1/E1 Int. *(i/f)* -ES THRESHOLD EXCEEDED	371004	Medium	Normal	This message indicates that the thresholds configured in the T1/E1 interface CMEM record have been exceeded. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1/E1 Int. *(i/f)* -BES THRESHOLD EXCEEDED	371004	Medium	Normal	This message indicates that the thresholds configured in the T1/E1 interface CMEM record have been exceeded. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1/E1 Int. *(i/f)* -SES THRESHOLD EXCEEDED	371004	Medium	Normal	This message indicates that the thresholds configured in the T1/E1 interface CMEM record have been exceeded. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1/E1 Int. *(i/f)* -SEFS THRESHOLD EXCEEDED	371004	Medium	Normal	This message indicates that the thresholds configured in the T1/E1 interface CMEM record have been exceeded. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
T1/E1 Int. *(i/f)* -UAS THRESHOLD EXCEEDED	371004	Medium	Normal	This message indicates that the thresholds configured in the T1/E1 interface CMEM record have been exceeded. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TDM_CLK Module fail (OS Memory)	404043	High	Critical	This message indicates that a node has failed to allocate memory for the TDM_CLK_MGT module.		This is an information message only. No corrective action is required.
Network Clock lost from TDM-*(i/f)*	404044	High	Normal	This message indicates that the T1/E1 interface providing the network clock for the node is in an ALARM state. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
Network Clock derives from TDM-*(i/f)*	404045	High	Normal	This message indicates that the network clock is derived from the indicated T1/E1 interface. The value *(i/f)* identifies the interface.		This is an information message only. No corrective action is required.
VPMT Module fail (OS Memory)	404046	High	Critical	This message indicates that a node does not have enough memory to accommodate the VPMT_CNTRLR module		This is an information message only. No corrective action is required.
VPMT Module fail (VPMT Memory)	404047	High	Critical	This message indicates that a node has failed to allocate memory for VPMT context		This is an information message only. No corrective action is required.
VPMT Module fail (VPMT_CB Memory)	404048	High	Critical	This message indicates that a node has failed to allocate memory for VPMT_CB for the virtual port entry		This is an information message only. No corrective action is required.
ISDN PRI INTERFACE *(i/f)* IS ACTIVE	404049	High	Normal	This message indicates that there is an active ISDN PRI line. The value *(i/f)* identifies the active PRI interface.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
ISDN PRI INTERFACE *(i/f)* IS INACTIVE	404050	High	Critical	This message indicates that there is an inactive ISDN PRI line. The value *(i/f)* identifies the inactive PRI interface.		This is an information message only. No corrective action is required.
INCOMING CALL FROM *(number)* ON DSL *(line)*	404051	Medium	Normal	This message indicates that there is an incoming call from phone number on ISDN PRI line. The value *(number)* identifies the incoming phone number and *(line)* identifies the line being used.		This is an information message only. No corrective action is required.
INCOMING CALL FROM UNKNOWN NUMBER ON DSL *(line)*	404052	Medium	Normal	This message indicates that there is an incoming call from unknown phone number on ISDN PRI line. The value *(line)* identifies the line being used.		This is an information message only. No corrective action is required.
OUTGOING CALL TO *(call)* ON DSL *(line)*	404053	Medium	Normal	This message indicates that there is an outgoing call on the ISDN PRI line. The value *(call)* identifies the outgoing call and *(line)* identifies the line being used.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TFR - INSUFFICIENT MEMORY - *(degree)*	298000	High	Critical	This alarm indicates that the memory is insufficient to bring up the TFR in the desired configuration. The value *(degree)* specifies the degree of failure, i.e., whether initialization has failed completely or whether the TFR has been initialized without DCP on one or more connections.		Complete these steps, in the order presented, to determine the cause of this alarm: • Reduce the configuration parameters in the TFR record if these have been configured with values much larger than necessary. • Set 'DCP Protection Level' to None if DCP isn't essential. • Add more memory to the node.
IPX protocol subsystem high priority traps	210000	High		This alarm indicates that an IPX Parameter boot was not successful. The reason for this failure was insufficient memory.		To correct this problem: a) Add additional DRAM to your Vanguard router. b) Boot the node to reserve memory at node restart/ power-up time.
TIME OF WEEK DISABLING:SWITCHED TO Low BANDWIDTH	230004	High	Normal	This is a special report generated under unique conditions. It implies that a Link has been switched back to low bandwidth because the Time Of Week (TOW) feature has disabled the high bandwidth link.		This is an information message only. There are no corrective actions necessary.
TPA-SDLC, IDCM NOT UP	315005	High	Major	This message indicates that an internal initialization sequence has failed.		To correct this problem you can do one of two things: • Reduce the image size/ • Add extra DRAM to the Vanguard device.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TPA-SDLC, IDCM OR TGO DOES NOT EXIST	315004	High	Critical	This alarm indicates that initialization of the TPA-SDLC failed because the TGO and IDCM modules do not exist in the image		Check the image contents for these modules
TPA-SDLC, NOT ENOUGH MEMORY	315003	High	Critical	This alarm indicates that there is insufficient memory available to allocate the TPA-SDLC instance.		To correct this problem you can do one of two things: a) Reduce the image size, or b) Add extra DRAM to the Vanguard device
TPA-UDP, NOT ENOUGH MEMORY	330001	High	Critical	This report indicates that initialization of TPA UDP is failed.		Two possible solutions to this problem are: • Add additional RAM to your Vanguard device. • Reduce the image size.
TPA-X25, IDCM NOT UP	324005	High	Major	This alarm indicates a TPA X.25 initialization has failed. Possible causes for this problem are: • Module (IDCM/TGO) is not present in the image • Memory is not available to initialize the modules (IDCM/TGO)		To correct this problem you can do one of two things: • Rebuild the image including the modules (IDCM/TGO). • Increase the amount of memory in your node.
TPA-X25, IDCM OR TGO DOES NOT EXIST	324004	High	Major	This alarm indicates that modules IDCME and TGO are not present in the image		To correct this problem you can do one of two things: • Rebuild the image including the modules (IDCM/TGO). • Increase the memory size.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TPA-X25, NOT ENOUGH MEMORY	324000	High	Critical	This alarm indicates that memory in the node is insufficient to initialize the X.25 TPA TPDU adapter.		Add additional DRAM to your Vanguard device.
TPA_TCP, CONNECTION RETRIES OVER	329006	CONN	Major	This message indicates that the TCP connection retries, towards the remote host, is exhausted.		Either the LAN is not working or the remote host is down.
TPA_TCP,PACKET ALLOCATION FAILED	329005	High	Major	This alarm indicates that an internal buffer pool is dry.		Increase the DRAM size to have more buffer pool / Internal buffer releasing error.
TPR-INIT *(s)* TPA module *(d)* init failed	317006	High	Critical	This alarm indicates that TPDU Router slot initialization has failed. The value *(s)* indicates the slot affected and *(d)* indicates the module affected.		To correct this problem you can do one of two things: • Reduce the Image Size. • Increase the DRAM of the Node.
TPR-INIT FAILED	317004	High	Critical	This report indicates that insufficient memory is available to creating a TPDU Router instance. Therefore the initialization is failed.		To correct this problem you can do one of two things: a) Reduce the Image Size b) Increase the DRAM of the Node
UNKNOWN CARD TYPE - SLOT %d	106002	High	Normal			Contact your customer service representative if this alarm is displayed.
USER_DISABLE: SWITCHED TO Low BANDWIDTH	230008	Low	Normal	This is a special report generated under unique conditions. It implies that a Link has been switched to low bandwidth because the BOD feature has been disabled.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
UTILIZATION DOWN:SWITCHED TO Low BANDWIDTH	230001	High	Normal	This is a special report generated under unique conditions. it implies that a Link has been switched back to low bandwidth because the normally used leased line is no longer congested.		This is an information message only. There are no corrective actions necessary.
UTILIZATION UP:SWITCHED TO High BANDWIDTH	230000	High	Normal	This is a special report generated under unique conditions. It implies that a Link has been switched to high bandwidth as the normally used leased line has become congested.		This is an information message only. There are no corrective actions necessary.

Chapter 8
ATM Alarms and Reports

Introduction

This chapter describes those alarms and reports that are generated by the ATM protocol on Vanguard nodes.

Note

The alarms and reports identified in this chapter do not currently have Trap Numbers associated with them.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
InATMARP *(ops)* received on *LCON (n)* with out of LIS remote IP Address *(add)*		Medium	Warning	This ATM alarm indicates that an InATMAP Request/Reply has been received. specifying a remote IP Address which is not in our LIS. The value *(ops)* identifies whether it is a Request or Replay, *LCON (n)* identifies the LAN Connection, and *(add)* identifies the remote IP Address.		To correct this problem, reconfigure the local and/or the remote interface IP addresses so that they are in the same LIS.
Remote IP Address Changed on *LCON (n)*, new IP address *(add)*		Medium	Normal	This ATM alarm indicates that the IP address of the remote end of a particular LCON, learned via InATMARP, is changed from the old IP address learned previously via InATMARP. The value *LCON (n)* identifies the LAN Connection, *(add)* identifies the remote IP Address.		This is an information message only. No corrective actions are required.
InATMARP *(ops)* received on *LCON (n)* with duplicate remote IP Address *(add)*		High	Warning	This ATM alarm indicates that an InATMAP Request/Reply has been received. specifying a remote IP Address which is not in our LIS. The value *(ops)* identifies whether it is a Request or Replay, *LCON (n)* identifies the LAN Connection, *(add)* identifies the remote IP Address.		To correct this problem reconfigure the IP address of the each remote interface so that each has a unique IP address

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Max InATMARP Retries over on *LCON (n)*.		Low	Warning	This ATM alarm indicates that the maximum number of InATMARP Retries has been reached on the LCON specified by the value *LCON (n)*.		To correct this problem identify the network segment that is causing InATMARP packets to get dropped or delayed and correct it.
InATMARP *(ops)* received with NULL Source IP Address on *LCON (n)*		Debug	Warning	This ATM alarm indicates that an InATMARP Request or Reply has been received, with a NULL Source IP Address on a particular LCON. The value *(ops)* identifies whether it is a Request or Replay and *LCON (n)* identifies the LAN Connection.		To correct this problem identify the node that is creating erroneous InATMARP packets and correct it. **■ Note** This is a debug alarm and should not normally appear unless your Vanguard product has been configured with Debug turned on.
InATMARP Reply received with NULL Target IP Address on *LCON (n)*		Debug	Warning	This ATM alarm is indicates that an InATMARP Reply has been received with a NULL Target IP Address, on a particular LCON. The value *LCON (n)* identifies the LAN Connection.		To correct this problem identify the node that is creating erroneous InATMARP packets and correct it. **■ Note** This is a debug alarm and should not normally appear unless your Vanguard product has been configured with Debug turned on.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Error in ATMARP Packet received on *LCON (n) - (msg), (field)*		Debug	Warning	This ATM alarm indicates that an InATMARP/ATMARP packet has been received on a particular LCON, containing either a bad value in one of the fields or with one or more fields missing. This report indicates the particular error condition along with the erroneous field value. The value *LCON (n)* identifies the LAN Connection, *(msg)* identifies the error message, and *(field)* identifies the error message field. These messages include: • Incomplete ATMARP packet. One or more ATMARP packet fields (fixed or variable length field) are missing. That is length of the ATMARP packet is less than the expected length. • Invalid Hardware Type. A Bad or Unsupported Hardware Type field. • Invalid Protocol Type. A Bad or Unsupported Protocol Type field. • Invalid Operation Type. A Bad or Unsupported Operation Code field.		To correct these problems, identify the remote node that is generating the errorneous InATMARP packet and correct it as required by the message indicated. **■ Note** This is a debug alarm and should not normally appear unless your Vanguard product has been configured with Debug turned on.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Error in ATMARP Packet received on *LCON (n) - (msg), (field)* (Continued)		Debug	Warning	• Bad Source/Target Protocol Length. A Source/Target Protocol Field is non null and not equal to 4. • Bad Source/Target ATM Number/Subaddress Length. The length of a Source/Target ATM Number/Subaddress is greater than 20. • Bad Source/Target ATM Number/Subaddress Type. a Source/Target ATM Number/ subaddress with an invalid type. • Invalid ATM Structure. A Source/Target ATM Address is in an Invalid ATM structure format.		To correct these problems, identify the remote node that is generating the errorneous InATMARP packet and correct it as required by the message indicated. **■ Note** This is a debug alarm and should not normally appear unless your Vanguard product has been configured with Debug turned on.
InATMARP *(ops)* received on *LCON (n)*		Debug	Normal	This ATM alarm indicates that an valid InATMARP Request or Reply has been received on a particular LCON. The value *(ops)* identifies whether it is a Request or Replay and *LCON (n)* identifies the LAN Connection.		Contact your customer service representative if this alarm appears. **■ Note** This is a debug alarm and should not normally appear unless your Vanguard product has been configured with Debug turned on.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
InATMARP *(ops)* sent on *LCON (n)*		Debug	Normal	This ATM alarm indicates that a InATMARP Request or Reply has been sent on a particular LCON. The value *(ops)* identifies whether it is a Request or Replay and *LCON (n)* identifies the LAN Connection.		Contact your customer service representative if this alarm appears. **■ Note** This is a debug alarm and should not normally appear unless your Vanguard product has been configured with Debug turned on.
Not Enough memory - *(msg)*		High	Critical	This ATM alarm indicates that insufficient memory is available to support the IPOATM operation. The value *(msg)* identifies an error message describing the consequences of a memory allocation failure.		To correct this problem: a) Install additional memory in your Vanguard device. b) Disable some of the other software features that not currently being used.
Invalid Protocol Packet to be sent on VC Multiplexed *LCON (n)*		Low	Warning	This ATM alarm indicates that the packet's protocol type does not match the protocol of the VC MUX LCON on which the packet is to be sent. The value *LCON (n)* identifies the LAN Connection involved.		To correct this problem change the Protocol Type on the VC MUX LCON to carry the correct protocol traffic.
Unsupported or invalid Protocol Packet to be sent on rfc1483_LLC_SNAP *LCON (n)*		Debug	Warning	This ATM alarm indicates that an unsupported protocol type exists on a packet. This packet has been sent on a specific LCON using RFC1483 LLC/SNAP Encapsulation. The value *LCON (n)* identifies the LAN Connection involved.		Change the LCON's encapsulation type to match the traffic type in question.

Chapter 9
BootP, IP, IPX, QoS, VPN, ARP, ETH, GW, ICMP, RIP, SNA, TKR, UDP, PIM, MBR, MFE and XN Alarms and Reports

Introduction

This chapter describes those alarms and reports that are generated from these protocols on Vanguard nodes.

- BootP - BootP messages
- IP - Internet Protocol
- IPX - Internet Packet Exchange
- OSPF - Open Shortest Path First
- ARP - Address Resolution Protocol
- ETH - Ethernet
- GW - Gateway
- ICMP - Internet Control Message Protocol
- RIP - Routing Information Protocol
- SNA - SNABSC
- QoS - Quality of Service
- TKR - Token Ring
- UDP - user diagram Protocol
- PIM - Protocol Independent Multicast Sparse Mode (PIM-SM)
- MBR - Multicast Border Router
- MFE - Multicast Forwarding Engine
- XN - Xerox Network Core
- VPN - Virtual Private Network

Note

The alarms and reports identified in this chapter may or may not have Trap Numbers associated with them. Some Tunneling alarms have different descriptions for the same Trap Number.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
Source port is in Busy Out state				This OSPF alarm indicates that a call has been rejected because port is in the busy-out state.		To correct this problem, enable port and then try the call again.
Source Station Record does not exist				This OSPF alarm indicates that a Copy Station Record operation was not performed because the record does not exist.		To correct this problem, configure the Port Record again. However, change the number of stations so that a default station record would be created.
BTP.001, received request from *(client_IP_address, net Network ID)*	479001			A BOOTP request has been received on a particular interface. The client IP address is included in the message, but may be unknown at this time, in which case it will show up as 0.0.0.0.		This is an informational message.
BTP.002, bad request from *(client_IP_address, net Network ID): reason*	479002			A BOOTP request has been received on a particular interface. The client IP address is included in the message, but may be unknown at this time, in which case iwill show up as 0.0.0.0. The request is bad for the stated reason, and is therefore discarded.		This is an informational message.
BTP.003, Forwarding request to *server_IP_address*	479003			A BOOTP request is being forwarded to a particular server.		This is an informational message.
BTP.004, Forwarding reply from *server_IP_address to client_IP_address*	479004			A BOOTP reply is being forwarded from a particular server back to the client, using the router as a relay agent.		This is an informational message.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
BTP.005, Bad reply from *server_IP_address to client_IP_address*	479005			A BOOTP reply was received. We are unable to relay the reply to the client due to the stated error. The BOOTP reply has been discarded.		Investigate the stated error.
OSPF.001, Bad length pkt, from *(source)*, type *(N)*	487001	Medium	Medium	This OSPF alarm indicates that an OSPF packet, smaller than the minimum size, was received and discarded. The value *(source)* identifies the packets source address and *(N)* identifies the packet type.		To correct this problem, investigate the OSPF implementation of the source address.
OSPF.002, Bad pkt checksum, from *(source)*, type *(N)*	487002	Medium	Medium	This OSPF alarm indicates an OSPF packet has been received. The length field indicates a longer packet than indicated by the IP header length field. This packet is discarded. The value *(source)* identifies the packets source address and *(N)* identifies the packet type.		To correct this problem, investigate the OSPF implementation of the source address. This could also be due to LAN problems.
OSPF.003, OSPF version, from *(source)*, type *(N)*	487003	Medium	Medium	This OSPF alarm indicates the OSPF version of a packet was different than the OSPF version in this router. The value *(source)* identifies the packets source address and *(N)* identifies the packet type.		To correct this problem, investigate the OSPF implementation of the source address.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.004, Duplicate Router ID, from *(source)*, type *(N)*	487004	Medium		This alarm indicates that an OSPF packet has been received. The router ID specified in the OSPF header is equal to the router's own ID. Either two interfaces are attached to the same network or there is a conflict in the assignment of OSPF router IDs. Either way, the packet is discarded. **■Note** This alarm should never be generated by a Vanguard device.		Contact your customer service representative if this alarm appears.
OSPF.005, No matching ifc for pkt from *(source)*, type *(N)*	487005	Medium		This alarm indicates that an OSPF packet has been received with: • An unacceptable destination address. • OSPF header parameters do not match the corresponding parameters configured for the receiving interface. • The value *(source)* identifies the packets source address and *(N)* identifies the packet type.		To correct this problem, check the configuration of the Area ID and the Dead Router interval in the source router. Verify that they match the this routers OSPF interface configuration.
OSPF.006, Authentication failure, from *(source)*, type *(N)*	487006	Medium	Medium	This OSPF alarm indicates that different authentication fields have been set in the two routers. The value *(source)* identifies the packets source address and *(N)* identifies the packet type.		To correct this problem, investigate the authentication set in the OSPF parameters of the source address.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.007, No matching nbr for pkt from *(source)*, type *(N)*	487007	Medium	Medium	This OSPF alarm indicates that an OSPF packet has been received from a router which is not a neighbor of this router. The value *(source)* identifies the packets source address and *(N)* identifies the packet type.		To correct this problem, check the configuration of the source address.
OSPF.008, Bad pkt type from *(source)*, type *(N)*	487008	Medium		This OSPF alarm indicates that an OSPF packet type is not recognized. The value *(source)* identifies the packets source address and *(N)* identifies the packet type.		To correct this problem, check the implementation of the source address.
OSPF.009, No buffer for mcast to *(dest)*	487009	High		This OSPF alarm indicates that an OSPF packet was not sent due to memory exhaustion. The value *(dest)* identifies the multicast destination.		To correct this problem, verify that the Vanguard device has sufficient memory. Upgrade the device memory as required.
OSPF.010, LPTRACE, Received packet type *(N)* from *(source)*	487010	PTrace		This OSPF message indicates that a packet has been received. The value *(source)* identifies the packets source address and *(N)* identifies the packet type.		This is an information message only. No corrective actions are required.
OSPF.011, Sending unicast type *(N)* dst *(dest)*	487011	UTrace		This OSPF message indicates that a unicast type packet is being sent. The value *(N)* identifies the packet type and *(dest)* identifies the destination address.		This is an information message only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
OSPF.012, Sending mcast type *(N)*, dst *(dest)*, net *(net_id)*	487012	PTrace		This OSPF message indicates that an OSPF multicast packet is being sent. The value *(N)* identifies the packet type, *(dest)* identifies the destination address, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
OSPF.013, Rxmit-ting type *(N)*, *(source)* -> *(dest)*	487013	Low		This OSPF message indicates that an OSPF packet is being retransmitted. The value *(N)* identifies the packet type, *(source)* identifies the source address, and *(dest)* identifies the destination address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.014, No FSM match, ifc *(i/f)* state *(state)*, event *(e)*	487014	High		This OSPF alarm indicates that some event has taken place that was not accepted on an interface in it's current state. The value *(i/f)* identifies the interface. The value *(e)* identifies the event that has occurred, including: • Event #1; IFE_UP Interface Operational • Event #2; IFE_WTIMWait Timer Expired • Event #3; IFE_BSEENBackup DR discovered • Event #4; IFE_NCHGChange in neighbor State • Event #5; IFE_LOOPInterface Looped • Event #6 ; IFE_UNLOOPInterface Unlooped • Event #7; IFE_DEADInterface is no longer operational The value *(state)* identifies the existing interface state including: • State 1; IFS_DOWN Interface dead • State 2; IFS_LOOPED Interface looped back • State 4; IFS_WAIT Waiting for DR selection • State 8; IFS_PPInterface is Pt-to-Pt or Virtual • State 16; IFS_OTHER IFS is neither DR or BDR • State 32; IFS_BDRIFS is Backup Designated Router • State 64; IFS_DRIFS is Designated Router		Identify the event which caused the problem and contact your customer service representative.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.015, State change, ifc *(i/f)*, new state *(state)* event *(e)*	487015	Low		This OSPF message indicates that a state change has occurred on an interface. The value *(i/f)* identifies the interface type.		This is an information message only. No corrective actions are required.
				The value *(e)* identifies the event that has occurred, including: • Event #1; IFE_UP Interface Operational • Event #2; IFE_WTIM Wait Timer Expired • Event #3; IFE_BSEEN Backup DR discovered • Event #4; IFE_NCHG Change in neighbor State • Event #5; IFE_LOOP Interface Looped • Event #6 ; IFE_UNLOOP Interface Unlooped • Event #7; IFE_DEAD Interface is no longer operational The value *(state)* identifies the existing interface state including: • State 1; IFS_DOWN Interface dead • State 2; IFS_LOOPED Interface looped back • State 4; IFS_WAIT Waiting for DR selection • State 8; IFS_PP Interface is Pt-to-Pt or Virtual • State 16; IFS_OTHER IFS is neither DR or BDR • State 32; IFS_BDRIFS is Backup Designated Router • State 64; IFS_DRIFS is Designated Router		
OSPF.016, No match for hlo (virtual link) from *(source)*	487016	Medium		This OSPF alarm indicates that no neighbor is configured for the virtual link on the IP source specified by the value *(source)*.		To correct this problem, check the virtual link configuration on both sides.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.017, Network mask mismatch with *(source)*	487017	Medium		This OSPF alarm indicates that a network mask mismatch for Hello packets exists. The value *(source)* identifies the source address of the mismatch.		To correct this problem, check the configuration on the source address. The network mask received in the hello packet should match the interface mask of the receiving interface.
OSPF.018, Hello interval mismatch with *(source)*	487018	Medium		This OSPF alarm indicates that a Hello interval mismatch exists for Hello Packets. The value *(source)* identifies the source address of the mismatch.		To correct this problem, check the configuration on the source address. The hello interval should be set to the same value in all routers connected to area.
OSPF.019, Dead interval mismatch with *(source)*	487019	Medium		This OSPF alarm indicates that a Dead interval mismatch exists in Hello packets. The value *(source)* identifies the source address of the mismatch.		To correct this problem, check the configuration on the source address. The dead router interval should be set to the same value in all routers connected to one area.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.020, No FSM match, nbr *(add)*, state *(state)*, event *(event)*	487020	High		This OSPF alarm indicates that there is no neighbor state machine match for states and events. The value *(add)* identifies the Neighbor IP address. The value *(state)* identifies the neighbor state code, including: • State 1; 0x01NBS_DOWN Neighbor is unreachable • State 2; 0x02NBS_ATTEMPT Attempt to contact Neighbor • State 4; 0x04NBS_INIT Have seen Neighbors hellos • State 8; 0x08NBS_2WAY Neighbor has seen our hellos • State 16; 0x10NBS_EXST Master/Slave negotiation • State 32; 0x20NBS_EXCH Database exchange • State 64; 0x40NBS_LOAD Request new DB records • State 128; 0x80NBS_FULL Fully Adjacent The value *(event)* identifies the neighbor event code, including: • Event #1; NBE_HELLO Hello packet received • Event #3; NBE_START Bi-directional Communication • Event #4; NBE_ADJOK OK for adjacency to form • Event #5; NBE_NEGDN Master/Slave Negotiation done • Event #6; NBE_EXCDN Database exchange done • Event #7; NBE_SEQMM Sequence number mismatch • Event #8; NBE_BADRQ Bad LS request received • Event #9; NBE_LDON All LS requests satisfied • Event #10; NBE_1WAY One-way communication only • Event #11; NBE_KILLN Interface is dead • Event #12; NBE_IATIM No hellos seen recently • Event #13; NBE_LLDWN Lower level indicates down • Event #14; NBE_GO Start adjacency establishment • Event #15; NBE_NOPROG Destroy adjacency; failure to thrive		Check the nbr State Machine Table and diagnose the problem indicated.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.021, State change, nbr *(add)*, new state *(state)*, event *(event)*	487021	Low		This OSPF message indicates that a state change has occurred in the nbr table. The value *(add)* identifies the neighbor IP address. The value *(state)* identifies the neighbor state code, including: • State 1; 0x01NBS_DOWN Neighbor is unreachable • State 2; 0x02NBS_ATTEMPT Attempt to contact Neighbor • State 4; 0x04NBS_INIT Have seen Neighbors hellos • State 8; 0x08NBS_2WAY Neighbor has seen our hellos • State 16; 0x10NBS_EXST Master/Slave negotiation • State 32; 0x20NBS_EXCH Database exchange • State 64; 0x40NBS_LOAD Request new DB records • State 128; 0x80NBS_FULL Fully Adjacent The value *(event)* identifies the neighbor event code, including: • Event #1; NBE_HELLO Hello packet received • Event #3; NBE_START Bi-directional Communication • Event #4; NBE_ADJOK OK for adjacency to form • Event #5; NBE_NEGDN Master/Slave Negotiation done • Event #6; NBE_EXCDN Database exchange done • Event #7; NBE_SEQMM Sequence number mismatch • Event #8; NBE_BADRQ Bad LS request received • Event #9; NBE_LDON All LS requests satisfied • Event #10; NBE_1WAY One-way communication only • Event #11; NBE_KILLN Interface is dead • Event #12; NBE_IATIM No hellos seen recently • Event #13; NBE_LLDWN Lower level indicates down • Event #14; NBE_GO Start adjacency establishment • Event #15; NBE_NOPROG Destroy adjacency; failure to thrive		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.022, Outstanding DD pkt not avail for nbr *(add)*	487022	High		This OSPF message indicates that an outstanding database description packet has not yet been acknowledged. The value *(add)* identifies the neighbor IP address.		This is an information message only. No corrective actions are required.
OSPF.023, Unable to get pkt, to *(dest)*, ifc *(i/f)*	487023	High		This OSPF alarm indicates that there is insufficient memory available to a specific interface. The value *(dest)* identifies the packets destination while *(i/f)* identifies the specific interface.		To correct this problem, verify that the Vanguard device has sufficient memory. Upgrade the device memory as required.
OSPF.024, Bad length LS adv from *(add)*	487024	Medium		This OSPF alarm indicates that the length of a received Link State update packet is invalid. The value *(add)* identifies the neighbor IP address.		To correct this problem, check the configuration of the source address.
OSPF.025, from *(add)*, adv. cksum fl:*(t), (dest), (orig)*	487025	Medium		This OSPF alarm indicates that a checksum failure has occurred. The value *(add)* identifies the neighbor IP address, *(t)* identifies the packet type, *(dest)* identifies the destination address, and *(orig)* identifies the origin of the failure.		To correct this problem, check the OSPF configuration of the source address.
OSPF.026, from *(add)*, bad type, adv: *(type) (id)*	487026	Medium		This OSPF alarm indicates that a received OSPF advertisement is invalid. The value *(add)* identifies the neighbor IP address, *(type)* identifies the link state type, and *(id)* identifies the link state advertisement ID.		To correct this problem, check the OSPF configuration of the source address.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.027, from *(add)*, old adv: (*type)* *(id)*	487027	Medium		This OSPF alarm indicates that an external adv has been received on a virtual link. The value *(add)* identifies the neighbor IP address, *(type)* identifies the link state type, and *(id)* identifies the link state advertisement ID.		To correct this problem, check the OSPF configuration of the source address.
OSPF.028, LUINFO, from *(add)*, old adv: *(type)*, *(id)*	487028	Low		This OSPF message indicates that an older Link State Update packet has been received. The value *(add)* identifies the neighbor IP address, *(type)* identifies the link state type, and *(id)* identifies the link state advertisement ID.		This is an information message only. No corrective actions are required.
OSPF.029, from *(add)*, self update: *(type)*, *(id)*	487029	Low		This OSPF message indicates that a self update packet has been received. The value *(add)* identifies the neighbor IP address, *(type)* identifies the link state type, and *(id)* identifies the link state advertisement ID.		This is an information message only. No corrective actions are required.
OSPF.030, from *(add)*, new adv: *(type)*, *(id)*	487030	Low		This OSPF message indicates that a valid new advertisement has been received. The value *(add)* identifies the neighbor IP address, *(type)* identifies the link state type, and *(id)* identifies the link state advertisement ID.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.031, from *(add)*, Old ack for adv: *(type)*, *(id)*	487031	Low		This OSPF message indicates that an old ACK message has been received old ACK for an interface advertisement. The value *(add)* identifies the neighbor IP address, *(type)* identifies the link state type, and *(id)* identifies the link state advertisement ID.		This is an information message only. No corrective actions are required.
OSPF.032, Bad ack from *(add)* for adv: *(type)*, *(id)*	487032	Low		This OSPF message indicates that a bad ACK message has been received for an interface advertisement The value *(add)* identifies the neighbor IP address, *(type)* identifies the link state type, and *(id)* identifies the link state advertisement ID.		This is an information message only. No corrective actions are required.
OSPF.033, LS update retransmission to *(add)*	487033	Low		This OSPF message indicates that a Link State Update packet has been retransmitted. The value *(add)* identifies the neighbor IP address.		This is an information message only. No corrective actions are required.
OSPF.034, LS ack sent direct to *(add)*	487034	Low		This OSPF message indicates that an LSU ACK message has been sent directly to the interface identified by the value *(add)*. This identifies the neighbor IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.035, Flushing advertisement: *(type)*, *(id)*	487035	Low		This OSPF message indicates that the aging of a specific database, the MAXAGE point has been reached. This results in the advertisement being flushed from the router. The value *(id)* identifies the advertisement and *(type)* identifies the link state type.		This is an information message only. No corrective actions are required.
OSPF.036, Originating adv: *(type)*, *(id)*	487036	Low		This OSPF message indicates that an originating advertisement has been sent. The value *(id)* identifies the advertisement and *(type)* identifies the link state type.		This is an information message only. No corrective actions are required.
OSPF.037, new route to *(dest)*, type *(type)*, cost *(cost)*	487037	Low		This OSPF message indicates that a new route generation exists. The value *(dest)* identifies the destination of the new route, *(type)* identifies the route type, and *(cost)* identifies the cost of this route.		This is an information message only. No corrective actions are required.
OSPF.038, NBMA hello sent to dest *(add)*	487038	PTrace		This OSPF message indicates that NBMA hello messages have been sent to an interface. The value *(add)* identifies the neighbor IP address.		This is an information message only. No corrective actions are required.
OSPF.039, The OSPF routing protocol is *(state)*	487039	Low		This OSPF message indicates that OSPF routing has been either enabled or disabled. The value *(state)* will identify either Enabled or Disabled.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.040, SPF Interface *(add)* is not an IP address, Interface not installed	487040	Low		This OSPF alarm indicates that an OSPF interface is not an IP address. The value *(add)* identifies the interface IP address.		To correct this problem, check and modify the IP configuration as required.
OSPF.041, Non-Broadcast net *(add)* is not an SPF interface.	487041	Low		This OSPF alarm indicates that an NBMA is not an OSPF interface. The value *(add)* identifies the interface IP address.		To correct this problem, check and modify the IP configuration as required.
OSPF.042, protocol (disabled): *(source)* -> *(dest)*, type *(type)* discarded	487042	PTrace		This message indicates that the OSPF protocol is disabled although an OSPF packet has been received. The OSPF packet is discarded. The value *(source)* identifies the IP source, *(dest)* identifies the IP destination, and *(type)* identifies the OSPF packet type. **■Note** This OSPF message should not appear.		Contact your customer service representative if this message appears.
OSPF.043, Duplicate LS ack received from *(add)*	487043	Low		This OSPF message indicates that a duplicate ACK message has been received from the source address. The value *(add)* identifies the neighbor IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.044, from *(add)*, bad age field, adv *(type), (id)*	487044	Medium		This OSPF alarm indicates that, if the age of a LS update packet is greater that the MAXAGE parameter or less than zero (0), it is received. The value *(add)* identifies the neighbor IP address, *(type)* identifies the link state type, and *(id)* identifies the link state advertisement.		To correct this problem, check the originator of the advertisement and correct as required.
OSPF.045, non-existent area *(area)*, VL discarded	487045	Low		This OSPF alarm indicates that an area on which a VL is configured does not exist and the virtual link is being discarded. The value *(area)* identifies the proposed transit area.		To correct this problem, check area configuration and modify as required.
OSPF.046, No backbone configured, VL s discarded	487046	Low		This OSPF alarm indicates that a router that has a VL configured has to have the area 0.0.0.0 configured in its router.		To correct this problem, configure an area 0.0.0.0 in the router.
OSPF.047, *(dest)* now unreachable	487047	Low		This OSPF message indicates that a route is now unreachable. The value *(dest)* identifies the unreachable destination.		This is an information message only. No corrective actions are required.
OSPF.048, AS ext adv limit exceeded; origination deferred	487048	Medium		This OSPF message should not appear.		Contact your customer service representative if this message appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.050, from *(add)*, Max Age: *(type)*, *(id)*	487050	Low		This OSPF message indicates that a received link state advertisement has reached the MAXAGE point. The value *(add)* identifies the neighbor IP address, *(type)* identifies the link state type, and *(id)* identifies the link state advertisement.		This is an information message only. No corrective actions are required.
OSPF.051, bad adv/ ovflo: *(type)*, *(dest)*, *(orig)*	487051	Medium		This OSPF message indicates that a new link state advertisement could not be installed in the database. This could be because of memory problems or an internal error. The value *(type)* identifies the link state type, and *(id)* identifies the link state advertisement.		To correct this problem, verify that sufficient memory exists in the Vanguard device and upgrade as required.
OSPF.052, Stub area mismatch with *(source)*, recvd in stub area, adv	487052	Medium		This OSPF message indicates that Hello packets show the same area to be configured differently.		To correct this problem, check the OSPF configuration of the source address.
OSPF.053, from *(source)*, recvd in stub area, adv	487053	Medium		If area is a stub area, and external advertisements are received, then this OSPF error is generated.		To correct this problem, check the OSPF implementation of the source address.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPF.054, Internal Programming error	487054	UTrace		This OSPF alarm indicates that an internal programming error has occurred.		This is usually a serious error that may occur at runtime or at init time. a) If it occurs at runtime, it should be carefully diagnosed. b) If it occurs at init time, the OSPF protocol does not come up.
OSPF.055, Memory allocation failed	487055	UTrace		This alarm indicates that a memory allocation failure has occurred.		This is usually a serious error which could occur at runtime or init time. a) If it occurs at runtime, it should be carefully diagnosed. b) If it occurs at init time, the OSPF protocol does not come up.
OSPF.056, Timer allocation failed	487056	UTrace		This alarm indicates that a Timer allocation has failed.		This alarm occurs only at init time. The OSPF does not come up.
OSPF -> %s	207003	Debug				This alarm is a debug alarm.
OSPF -> Not Enough Permanent memory - %s	207004	High				Contact your customer service representative if this message appears
OSPF -> Not Enough Dynamic Memory - %s	207005	High				Contact your customer service representative if this message appears

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
OSPF -> Configuration Error - %s	207006	High				Contact your customer service representative if this message appears
OSPF -> Route to %s / %d imported from BGP into OSPF Routing Domain	207007	Low				None
OSPF -> Route to %s / %d withdrawn by BGP from OSPF Routing Domain	207008	Low				None
OSPF -> Route to %s / %d is Not Imported into OSPF due to 'Deny' Policy No. %d	207009	Debug				None
OSPF -> Route to %s / %d matched to BGP-OSPF Import 'Permit' Policy No. %d	207010	Debug				None
OSPFM *(n)* - PVC CONNECTION FAILED ON *(node)*		Low		This OSPF alarm indicates that the address of a serial port or the FRI Bypass Station in a SPFM table does not exist on the Node or it is already being used. The value *PORT (n)* identifies the table entry number and *(node)* identifies the node affected.		To correct this problem, check the SPFM table entry for correct configuration. Ensure that the source and destination ports/ stations exist.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OSPFM *(n)* - PVC CONNECTED *(source) -> (dest)*		Low		This OSPFM message indicates that a PVC Connection between a *(source)* and *(dest)* has been established. The value *PORT (n)* identifies the table entry number.		This is an information message only. No corrective actions are required.
OSPFM *(n)* - DISABLED, DUPLICATE SLOT ON SPFM *(con)*		Low		This OSPFM alarm indicates that a multiplexed DLCI slot in an SPFM table entry is already used in another PVC connection. The value *PORT (n)* identifies the table entry number and *(con)* identifies the connection.		To correct this problem, correct the SPFM records to ensure that the unique slot number is used.
Invalid N(R)				This alarm indicates that a frame has been received with a bad N(R).		To correct this problem, verify that both ends of the link are running the same port type. If the problem persists, check the hardware. Check the K Level 2 Windows.
Invalid number of X.25 data bytes out of range				This alarm indicates that the value of Remote Datascope Interactive mode n parameter lies outside the allowable range 0 to 1024.		To correct this problem, enter a value within the acceptable range. **■ Note** Refer to the *Remote Datascope Feature Manual* (Part Number T0103-07) for additional information.
Invalid P(R)				This alarm indicates that packet testing has located an error.		To correct this problem, check the K Level 2 Windows. **■ Note** Contact your representative if this alarms appears repeatedly.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Invalid P(S)				This alarm indicates that packet testing has located an error.		**Note** Contact your representative if this alarms appears repeatedly.
Invalid Port Number				This alarm indicates that an LBU port was not configured in the LBU Tables.		To correct this problem, configure the port number in the LBU Tables and boot the tables.
Invalid Port Subtype				This alarm indicates that an attempt was made to boot an MX25 port, but the port subtype was neither MASTER nor SLAVE.		If repeated, consult your customer service representative.
Invalid value of X.25 level				This alarm indicates that the value of the Remote Datascope Single-line mode k parameter is configured to a value other than 1, 2, or 3.		To correct this problem, enter a valid k value for this parameter.
IP Interface - *(n)* - Exceeding Maximum Range Allowed		High		This IP alarm indicates that the number of IP Router Interfaces found at node initialization exceeds the maximum number of IP Interfaces allowed. The value *PORT (n)* identifies the invalid interface number.		To correct this problem, provided that the use of the IP Router Interface is absolutely necessary, increase the maximum number of IP Router Interfaces allowed.
IP Interfaces - *(x)* to *(y)* - Exceeding Maximum Range Allowed		High		This IP alarm indicates that the number of IP Router Interface(s) found at node initialization exceeds maximum number of IP Router Interfaces allowed. The values *(x)* and *(y)* identify the invalid interface numbers.		To correct this problem, provided that the use of the IP Router Interface is absolutely necessary, increase the maximum number of IP Router Interfaces allowed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.001 q ovrf *(source)* -> *(dest)* nt *(net_id)*	481001	Low		This IP alarm indicates that the forwarder must discard a packet because of a queue overflow.The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
IP.002 not V4 hdr version_number nt *(net_id)*	481002	Medium		This IP alarm indicates that a packet has an incorrect version number. The value and *(net_id)* identifies the network.		Provided that no other versions of IP are running on the node, this alarm would indicate that a packet has been damaged. If this alarm appears repeatedly, examine a line trace to determine where the packet is being damaged.
IP.003 shrt hdr *(hdr_length)* pkt ln *(pkt_length)* nt *(net_id)*	481003	Medium		This IP alarm indicates that a packet's indicated header length is below the minimum possible length. This is usually an indication of damaged packets but it could also be the result of another node building incorrect headers. The value *(hdr_length)* identifies the length of the received header. *(pkt_length)* identifies the length of the packet and *(net_id)* identifies the network.		If this alarms appears repeatedly, examine a line trace to determine where the packet is being damaged.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
IP.004 bd hdr cks *(rcsum), (ccsum), (source) -> (dest)*	481004	Medium		This IP alarm indicates that a packet has an invalid checksum. This is usually an indication of damaged packets but it could also be the result of another node building incorrect headers. The value *(rcsum)* identifies the received checksum, *(ccsum)* identifies the correct checksum, *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		If this alarms appears repeatedly, examine a line trace to determine where the packet is being damaged.
IP.005 pkt trunc *(sleng)* pkt ln *(tleng) (source) -> (dest)*	481005	Medium		This IP alarm indicates that the packet length specified in the header is greater than the packet buffer length. The value *(sleng)* identifies the specified length, *(tleng)* identifies the true length, *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		There are two possible causes of this problem: a) Packet corruption occurring during transit - check all connecting networks and routers. b) A programming error in a remote node - check the configurations of al remote nodes and correct as necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.006 pkt *(source)* -> *(dest)* dsc rsn *(cause)*, nt *(net_id)*	481006	High		This IP message indicates that a packet was not accepted for transmission on the network. if this is due to flow control, an ICMP source quench will be sent to the sender; otherwise, an ICMP destination unreachable will be sent. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address, the *(cause)* identifies why the packet was not accepted, and *(net_id)* identifies the network. • *#define D_OK 0 /* Packet successfully accepted */* • *#define D_ERR 1 /* Random error */* • *#define D_OVFL 2 /* Packet not accepted for flow control reasons */*		This is an information message only. No corrective actions are required.
IP.007 *(source)* ->*(dest)*	481007	PTrace		This IP message indicates that a packet has passed first-level reasonableness checks. The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.008 no rte *(source)* -> *(dest)* dsc	481008	Low		This IP message indicates that a packet is discarded because there is no route to the destination. The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
IP.009 TTL zero *(source)*-> *(dest)*	481009	Medium		This IP message indicates that a packet is discarded because the time-to-live expired. The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
IP.010 dsc pkt *(source)* -> *(dest)* nt *(net_id)* no IP	481010	PTrace		This IP message appears when a fake IP forwarder for each packet is received. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
IP.011 unsup mcst *(source)* -> *(dest)*	481011	Low		This IP message appears when an unsupported multicast packet is received. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
IP.012 bd nt cl *(source)*s -> *(dest)*	481012	Medium		This IP message indicates that a packet is destined for a network which is not class A, B, C, or D. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.013 unsup bcst *(source)*s -> *(dest)*	481013	Low		This IP message indicates that an unsupported broadcast packet was received. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address		This is an information message only. No corrective actions are required.
IP.015 bad subnet *(source)*s -> *(dest)*	481015	Medium		This IP message indicates that a packet cannot be routed because of an invalid subnet specification. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address		This is an information message only. No corrective actions are required.
IP.016 nt *(sub_add)* add fail, bd sbnt	481016	High		This IP message indicates that a network cannot be added to the routing table due to a bad subnet number. This subnet number is identified by the value *(sub_add)*.		This is an information message only. No corrective actions are required.
IP.017 nt *(net_add)* add fail, tbl ovrfl	481017	High		This IP message indicates a network cannot be added to the routing table because the table is full. The value *(net_add)* identifies the network address of the node affected.		This is an information message only. No corrective actions are required.
IP.018 nt *(net_add)* add fail, bd nt	481018	High		This IP message indicates a network cannot be added to the routing table because of a bad network number. The value *(net_add)* identifies the network address of the node affected.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.019 re-add stat rt to *(net)*	481019	Low		This IP message indicates a static route to a network was brought back into use. The value *(net)* identifies the network involved.		This is an information message only. No corrective actions are required.
IP.020 int for *(net)* add fail, dup addr	481020	High		This IP message indicates a network could not be added to the routing table due to denied access. The value *(net)* identifies the network involved.		This is an information message only. No corrective actions are required.
IP.022 add nt *(net_ip_add)* int *(int_ip_add)* nt *(net_id)*	481021	Low		This IP message indicates that a new directly connected network is added to the routing table. The value *(net_ip_add)* identifies the network IP Address, *(int_ip_add)* identifies the intermediate IP Address, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
IP.024 ign stat rt to *(net)*, mask *(mask)*	481024	Medium		This IP message indicates that a bad static route or IP filter is encountered. The value *(net)* identifies the network and *(mask)* identifies the network mask.		This is an information message only. No corrective actions are required.
IP.025 add nt *(new_net)* rt via *(cur_net)* nt *(net_id)*.	481025	Low		This IP message indicates that a new indirectly connected network is added to the routing table. The value *(new_net)* identifies the new network being added, *(cur_add)* identifies the current network that will support the new network, and *(net_id)* identifies the new overall network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.028 unnum stat rt on non-SL, *(nets)* thru *(nets)*	481028	Always		This IP message indicates that a static route has been configured with next hop of 0.0.0.x. However, x is not the interface number of an unnumbered serial line. The static route is ignored. The value *(nets)* identify networks involved.		This is an information message only. No corrective actions are required.
IP.031 Unnum addr rej, nt *(net_id)*	481031	Always		This IP message indicates that an attempt has been made to configure an unnumbered interface. However, the interface is not a serial line or the interface already has already been assigned an IP address. The unnumbered configuration request is ignored. The value *(net_id)* identifies the network involved.		This is an information message only. No corrective actions are required.
IP.032 fq ovf *(source)* -> *(dest)* nt *(net_id)*	481032	High		This IP message indicates that an incoming fragment has been discarded because the fragment queue overflowed. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address, and *(net_id)* identifies the network involved.		This is an information message only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
IP.033 cant frg *(source)*s -> *(dest)* nt *(net_id)*	481033	Medium		This IP message indicates that an outgoing packet needs to be fragmented but has the “Don't Fragment” bit set. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address, and *(net_id)* identifies the network involved.		This is an information message only. No corrective actions are required.
IP.034 bd frg *(source)* -> *(dest)* foff offset	481034	Medium		This IP message indicates that an outgoing packet has an invalid length of fragment offset. The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
IP.035 cant alloc for frg nt *(net_id)*	481035	High		This IP message indicates that there are no buffers available to fragment a packet. The value *(net_id)* identifies the network involved.		This is an information message only. No corrective actions are required.
IP.036 rcv pkt prt *(prot)* frm *(source)*	481036	PTrace		This IP message is generated for each packet destined for the router. the value *(prot)* identifies the protocol involved and (source) identifies the source IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.037 brd pkt *(source)* -> *(dest)* prot *(prot)* no srvr	481037	CTrace		This IP message indicates that a broadcast packet, for an unknown protocol, has arrived. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address, and *(prot)* identifies the protocol type.		This is an information message only. No corrective actions are required.
IP.038 pkt *(source)* -> *(dest)* prt *(prot)* no srvr	481038	Low		This IP message indicates that an unknown protocol packet has arrived. The packet was destined for the router. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address, and *(prot)* identifies the protocol type.		This is an information message only. No corrective actions are required.
IP.039 GGP echo frm *(source)* -> *(dest)*	481039	Low		This IP message is generated for each GGP echo packet. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
IP.040 GGP unhnd opc *(opcode)*, *(source)* -> *(dest)*	481040	Low		This IP message indicates that a GGP packet has arrived with an unhandled opcode. The value *(opcode)* identifies the unhandled opcode, *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.041 GGP bd opc *(opcode) (source) -> (dest)*	481041	Medium		This IP message indicates that a GGP packet arrived with an invalid opcode. The value *(opcode)* identifies the invalid op code, *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
IP.042 illgl ARP sbnt req *(source) -> (dest)*	481042	Medium		This IP alarm indicates that an ARP subnet request has not been honored due to illegal source or destination IP addresses in the ARP packet. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		To correct this problem, perform one of these activities: a) If there is no route to the requested subnet, determine why the subnet is not reachable. b) If the request is for a different IP network than the source address, correct the routing configuration in the host. ARP subnet routing is only for subnets of the host's network. c) Ensure that the IP network is subnetted. ARP subnet routing is only supported on subnets.
IP.043 rcvd ARP sbnt rqst *(source) -> (dest)*	481043	PTrace		This IP message indicates that an ARP subnet request has been received. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.044 ARP sbnt rqst ign *(source)* -> *(dest)*	481044	CTrace		This IP message indicates that an ARP subnet request has not been answered because the route to the target subnet is via another router, on the same physical network as the originator. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		ARP subnet routing code only responds when this router is the best route to the target subnet. The best router should respond to the ARP subnet request.
IP.045 snt ARP rte *(source)* -> *(dest)*	481045	Low		This IP message indicates that an ARP subnet request was answered. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
IP.046 unkn opt *(opt)* frm *(source)*	481046	Low		This IP message indicates that an unknown option is specified in the IP header of a packet. The value *(opt)* identifies the unknown option and *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.
IP.047 opt *(opt)* bd fmt frm *(source)*	481047	Medium		This IP message indicates that an option is incorrectly formatted in the IP header. The value *(opt)* identifies the unknown option and *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
IP.048 strict src rt bd nxt hop *(source)* -> *(dest)*	481048	Medium		This IP message indicates that the next hop specified in the strict source route is invalid. The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
IP.049 bd tmstmp fmt *(tstamp)* frm *(source)*	481049	Medium		This IP message indicates that the format of the timestamp option is invalid. The value *(tstamp)* identifies the time that this event occurred and *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.
IP.050 tmstmp ovrf, *(source)* -> *(dest)*	481050	Medium		This IP message indicates that the timestamp list is full and the new timestamp cannot be added. The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
IP.051 rs ovfl, *PORT (n)* frm *(source)*	481051	High		This IP message indicates that a new packet needs re-assembly although the maximum number of re-assembly buffers has already been assigned. The value *PORT (n)* identifies the port and *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.052 no stor for rs, *PORT (n)* frm *(source)*	481052	High		This IP message indicates that a new packet needs re-assembly although there is insufficient storage to allocate a re-assembly buffer. The value *PORT (n)* identifies the port and *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.
IP.053 reas pkt too big *(psize)*, *PORT (n)* frm *(source)*	481053	Medium		This IP message indicates that a new packet needs re-assembly but is larger than the maximum size re-assembly buffer. The value *(psize)* identifies packet size, in bytes, after adding this fragment. This fragment may not be the last to be added. The value *PORT (n)* identifies the port number and *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.
IP.054 rs TTL exp, *PORT (n)* frm *(source)*	481054	Low		This IP message indicates that the "time-to-live" timer has expired will a packet was being re-assembled. The value *PORT (n)* identifies the port number and *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.
IP.055 rs free, *PORT (n)* frm *(source)*	481055	PTrace		This IP message indicates that a re-assembly buffer is de-allocated. The value *PORT (n)* identifies the port number and *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.056 add dflt nt gw *(add)* nt *(net_id)*	481056	Low		This IP message indicates that an interface using a default gateway came up. The value *(add)* identifies the gateways IP address and *(net_id)* identifies the network involved.		This is an information message only. No corrective actions are required.
IP.058 del nt *(net)* rt via *(gate)* nt *(net_id)*	481058	Low		This IP message indicates that a network went down. The value *(net)* identifies the network routing, *(gate)* identifies the gateway IP address and *(net_id)* identifies the network involved.		This is an information message only. No corrective actions are required.
IP.059 sbnt *(net)* dfnd	481059	Low		This IP message indicates that a new subnetted network was defined. The value *(net)* identifies the network involved.		This is an information message only. No corrective actions are required.
IP.060 del sbntd nt *(net)*	481060	Low		This IP message indicates that a subnetted network was deleted. This happens when there are no longer any interfaces to that network. The value *(net)* identifies the network involved.		This is an information message only. No corrective actions are required.
IP.061 add lcl pkt to ip op q	481061	CTrace		This IP message indicates that a locally generated packet was put on the IP output queue.		This is an information message only. No corrective actions are required.
IP.062 rcvd ip frg frm *(source)*	481062	CTrace		This IP message indicates that an IP fragment, requiring re-assembly, was received. The value *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.063 rasmd pkt frm *(source)*	481063	CTrace		This IP message indicates that an IP packet has been successfully re-assembled. The value *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.
IP.064 frg pkt *(source)* -> *(dest)*	481064	CTrace		This IP message indicates that an IP packet must be fragmented before transmission. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
IP.065 add frg to op frg q *(source)* -> *(dest)*	481065	CTrace		This IP message indicates that an IP packet fragment has been put on the output fragment queue. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
IP.066 dsc pkt *(source)* -> *(dest)* nt *(net_id)* no IP on int	481066	PTrace		This IP message appears for the stub IP forwarder of each packet received on an interface for which IP is not enabled. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
IP.067 RIP disabld on int *(add)* var len sbnt msks	481067	Medium		This IP message indicates that the router is configured with variable length subnet masks on the same network, which RIP cannot handle; RIP is disabled on the interface. The value *(add)* identifies the interface IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.068 routing cache cleared	481068	Low		This IP message indicates that the IP routing cache has been cleared, probably as the result of a routing table change.		This is an information message only. No corrective actions are required.
IP.069 routing cache garbage collecting...	481069	Low		This IP message indicates that the IP routing cache is being garbage collected. This takes several passes and is only done when the cache starts overflowing.		This is an information message only. No corrective actions are required.
IP.070 cache entry *(dest)* cleared	481070	Low		This IP message indicates that the IP routing cache entry for the listed destination has been cleared. The value *(dest)* identifies the IP destination.		This is an information message only. No corrective actions are required.
IP.071 ARP sbnt rqst *(source)* -> *(dest)*, same sbnt, ign	481071	CTrace		This IP message indicates that an ARP subnet request was received for a host on the same subnet as it was received on. The router ignores this, since that node is on this subnet, and should respond on its own. This IP message also appears when the router sends an ARP request on a network where the hardware receives its own broadcasts. The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.072 LL broadcast *(source)* -> *(dest)*, discarded	481072	Medium		An attempt was made to forward an IP packet that was received as a link level broadcast/multicast. Such packets are not forwarded and are discarded without even sending back an ICMP message to the source. The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
IP.073 can't copy *(source)* -> *(dest)*, discarded	481073	High		This alarm indicates that an attempt to copy an incoming IGMP, ICMP, or multicast packet for internal processing has failed because a buffer was not available. The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address.		If possible, allocate additional memory for IORB buffers.
IP.074 Acc cont # *(acte)* cache *(action)*, *(source)* -> *(dest)*, prot *(proto)*	481074	Low		This alarm indicates that an incoming IP packet matches an entry in the Access Control cache. The value *(acte)* identifies the Access Control Table entry number that matched the packet. The value *(action)* identifies how the packet will be processed and will either be "dropped" or "passed". The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address. The value *(proto)* identifies the protocol number from the IP header.		This is an information message only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
IP.075 Acc cont # *(acte)* cache *(action)*, *(source)* -> *(dest)*, *(proto)* port *(srcprt)* -> *(dstprt)*	481075	Low		This alarm indicates that an incoming IP packet matches an entry in the Access Control cache. The value *(acte)* identifies the Access Control Table entry number that matched the packet. The value *(action)* identifies how the packet will be processed and will either be "dropped" or "passed". The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address. The value *(proto)* identifies the protocol and will have one of the following values; "TCP" or "UDP". The value *(srcprt)* identifies the source port and *(dstprt)* identifies the destination port.		This is an information message only. No corrective actions are required.
IP.076 Acc cont # *(acte)* *(action)*, *(source)* -> *(dest)*, port *(proto)*	481076	Low		This alarm indicates that an incoming IP packet matches an entry in the Access Control Table. The value *(acte)* identifies the Access Control Table entry number that matched the packet. The value *(action)* identifies how the packet will be processed and will either be "dropped" or "passed". The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address. The value *(proto)* identifies the protocol number from the IP header.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.077 Acc cont # *(acte) (action)*, *(source) -> (dest)*, *(proto)* port *(srcprt) -> (dstprt)*	481077	Low		This alarm indicates that an incoming IP packet matches an entry in the Access Control Table. The value *(acte)* identifies the Access Control Table entry number that matched the packet. The value *(action)* identifies how the packet will be processed and will either be "dropped" or "passed". The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address. The value *(proto)* identifies the protocol and will have one of the following values; "TCP" or "UDP". The value *(srcprt)* identifies the source port and *(dstprt)* identifies the destination port.		This is an information message only. No corrective actions are required.
IP.078 Acc cont miss dropped, *(source) -> (dest)*, port *(proto)*	481078	Low		This alarm indicates that an incoming IP packet has been dropped because Access Control Lists are enabled and this packet did not match any of the defined flows. The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address. The value *(proto)* identifies the protocol number from the IP header.		This is an information message only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
IP.079 Acc cont miss dropped, *(source)* -> *(dest)*, *(proto)* port *(srcprt)* -> *(dstprt)*	481079	Low		This alarm indicates that an incoming IP packet has been dropped because Access Control Lists are enabled and this packet did not match any of the defined flows. The value (source) identifies the source IP address and (dest) identifies the destination IP address. The value (proto) identifies the protocol number from the IP header. The value (proto) identifies the protocol and will have one of the following values; "TCP" or "UDP". The value (srcprt) identifies the source prot and (dstprt) identifies the destination port.		This is an information message only. No corrective actions are required.
IP.080	481080	Low		This alarm is not used in 5.5 or later releases.		Not used.
IP.081 shrt pkt ln *(len)*, *(source)* -> *(dest)*	481081	Medium		An IP packet has been received that is less than the minimum length. The value *(len)* identifies the length of the packet. The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IP.082 dsc ASB pkt *(source)* -> *(dest)* nt %d int %s/ %d not frm shortest path	481082	Low		This alarm indicates that an incoming All Subnet Broadcast (ASB) packet has been discarded because the rout to the source is via an interface other than the interface on which the packet was received. The packet is discarded to avoid looping as per RFC922. The value *(source)* identifies the source IP address and *(dest)* identifies the destination address.		This is an information message only. No corrective actions are required.
IP.083 ASB pkt *(source)* -> *(dest)* sending to nt %d int %s / %d	481083	Low		This alarm indicates that an incoming All Subnet Broadcast (ASB) packet has been received and routed successfully. The value *(source)* identifies the source IP address and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
IP.084	481084			This alarm is used for several purposes. Please contact customer service for information.		Contact Customer Service.
IP.085 addr *(dupaddr)* ->int *(intf)* may conflict with other addr in network	481085	Medium		The “Duplicate Address Detection” feature has determined that the address configured for an interface already exists in the network. The value *(dupaddr)* is the IP address that was being checked and *(intf)* is the interface number.		Assign a new IP address for the interface.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
IPCP negotiated address -*(x.x.x.x)*		Low		This report is generated when the IPCP has negotiated an address with the ISP. The value *(x.x.x.x)* identifies the negotiated address.		This is an information message only. No corrective actions are required.
IP Parameter Boot Complete		High		This IP message indicates that an IP Parameters Boot has been completed successfully.		This is an information message only. No corrective actions are required.
IP Parameter Boot Failed		High		This IP message indicates that an IP Parameters Boot has failed. This could be due to lack of memory. Parameters that require a node boot have been changed.		This is an information message only. No corrective actions are required.
IP Tables Boot Complete		High		This IP message indicates that an IP interface has been enabled by the user.		This is an information message only. No corrective actions are required.
IP Tables Boot Failed		High		This IP message indicates that an IP interface has been disabled by the user		This is an information message only. No corrective actions are required.
IPX.001 Packet from *(s_net) (s_node)* for *(d_net) (d_node)* ignored.	488001	PTrace		This IPX message indicates that an IPX packet arrived on a network and the IPX forwarder is not installed. The value *(s_net)* identifies the source network, *(s_node)* identifies the source node, *(d_net)* identifies the destination network, and *(d_node)* identifies the destination node.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.002 ovf *(s_net) (s_node) (d_net) (d_node)* nt *(net_id)*	488002	High		This IPX message indicates that an IPX forwarder input queue has overflowed, i.e., more packets are being received than the forwarder can forward. The value *(s_net)* identifies the source network, *(s_node)* identifies the source node, *(d_net)* identifies the destination network, *(d_node)* identifies the destination node, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
IPX.003 bd hst chksm frm *(s_net) (s_node)*	488003	Medium		This IPX message is generated whenever a packet arrives for this host with an incorrect checksum. The value *(s_net)* identifies the source network and *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.
IPX.004 err pkt *(type)* frm *(s_net) (s_node)*	488004	Low		This IPX message is generated when an error packet is received. The value (type) identifies the error type, *(s_net)* identifies the source network, and *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
IPX.005 no hndlr for skt *(dest_soc)* typ *(type)* frm *(s_net)* *(s_node)*	488005	CTrace		This IPX message indicates that an error packet is received. A packet arrived for an unknown or unsupported socket or type. The packet was a broadcast packet. The value *(dest_soc)* identifies the destination socket, *(type)* identifies the packet type, *(s_net)* identifies the source network and *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.
IPX.006 *(dest_soc)* typ *(type)* frm *(s_net)* *(s_node)*	488006	Medium		This IPX message indicates that a packet arrived for an unknown or unsupported socket or type. The packet was addressed to the router. The value *(dest_soc)* identifies the destination socket, *(type)* identifies the packet type, *(s_net)* identifies the source network and *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.
IPX.007 no host address set for net *(net_id)*, not enabled	488007	Medium		This IPX alarm indicates that a forwarder was bringing up IPX on the specified serial line interface, but no host address was set so the interface was not enabled. The serial line enabled without setting the host address. The value *(net_id)* identifies the network.		Configure an IPX host address.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.008 SAP bad type *(type) (s_net) (s_node)*	488008	Medium		This IPX message indicates that a packet has been received with a bad SAP type. The value *(type)* identifies the packet type, *(s_net)* identifies the source network and *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.
IPX.009 SAP gen reply from *(s_net) (s_node)*	488009	CTrace		This IPX message indicates that SAP has received a General Reply packet from the specified host. The data in the packet is used to update the SAP database. The value *(s_net)* identifies the source network and *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.
IPX.010 SAP table overflow, discarded type *(type) (name)*	488010	High		This IPX alarm indicates that the SAP table is full and a new entry cannot be added; the new entry is discarded. The SAP table is smaller than the number of services on IPX internet. The value *(type)* identifies the service type and *(name)* identifies the service name.		Increase the size of the SAP table.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.011 SAP service type *(type) (name)* moved to *(new_net) (new_node)*	488011	Medium		This IPX alarm indicates that a SAP General Reply was received with a different network/address pair than is presently in the SAP database. Duplicate name assigned for service or service physically moved faster than SAP timeout. The value *(type)* identifies the service type, *(name)* identifies the service name, *(new_net)* identifies the new network name, and *(new_node)* identifies the new nodename.		To correct this problem, eliminate duplicated name or do not move services so fast.
IPX.012 SAP deleted type *(type) (name)*	488012	Low		This IPX message indicates that a SAP table entry has been declared dead. It will be advertised as unreachable for another 60 seconds, and then removed from the SAP table. No SAP General Reply has been heard containing data on this service type/name pair in 240 seconds. The value *(type)* identifies the service type and *(name)* identifies the service name.		No corrective actions are required unless this service should be up. If so, bring up the network.
IPX.013 SAP bad length Nearest Service Query from *(s_net) (s_node)* length	488013	Medium		This IPX message indicates that a SAP Nearest Service Query was received with an illegal length programming error in the remote node. This query should be tagged as defunct. The value *(s_net)* identifies the source network and *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.014 SAP nearest query from *(s_net) (s_node)*	488014	CTrace		This IPX message indicates that a SAP Nearest Service Query was received from the specified node. It will be answered as appropriate. The value *(s_net)* identifies the source network and *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.
IPX.015 SAP General query from *(s_net) (s_node)*	488015	Low		This IPX message indicates that a SAP General Query was received from the specified node. It will be answered as appropriate. The value *(s_net)* identifies the source network and *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.
IPX.016 SAP general Service Query sent, net *(net_id)*	488016	UTrace		This IPX message indicates that a SAP General Service Query was sent on the specified network. One is sent on a network when it comes up. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
IPX.017 No memory for SAP General Service Query of Reply, net *(net_id)*, *(count)* packet sent	488017	Low		This IPX message indicates that there are no buffers available to send a SAP General Service Query or Reply packet. Since a General Service Reply can require multiple packets, the message notes how many packets were sent on this network before they ran out. The value *(net_id)* identifies the network and *(count)* identifies the number of packets sent.		This is an information message only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
IPX.018 SAP General Service Reply sent, net *(net_id)*, *(count)* packets	488018	CTrace		This IPX message indicates that a SAP General Service Reply has just been sent on the specified network. It took the specified number of packets to send the complete SAP database. The value *(net_id)* identifies the network and *(count)* identifies the number of packets.		This is an information message only. No corrective actions are required.
IPX.019 NB brd *(s_net) (s_node) -> (d_net) (d_node)*, nt *(net_id)*, *(count)* hops	488019	PTrace		This IPX message indicates that a NETBIOS emulation multi-network broadcast packet has been received for forwarding to other IPX networks. The IPX hop count indicates how many routers it has been through. The value *(s_net)* identifies the source network, *(s_node)* identifies the source node, *(net_id)* identifies the network, and *(count)* identifies the number of hops (routers) the packet has been through.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.020 NB too many hops frm *(s_net) (s_node)* nt *(net_id)*, ign	488020	Medium		This IPX message indicates that a NETBIOS emulation broadcast packet has been through more than 8 routers. It will be dropped. Normal looping due to multiple paths from source of broadcast packet. IPX NETBIOS traffic trying to go across more than 8 hops (networks) between source and destination. The value *(s_net)* identifies the source network, *(s_node)* identifies the source node, and *(net_id)* identifies the network		This is an information message only. No corrective actions are required. This is a normal consequence of the protocol used. However, if IPX NETBIOS traffic goes across more than 8 hops (networks) between the source and destination, the network must be reconfigured
IPX.021NETBIOS from *(s_net) (s_node)* net *(net_id)*, already *(con_net)*	488021	CTrace		This IPX message indicates that a IPX NETBIOS emulation broadcast packet has already been on one of the directly attached networks. It will not be forwarded, as that would generate a duplicate. This is a normal side-effect of the protocol used. The value *(s_net)* identifies the source network, *(s_node)* identifies the source node, and *(net_id)* identifies the network, and *(con_net)* identifies the directly connected network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.022 NETBIOS from *(s_net) (s_node)*, no memory to copy	488022	Low		This IPX message indicates that there is insufficient memory available to make a working copy of this NETBIOS emulation packet to send it out on multiple interfaces. The value *(s_net)* identifies the source network and *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.
IPX.023 NETBIOS from *(s_net) (s_node)*, non-broadcast net *(net_id)* unsupported	488023	High		This IPX message indicates that an attempt has been made to send the NETBIOS emulation packet on a network that does not support broadcast. The packet is not sent on that network. The value *(s_net)* identifies the source network, *(s_node)* identifies the source node, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
IPX.024 NETBIOS from *(s_net) (s_node)*, unnumbered net *(net_id)* unsupported	488024	Low		This IPX message indicates that an attempt has been made to send NETBIOS emulation packet on a network with no network number. The packet is not sent on that network. Serial line network operating without a network number. The value *(s_net)* identifies the source network, *(s_node)* identifies the source node, and *(net_id)* identifies the network.		If you want to run NETBIOS emulation across a serial line network, it must have a network number.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.025 NETBIOS from *(s_net)* *(s_node)*, no buffer to copy	488025	Low		This IPX message indicates that there are packet buffers available to copy this NETBIOS emulation broadcast packet to or send it on a network. The value *(s_net)* identifies the source network and *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.
IPX.026 NB and dsc, nt *(net_id)* , rsn *(cause)*	488026	Low		This IPX alarm indicates that an outgoing NETBIOS emulation broadcast packet was not successfully transmitted. The value *(net_id)* identifies the network involved and *(cause)* identifies the cause code (code 1 through code 5) for this failure.		To correct this problem: a) For cause code #1; Check for error messages from handler for network ID, a Miscellaneous Handler Error may have occurred. b) For cause code #2; An output queue has overflowed, or there are other flow control problems. Correct the congestion condition. c) For cause code #3; The network is down. Identify why the handler thinks the network is down. d) For cause code #4; The packet was dropped by the handler to avoid looping, or bad broadcast. Check configuration. e) For cause code #5; The host is down. identify why the handler thinks the host is down.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.027 bd RIP typ *(RIP_opcode)* frm *(s_net) (s_node)*	488027	Medium		This IPX alarm indicates that a RIP packet has been received which was not a request or response. The value *(RIP_opcode)* identifies the RIP operation code, *(s_net)* identifies the source network and *(s_node)* identifies the source node.		Check for configuration errors on the remote node.
IPX.028 RIP resp frm *(s_net) (s_node)*	488028	CTrace		This IPX message indicates that a RIP response packet has been received. It is parsed, and the data incorporated into the routing table. The value *(s_net)* identifies the source network and *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.
IPX.029 bd nt network in RIP frm *(s_net) (s_node)*	488029	Medium		This IPX alarm indicates that a RIP response has been received with an entry having a network number of 00000000 or FFFFFFFF. This entry is ignored. The value *(s_net)* identifies the source network and *(s_node)* identifies the source node.		Check for configuration errors on the remote node.
IPX.030 nt rttbl ovrfl, dscrd *(net)*	488030	Medium		This IPX alarm indicates that a new network cannot be added to the routing table because it is full. The entry is discarded. The value *(net)* identifies the network.		The routing table too small. Reconfigure IPX protocol to make routing table larger.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.031 nw rt to *(net)* via *(router_net)*, *(router_node)*, *(count)* hops	488031	Low		This IPX alarm indicates that the route to a network changes. The specified router_net/router_node is now the best route to this network, with the noted number of hops. The value *(net)* identifies the network, *(router_net)*, identifies the routers network, *(router_node)* identifies the node, and *(count)* identifies the number of hops.		This may result from a newly reachable network (if preceded by message IPX.055). Change in network topology causes best route to a network to change. This can happen when networks come up or go down. Determine what changes in network topology occurred.
IPX.032 rt to network aged away	488032	Low		This IPX alarm indicates that a network has been declared unreachable because no routing updates have been received from it in 240 seconds. It will be advertised as unreachable for another 60 seconds, and then deleted from the routing table.		Verify that the intervening router that was advertising this network has crashed and repair as required.
IPX.033 Rspnd to RIP rqst frm *(s_net)*, *(s_node)*	488033	CTrace		This IPX alarm indicates that a RIP Request packet is being parsed for a Reply. The value *(s_net)* identifies the source network and *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.
IPX.034 RIP rqst frm *(s_net)*, *(s_node)* shrt, In (*pac_len)*	488034	Medium		This IPX alarm indicates that a RIP request packet was discarded because it was too short to contain one RIP entry. The value *(s_net)* identifies the source network, *(s_node)* identifies the source node, and *(pac_len)* identifies the packet length.		Check for programming errors on the remote node.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
IPX.035 RIP Query sent, net *(net_id)*	488035	UTrace		This IPX message indicates that a RIP Query has been sent on the specified interface. A Query is sent on each interface when it comes up. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
IPX.036 no mem for RIP pkt nt *(net_id)*, *(count)* pkts sent	488036	Low		This IPX message indicates that there are no buffers available to send a RIP Query or Response packet. The value *(net_id)* identifies the network and *(count)* identifies the number of packets sent.		This is an information message only. No corrective actions are required.
IPX.037 RIP resp sent nt *(net_id)* *(count)* pkts	488037	CTrace		This IPX message indicates that a RIP Response has been sent. The response was sent in the specified number of packets. The value *(net_id)* identifies the network and *(count)* identifies the number of packets sent.		This is an information message only. No corrective actions are required.
IPX.038 *(s_net)* *(s_node)* *(d_net)* *(d_node)* ign	488038	UTrace		This IPX message indicates that an IPX packet has arrived on a network and the IPX forwarder is not active on that network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.039 RIP delta resp sent nt *(net_id)*, *(count)* pkts	488039	CTrace		This IPX message indicates that a RIP delta Response has been sent. This response only includes those networks whose data changed in the last update period. The response was sent in the specified number of packets. The value *(net_id)* identifies the network and *(count)* identifies the number of packets sent.		This is an information message only. No corrective actions are required.
IPX.040 RIP resp snd dsc, nt *(net_id)*, rsn *(cause)*	488040	Low		This IPX alarm indicates that an outgoing RIP response packet was not successfully transmitted for the reason indicated by the error code. The value *(net_id)* identifies the network and *(cause)* identifies the cause of this problem.		To correct this problem: a) Check for error messages from handler for network ID. b) Check the configuration. c) See why handler thinks host is down.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX_041 RIP query snd dsc, nt *(net_id)*, rsn *(cause)*	488041	Low		This IPX alarm indicates that an outgoing RIP query packet was not successfully transmitted. The value *(net_id)* identifies the network and *(cause)* identifies the cause of this failure.		To correct this problem: a) Check for error messages from handler for network ID, a Miscellaneous Handler Error may have occurred. b) An output queue has overflowed, or there are other flow control problems. Correct the congestion condition. c) The network is down. Identify why the handler thinks the network is down. d) The packet was dropped by the handler to avoid looping, or bad broadcast. Check configuration. e) The host is down. identify why the handler thinks the host is down.
IPX_042 SAP gives near reply typ *(type)* nm *(name)* to *(s_net)* *(s_node)*, *(net_id)*	488042	CTrace		This IPX alarm indicates that a SAP Nearest Service Reply will be sent to the specified node. The value *(type)* identifies the service type and *(name)* identifies the service name, *(s_net)* identifies the source network, *(s_node)* identifies the source node, and *(net_id)* identifies the network ID.		Node sent Nearest Server Request, and the nearest server of that type is reachable through this router.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX_043 SAP nearest qry for typ *(type)* frm *(s_net)* *(s_node)* nt *(net_id)*	488043	CTrace		This IPX alarm indicates that a SAP Nearest Service Query was received from the specified node via the specified interface. If this router is the best route to the closest server of the specified service_type, this router will answer. The value *(type)* identifies the service type, *(s_net)* identifies the source network, *(s_node)* identifies the source node, and *(net_id)* identifies the network ID.		New IPX node booting on an attached LAN, looking for a first file server (service_type of 4). Or: Node attempting to locate a particular server by service type such as a communications server or database server.
IPX.044 SAP delta gen rply nt *(net_id)*, *(count)* pkts	488044	CTrace		This IPX message indicates that a SAP delta General Service Reply has just been sent on the specified network. This Reply only includes those services whose data changed in the last update period. It took the specified number of packets to send the changes in the SAP database. The value *(net_id)* identifies the network and *(count)* identifies the number of packets sent.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.045 SAP new serv typ *(type)* nm *(name)* via *(net)* *(node)*, *(count)* hops, nt *(net_id)*	488045	Low		This IPX message indicates that a new service has been added to the SAP table. The specified via_net/ via_node is the route to this service, with the noted number of hops. Existing service becomes reachable, due to change in network connectivity. The value *(type)* identifies the service type, *(name)* identifies the service name, *(net)* identifies the network, *(node)* identifies the node, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
IPX.046 SAP nearest qry frm *(s_net)* *(s_node)* ignored, nt *(net_id)*	488046	UTrace		A SAP Nearest Service Query was received from the specified node via the specified interface, but processing of these packets has been administratively disabled on this interface. The query will be ignored. The value *(s_net)* identifies the source network, *(s_node)* identifies the source node, and *(net_id)* identifies the network.		The IPX Config command DISABLE REPLY-TO-GET-NEAREST-SERVER has been used. If this is the desired action, then no other actions are required. To enable a default response, use the IPX Config command ENABLE REPLY-TO-GET-NEAREST-SERVER.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.047 SAP query snd dsc, nt *(net_id)*, rsn *(cause)*	488047	Low		This IPX alarm indicates that an outgoing SAP query packet was not successfully transmitted. The value *(net_id)* identifies the network and *(cause)* identifies the reason for this failure.		To correct this problem: a) Check for error messages from handler for network ID, a Miscellaneous Handler Error may have occurred. b) An output queue has overflowed, or there are other flow control problems. Correct the congestion condition. c) The network is down. Identify why the handler thinks the network is down. d) The packet was dropped by the handler to avoid looping, or bad broadcast. Check configuration. e) The host is down. identify why the handler thinks the host is down.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.048 SAP resp snd dsc, nt network ID, rsn *(cause)*	488048	Low		This IPX alarm indicates that an outgoing SAP response packet was not successfully transmitted. The value *(cause)* identifies the reason for this failure.for the reason indicated by the error code.		To correct this problem: a) Check for error messages from handler for network ID, a Miscellaneous Handler Error may have occurred. b) An output queue has overflowed, or there are other flow control problems. Correct the congestion condition. c) The network is down. Identify why the handler thinks the network is down. d) The packet was dropped by the handler to avoid looping, or bad broadcast. Check configuration. e) The host is down. identify why the handler thinks the host is down.
IPX.049 SAP no serv typ *(type)* for *(s_net)* *(s_node)* , nt *(net_id)*	488049	UTrace		This IPX alarm indicates that a SAP Nearest Service Query was received from s_net/s_node, but the SAP database has no service registered of the desired service_type. The value *(type)* identifies the service type, *(s_net)* identifies the source network, *(s_node)* identifies the source node, and *(net_id)* identifies the network.		To correct this problem: a) Identify why the desired service_type is down or unreachable. b) The workstation may be looking for a nonexistent service type. Correct query on workstation.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.050 SAP dead serv type *(type)* nm *(name)* from *(net)* *(node)*, nt *(net_id)*	488050	Low		This IPX alarm indicates that a previously reachable service has become unreachable, and is marked as Dead in the SAP table. The specified via_net/via_node is the server or router that announced the service as being unreachable. The value *(type)* identifies the service type, *(name)* identifies the service name, *(net)* identifies the network, *(node)* identifies the node, and *(net_id)* identifies the network. There are three possible causes for this alarm: a) The server has been administratively disabled. b) The server has crashed. c) The network on which the service is provided has become unreachable		To correct this problem, determine the cause and correct as indicated below: a) No corrective actions are required if the server has been administratively disabled. b) Identify the cause of a server crash and correct as necessary. c) Use the IPX console DUMP command to see if the network is reachable.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.051 RIP route died to network from *(router_net)* *(router_node)*	488051	Low		This IPX alarm indicates that a previously reachable network becomes unreachable, and is marked as Dead in the RIP table. The values *(router_net)* *(router_node)* identify the router that announced the network as being unreachable. There are three possible causes for this failure: a) The remote network, or intervening network has gone down. b) The network is on the router that has failed. c) The network is connected through a file server that has been taken down administratively.		To correct this problem, determine the cause and correct as indicated below: a) Identify the cause of the remote network failure and correct as necessary. b) Identify why the remote router failed and correct as necessary. c) If the file server has been taken down administratively there are no corrective actions required.
IPX.052 RIP resp frm wrong *(s_net)* *(s_node)* not *(local_net)*, nt *(net_id)*	488052	Medium		This IPX alarm indicates that a RIP response packet has been received with a source network number that is not the same as the network number of this interface. The packet will be ignored. The value *(s_net)* identifies the source network, *(s_node)* identifies the source node, *(local_net)* identifies the local network, and *(net_id)* identifies the current network.		Check and correct the router configuration.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
IPX.053 SAP resp frm wrong net *(s_net)* *(s_node)* not *(local_net)*, nt *(net_id)*	488053	Medium		This IPX alarm indicates that a SAP response packet has been received with a source network number that is not the same as the network number of this interface. The packet will be ignored. The value *(s_net)* identifies the source network, *(s_node)* identifies the source node, *(local_net)* identifies the local network, and *(net_id)* identifies the current network.		Check and correct the router configuration.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.054 SAP serv typ *(type)* nm *(name)* now via *(net)* *(node)*, *(count)* hops, nt *(net_id)*	488054	Low		This IPX alarm indicates the route to a service in the SAP table changes. The specified network/ node is the new route to this service, with the noted number of hops. The value *(type)* identifies the service type, *(name)* identifies the service name, *(net)* identifies the transport network, *(node)* identifies the network node, *(count)* identifies the number of hops, and *(net_id)* identifies the network. There are two possible causes for this failure: a) This is a newly reachable service when the alarm is proceeded by IPX.045. b) Changes have been made in the network topology. This has caused a change in the best route to a service. (This can happen when new networks come up or go down.)		To correct this problem perform one of these steps: a) If this is a newly reachable service, no corrective actions are required. b) Determine what changes in network topology occurred and address them in you network configuration.
IPX.055 new RIP net network via *(router_net)* *(router_node)* *(count)* hops	488055	Low		This IPX message indicates that a new network has been added to the RIP routing table. The new network was advertised by router_net/router_node, which is now the route to this network, with the noted number of hops.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.056 RIP route to network garbage coll	488056	UTrace		This IPX message is generated when a network is removed from the RIP routing table because no routing updates have been heard for it in 300 seconds. This normally happens 60 seconds after an IPX.012 message on the same service.		This is an information message only. No corrective actions are required.
IPX.057 SAP del typ *(type)* nm *(name)*, nt *(net_id)* down	488057	Low		The specified network interface has gone down, and this SAP service having a first hop on that network will be placed in the dead state. It will be advertised as unreachable for another 60 seconds, and then removed from the SAP table. However, if there are alternate routes to the same service, they will be learned about within 60 seconds. The value *(type)* identifies the service type, *(name)* identifies the service name, and *(net_id)* identifies the network.		The network via which we reached this service went down. Bring up network.
IPX.058 SAP typ *(type)* nm *(name)* garbage coll	488058	UTrace		This IPX message is generated when a network is removed from the SAP routing table because no SAP responses have been heard for it in 300 seconds. The value *(type)* identifies the service type, *(name)* identifies the service name, and *(net_id)* identifies the network.		Verify that the intervening router that was advertising this service has gone down and repair as required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.059 SAP unreach serv typ *(type)* nm *(name)* at *(serv_net)* *(serv_node)* from *(via_net)* *(via_node)* , nt *(net_id)*	488059	Medium		This IPX message is generated when an advertisement for a service is received, but that service is on an IPX network that this router has no route to. This advertisement is ignored. The value *(type)* identifies the service type, *(name)* identifies the service name, *(serv_net)* identifies the IPX network, *(serv_node)* identifies the IPX node, *(via_net)* and *(via_node)* identify the network and node through which the advertisement travels, and *(net_id)* identifies the network.		Correct the node configuration error. Service information for some new service has propagated faster than the associated routing information. No action is required if service_net becomes reachable shortly, and this message does not repeat.
IPX.060 SAP periodic GSR starting	488060	CTrace		The SAP protocol is beginning the transmission of SAP General Service Response packets on all IPX interfaces. This happens approximately every 60 seconds. It will generally be followed by IPX.064 messages (if there are any services), followed by an IPX.061 message.		This is an information message only. No corrective actions are required.
IPX.061 SAP periodic GSR completed, *(count)* pkts	488061	CTrace		The SAP protocol has completed the transmission of the periodic SAP General Service Response packets on all IPX interfaces. In doing this, it attempted to send packet_count packets in total. The value *(count)* identifies the number of response packets sent.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPX.062 No mem for SAP periodic GSR pkt *(count),* delaying, nt *(net_id)*	488062	High		There was no packet buffer available to send one packet of the periodic SAP General Service Response. The response will stall for half a second, waiting for a buffer to become available. The value *(count)* identifies the packet number, within the complete response, starting at 0 and *(net_id)* identifies the network.		This problem could be as a result of temporary packet buffer shortages due to traffic peak. See if message recurs after half a second. The possibility exists that there may be a permanent buffer shortage. Copy the router configuration and contact your customer service representative.
IPX.063 SAP periodic GSR snd dsc, nt *(net_id)*, rsn *(code)*	488063	High		This IPX alarm indicates that an outgoing SAP periodic General Service Response packet was not successfully transmitted for the reason indicated by the error code. The value *(net_id)* identifies the network and *(code)* identifies the reason for this error.		To correct this problem: a) Check for error messages from handler for network ID, a Miscellaneous Handler Error may have occurred. b) An output queue has overflowed, or there are other flow control problems. Correct the congestion condition. c) The network is down. Identify why the handler thinks the network is down. d) The packet was dropped by the handler to avoid looping, or bad broadcast. Check configuration. e) The host is down. identify why the handler thinks the host is down.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
IPX.064 SAP periodic GSR sent, *(count)* entries, nt *(net_id)*	488064	PTrace		This IPX alarm indicates that an SAP periodic General Service Reply packet has just been sent on the specified network. The value *(count)* identifies the number of services in the packet and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
IPX Parameters Boot Complete		High		This IPX message indicates that an IPX Parameters Boot has been successfully completed.		This is an information message only. No corrective actions are required.
IPX Parameters Boot Failed		High		This IPX message indicates that an IPX interface Boot has failed. This could be due to a lack of memory. Parameters that require a node boot have been changed.		This is an information message only. No corrective actions are required.
IPX Tables Boot Complete		High		This IPX message indicates that an IPX interface has been enabled.		This is an information message only. No corrective actions are required.
IPX Tables Boot Failed		High		This IPX message indicates that an IPX Interface has been disabled.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Error in ATMARP Packet received on *LCON (n) - (msg), (field)* (Continued)		Debug	Warning	• Bad Source/Target Protocol Length. A Source/Target Protocol Field is non null and not equal to 4. • Bad Source/Target ATM Number/Subaddress Length. The length of a Source/Target ATM Number/Subaddress is greater than 20. • Bad Source/Target ATM Number/Subaddress Type. a Source/Target ATM Number/ subaddress with an invalid type. • Invalid ATM Structure. A Source/Target ATM Address is in an Invalid ATM structure format.		To correct these problems, identify the remote node that is generating the errorneous InATMARP packet and correct it as required by the message indicated. **■ Note** This is a debug alarm and should not normally appear unless your Vanguard product has been configured with Debug turned on.
Unsupported or invalid Protocol Packet received on rfc1483_LLC_SNAP *LCON (n)*		Debug	Warning	This report indicates that an unsupported protocol type exists on a packet. This packet has been received on a specific LCON using RFC1483 LLC/SNAP Encapsulation. The value *LCON (n)* identifies the LAN Connection involved.		Change the LCON's encapsulation type to match the traffic type in question.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Bridged or Routed packet received with invalid rfc1483 encapsulation on *LCON (n)*		Debug	Warning	This report indicates that a bridged or routed packet has been received. This packet has either an incomplete RFC1483 encapsulation or an invalid value in the LLC or SNAP header. The value *LCON (n)* identifies the LAN Connection involved.		Identify the remote node that is generating packets with the invalid RFC1483 encapsulation and correct it.
Not Enough memory - *(msg)*		High	Critical	This report indicates that sufficient memory is unavailable to support RFC1483 encapsulation. The value *(msg)* identifies an error message describing the consequences of a memory allocation failure.		To correct this problem: a) Install additional DRAM in your Vanguard device. b) Disable some of the other software features that not currently being used.
AAM- *PORT (n)* - PORT INITIALIZATION FAILED - *(cause)*		High	Critical	This ATM alarm is generated when sufficient memory is unavailable to create a running version of the AAM port. The value *PORT (n)* identifies the AAM port and *(cause)* identifies the reason for the failure: • INVALID PORT CONFIGURATION		This is a condition that does not change for any configuration. To correct this situation either: • Install additional memory in your Vanguard device. • Reduce the size of your software image.
AAM- *PORT (n)* - OUT OF MEMORY - SOME STATIONS NOT CREATED		High	Critical	This ATM alarm is generated whenever insufficient memory is available to create a running version of an AAM station on an existing port. The value *PORT (n)* identifies the AAM port.		This is a condition that does not change for any configuration. To correct this situation either: a) Install additional memory in your Vanguard device. b) Reduce the size of your software image.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
AAM- *PORT (n)* - PORT STATUS WARNING - PORT DISABLED		High		This ATM message appears whenever a port running version has been created (node boot or power on events) and the port is in a disabled status. The value *PORT (n)* identifies the AAM port.		This is an information message only. No corrective actions are required.
AAM- *PORT (n)* - PORT BOOT COMPLETE		High		This report indicates that an AAM port boot is complete. The value *PORT (n)* identifies the AAM port.		This is an information message only. No corrective actions are required.
AAM- *PORT (n)* - PORT BOOT FAILURE - *(cause)*		High	Critical	This ATM alarm indicates that a port boot was not successful. The value *PORT (n)* indicates the AAM port and *(cause)* identifies one of these reasons for the failure: • RUNNING PORT TYPE IS NOT AAM • NO PORT CONFIGURATION • CONFIGURED PORT TYPE IS NOT AAM • PORT DISABLED		To correct this problem check that: a) The correct port number has been entered, b) The port has a valid configuration record, c) The port is not disabled.
AAM- *PORT (n)* - PORT DISABLED		High		This message appears whenever a port disable operation has been completed. The value *PORT (n)* identifies the AAM Port that has been disabled.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
AAM- *PORT (n)* - PORT ENABLED		High		This message appears whenever a port enable operation has been completed. The value *PORT (n)* identifies the AAM Port that has been enabled.		This is an information message only. No corrective actions are required.
AAM- *PORT (n) STATION (s)* - STATION BOOT COMPLETE		High		This message appears whenever a station boot operation has been completed. The value *PORT (n)* identifies the AAM Port and *STATION (s)* the specific station that has been booted.		This is an information message only. No corrective actions are required.
AAM - *PORT (n) STATION (s)* - STATION BOOT FAILURE - *(cause)*		High	Critical	This ATM alarm indicates that a station boot was not successful. The value *PORT (n)* identifies the AAM Port, *STATION (s)* the specific station, and *(cause)* identifies one of these reasons for the failure: • RUNNING PORT TYPE IS NOT AAM • NO PORT CONFIGURATION • CONFIGURED PORT TYPE IS NOT AAM • STATION NOT RUNNING • NO STATION CONFIGURATION • PORT DISABLED • STATION DISABLED		To correct this problem check that: a) The correct port and station number have been entered b) The port and station have valid configuration records. c) Neither the port or station are disabled

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
AAM - *PORT (n) STATION (s)* - STATION DISABLED		High		This message appears when a station disable operation has been completed. The value *PORT (n)* identifies the AAM Port, *STATION (s)* the specific station that has been disabled.		This is an information message only. No corrective actions are required.
AAM - *PORT (n) STATION (s)* - STATION ENABLED		High		This message appears when a station enable operation has been completed. The value *PORT (n)* identifies the AAM Port, *STATION (s)* the specific station that has been enabled.		This is an information message only. No corrective actions are required.
AAM- *PORT (n)* - PORT UTILIZATION > THRESHOLD		Medium		This alarm indicates that the level of data traffic on this port exceeds the node's configured report threshold level. The vFalue *PORT (n)* identifies the port number,		Perform one of these actions to correct this problem: a) Set the reporting threshold in the node's configuration to a higher level. b) Redistribute the port's data traffic.
AAM - *PORT (n) STATION (s)* - ATM STATION UP	406002	Medium		This alarm indicates that a station is ready to pass data. The value *PORT (n)* identifies the port number and *STATION (s)* identifies the station that will pass the data.		This is an information message only. No corrective actions are required.
AAM - *PORT (n) STATION (s)* - ATM STATION DOWN	406003	High		This alarm indicates that a station has entered a state where it can not pass data. The value *PORT (n)* identifies the port number and *STATION (s)* identifies the station that will pass the data.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
AAM - *PORT (n)* - ATM PORT UP		High		This alarm indicates that an ATM port has become operational. The value *PORT (n)* identifies the port number.		This is an information message only. No corrective actions are required.
AAM - *PORT (n)* - ATM PORT DOWN		High		This alarm indicates that an ATM port is not operational. The value *PORT (n)* identifies the port number.		This is an information message only. No corrective actions are required.
AAM - *PORT (n)* CANNOT CREATE VCC FOR VPI *(vpi)* VCI *(vci)*		High		This alarm indicates that a software problem has developed and the hardware has failed to initialize hardware and create the VCC. The value *PORT (n)* identifies the port number, *(vpi)* identifies the Virtual Path Identifier and *(vci*) identifies the Virtual Circuit Identifier.		To correct this problem boot the node.
INCOMING CALL FROM *(call num)* ON BRI INTER-FACE *(I/F #1)* B *(I/F #2)* CHANNEL		Code		This message indicates that there is an incoming phone call on either the B1 or B2 channel. It is displayed when the dial call is established. The value *(call num)* identifies the calling phone number (this may also appear as Unknown), *(I/F #1)* identifies BRI Interface Number 1, 2, or 3, and *(I/F #2)* identifies the B Channel 1 or 2.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
INCOMPATIBLE *(h)* DETECTED FOR ISDN		High		This ISDN alarm indicates that ISDN will not activate because the wrong motherboard/ daughtercard revision has been detected. The value *(h)* identifies either the Motherboard or Daughtercard.		To correct this problem, replace the board indicated in the alarm message, with compatible hardware. **Note** Refer to the ISDN compatibility chart located in the *Vanguard Daughtercard Installation Instructions* (Part Number T0020) for additional information
xx IS CONNECTED TO ANOTHER AP, COMPRESSION IS NOT ALLOWED		High		This alarm indicates that both source and destination channels are configured as AP. Data compression is not supported for such configurations. When data compression is configured, the network port must be configured as NP.		To correct this problem, either: • Disable data compression on both endpoints, or • Configure the network port as NP.
ARP.001 Q ovf nt *(net)*	485001	Low		This alarm indicates that an ARP packet was discarded, rather than being queued, because the queue of unprocessed ARP packets was too long. This means that ARP packets are arriving faster than they can be processed. The value *(net)* identifies the network.		Prevail on the appropriate host manufacturer to bring their software into compliance with the specification. In the short term, it may be possible to disable the source of the packets, or cause it to use an address that the misbehaving hosts do recognize as a broadcast.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
ARP.002 Pkt in *(op_type) (hwd_add) (type)* nt *(net_id)*	485002	PTrace		This message indicates that an ARP packet of the type indicated has just arrived for processing. The value *(op_type)* identifies the type of operation, *(hwd_add)* identifies the hardware address, *(type)* identifies the protocol type, and *(net_id)* provides the network identifier.		This is an information message only. No corrective actions are required.
ARP.003 Unkwn hdw *(hwd_add)* nt *(net_id)*	485003	Low		This alarm indicates that an incoming ARP packet was received on a network that is not using ARP for address translation in any protocol. The value *(hwd_add)* identifies the hardware address and *(net_id)* provides the network identifier.		The gateway is misconfigured. Correct the configuration.
ARP.004 Bd hdw *(hwd_add) (add_len)* nt *(net_id)*	485004	Medium		This alarm indicates that an incoming ARP packet was received with a hardware address space code or hardware address length which does not match the one which should be used on that network. The value *(net_id)* identifies the hardware address, *(add_len)* identifies the length of the hardware address, and *(net_id)* provides the network identifier.		Use a network management tool to detect the source host and contact the manufacturer of that equipment to report the problem.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ARP.005 Unkwn prt *(type)* nt *(net_id)*	485005	PTrace		This alarm indicates that an incoming ARP packet was received for a protocol for which the router is not using ARP for address translation. The value *(type)* identifies the protocol type and *(net_id)* provides the network identifier.		The gateway is misconfigured. Correct the configuration.
ARP.006 Bd prt *(type)* *(add_len)* nt *(net_id)*	485006	Medium		This alarm indicates that an incoming ARP packet was received with a protocol address length that does not match the one which should be used on that network. The value *(type)* identifies the protocol type, *(add_len)* identifies the length of the protocol address, and *(net_id)* provides the network identifier.		Use a network management tool to detect the source host and contact the manufacturer of the equipment and report the problem.
ARP.007 Mk ent *(hwd_add)* *(type)* nt *(net_id)*	485007	UTrace		This alarm indicates that an incoming ARP packet addressed to this host contained a mapping that was not in the translation cache. A new cache entry was filled in with the information in the packet. The value *(hwd_add)* identifies the hardware address, *(type)* identifies the protocol type, and *(net_id)* provides the network identifier.		This is an information message only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
ARP.008 Bd opc *(op_type) (hwd_add) (type)* nt *(net_id)*	485008	Medium		This alarm indicates that an incoming ARP packet was received with an illegal operation code. The value *(op_type)* identifies the type of operation, *(hwd_add)* identifies the hardware address, *(type)* identifies the protocol type, and *(net_id)* provides the network identifier.		Use a network management tool to detect the source host and contact the manufacturer of the equipment and report the problem.
ARP.009 Rply *(hwd_add) (type)* nt *(net_id)*	485009	UTrace		This alarm indicates that an ARP reply is being sent as the result of a request for a translation from another host. The value *(hwd_add)* identifies the hardware address, *(type)* identifies the protocol type, and *(net_id)* provides the network identifier.		This is an information message only. No corrective actions are required.
ARP.010 Err on rply nt *(net_id)*	485010	High		This alarm indicates that an outgoing reply packet was dropped as the result of some problem in the router. The value *(net_id)* provides the network identifier.		Consult logging output from the relevant network subsystem for more information.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ARP.011 Del ent *(hwd_add) (type)* nt *(net_id)*	485011	UTrace		This alarm indicates that an translation cache entry timed out (was not used or refreshed recently) and has been deleted. The value *(hwd_add)* identifies the hardware address, *(type)* identifies the protocol type, and *(net_id)* provides the network identifier.		Consult the ARP manual for more details on controlling this process.
ARP.012 No iorb fr rqst nt *(net_id)*	485012	High		This alarm indicates that an outgoing reply packet was dropped as the result of a lack of buffers in the router. The value *(net_id)* provides the network identifier.		Consult logging output from the rest of the router for more information. If the problem persists, contact your authorized service representative.
ARP.013 No mem fr addr nt *(net_id)*	485013	High		This alarm indicates that an outgoing reply packet was dropped as the result of a lack of memory in the router. The value *(net_id)* identifies the network sending the request.		Consult the alarm output log (from the printer or display) for the rest of the router for additional information. If this problem persists, contact your authorized customer service representative.
ARP.014 Rqst *(hwd_add) (type)* nt *(net_id)*	485014	UTrace		This message indicates that an ARP translation request is being sent as the result of the transmission of a packet from the router for which the translation of another host's address is needed. The value *(hwd_add)* identifies the hardware address, *(type)* identifies the protocol type, and *(net_id)* provides the network identifier.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ARP.015 Err in rqst nt *(net_id)*	485015	High		This alarm indicates that an outgoing request packet was dropped as the result of some problem in the router. The value *(net_id)* identifies the network sending the request.		Consult the alarm output log, from the printer or display, from the relevant network subsystem for additional information.
ARP.016 unkn dst prot ad nt *(net_id)*	485016	PTrace		This message indicates that an ARP request specifies an unknown protocol address. For example, the request is not for the router that received the request. The value *(net_id)* identifies the network sending the request.		This is an information message only. No corrective actions are required.
ARP.017 No mem fr ent *(hw_addr)* *(type)* nt *(net_id)*	485017	High		This alarm indicates that an incoming ARP packet addressed to this host contained a mapping that was not in the translation cache. An attempt to create a new cache entry failed because there was insufficient memory available. The value *(hw_addr)* identifies the hardware address, *(type)* identifies the protocol type, and *(net_id)* provides the network identifier. **■Note** values for %s and %d are not provided.		Increase the amount of memory installed or reduce the configuration to free up memory.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ARP.018 No mem fr nt *(net_id)*	485018	High		During interface initialization, an attempt to allocate memory for ARP protocol handling on the interface failed. The value *(net_id)* provides the network identifier.		Increase the amount of memory installed or reduce the configuration to free up memory.
ARP.019 No mem fr prt *(proto_no)* nt *(net_id)*	485019	High		During interface initialization, an attempt to allocate memory for ARP protocol handling of a specific protocol failed. The value *(prot_no)* identifies the protocol number, and *(net_id)* provides the network identifier.		Increase the amount of memory installed or reduce the configuration to free up memory.
ARP.020 Bd src hdw fr nt *(src_prot_addr)*	485020	Medium		This alarm indicates that an incoming ARP packet addressed to this host contained a source hardware address that was a broadcast address. Packets of this type are discarded. The value (src_prot_addr) identifies the source protocol address of the packet. **■Note** If the sender's hardware address is a broadcast address, this packet should be discarded.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ARP.021 No mem fr dav *(net_id)*	485021	High		An attempt to allocate memory for the "Duplicate Address Validation" feature failed when an interface on which the feature was enabled became active. The value (net_id) provides the network identifier of the interface.		Increase the amount of memory installed or reduce the configuration to free up memory.
ARP.022 Bd src prt fr nt *(src_prot_addr)*	485022	Medium		This alarm indicates that an incoming ARP packet addressed to this host contained a source protocol address that was the same as one of the interfaces addresses, which is not acting as a proxy. The value *(src_prot_addr)* identifies the source protocol address of the packet.		There are two interfaces connected to the network with the same address. The address of one of the interfaces should be changed.
ETH.001 brd rev unkwn typ *(type)* *(source)* -> *(dest)* nt *(net)*	491001	PTrace		This alarm indicates that a broadcast packet was received with an unknown or unsupported Ethernet type field. The value *(type)* identifies the packet type, *(source)* identifies the source Ethernet address, *(dest)* identifies the destination Ethernet address, and *(net)* identifies the network.		To correct this problem, enter a valid value for the field type.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ETH.002 rev unkwn typ *(type) (source)* -> *(dest)* nt *(net)*	491002	Medium		This alarm indicates that a non-broadcast packet was received with an unknown or unsupported Ethernet type field. The value *(type)* identifies the packet type, *(source)* identifies the source Ethernet address, *(dest)* identifies the destination Ethernet address, and *(net)* identifies the network.		To correct this problem, enter the default value to the **s** parameter or reconfigure the **f** parameter.
ETH.003 brd 802.3 bd in *(actual) (claimed) (source)* -> *(dest)* nt *(net)*	491003	PTrace		This message indicates that a broadcast packet was received with a type field that indicated 802.3 but was shorter than data length claimed in the 802.3 header. The value *(actual)* identifies the actual length of the broadcast packet, *(claimed)* identifies the claimed length of the packet, *(source)* identifies the source Ethernet address, *(dest)* identifies the destination Ethernet address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ETH.004 802.3 bd in *(actual) (claimed) (source) -> (dest)* nt *(net)*	491004	Medium		This message indicates that a non-broadcast packet was received with a type field that indicated 802.3 but was shorter than data length claimed in the 802.3 header. The value *(actual)* identifies the actual length of the non-broadcast packet, *(claimed)* identifies the claimed length of the packet, *(source)* identifies the source Ethernet address, *(dest)* identifies the destination Ethernet address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.005 DN bd Ln *(actual) (claimed) (source) -> (dest)* nt *(net)*	491005	Medium		This message indicates that a DECnet packet was received with a length field that was larger than the actual length of the packet. The value *(actual)* identifies the actual length of the DECnet packet, *(claimed)* identifies the claimed length of the packet, *(source)* identifies the source Ethernet address, *(dest)* identifies the destination Ethernet address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.006 IPX bd ECONFIG 8137 nd *(add)* nt *(net)*	491006	Medium		This message indicates that an IPX packet was received with the wrong ECONFIG. The value *(add)* identifies the address and *(net)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ETH.007 IPX bd ECONFIG 802.2 nd *(add)* nt *(net)*	491007	Medium		This message indicates that an IPX packet was received with the wrong ECONFIG. The value *(add)* identifies the address and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.008 IL *(selft-est)* fld *(error)* nt *(net)*	491008	Medium		The self-test for the Interlan Ethernet card has reported an error during self-test. The value *(selftest)* identifies the specific self test that has been performed, *(error)* identifies the error detected, and *(net)* identifies the network.		This is an information message only. No corrective actions are required. **■ Note** Refer to the *IP Routing Manual* (Part Number T0100-03) and your Vanguard installation manual for additional information.
ETH.009 PE *selftest)* fld *(error)* nt *(net)*	491009	Medium		The self-test for the installed Ethernet card has reported an error during self-test. The value *(selftest)* identifies the specific self test that has been performed, *(error)* identifies the error detected, and *(net)* identifies the network.		This is an information message only. No corrective actions are required. **■ Note** Refer to the *IP Routing Manual* (Part Number T0100-03) and your Vanguard installation manual for additional information.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ETH.010 LLC unk SAP *(DSAP) (source) -> (dest)* nt *(net)*	491010	Low		This alarm indicates that an 802.2 LLC packet was received from the network with an inactive (unrecognized) DSAP. (This alarm generally indicates that a card is defective.) The value *(source)* identifies the source Ethernet address, *(dest)* identifies the destination Ethernet address, and *(net)* identifies the network.		To correct this problem, verify that all Ethernet cards are functioning properly and replace as required. **■ Note** Refer to the *IP Routing Manual* (Part Number T0100-03) and your Vanguard Installation manual for additional information.
ETH.011 LLC nt typ 1 *(LLC_Cont)* nt *(net)*	491011	Low		This message indicates that a packet was received from the network that had an LLC but was not a Type 1 LLC. This alarm generally indicates that a card is defective.) The value *(LLC_Cont)* identifies the LLC control type packet and *(net)* identifies the network.		To correct this problem, verify that all Ethernet cards are functioning properly and replace as required. **■ Note** Refer to the *IP Routing Manual* (Part Number T0100-03) and your Vanguard Installation manual for additional information.
ETH.012 LLC RSP *(LLC_SSAP)* nt *(net)*	491012	Low		This message indicates that an LLC Response was received from the network. The value *(LLC_SSAP)* identifies the LLC response packet and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.013 LLC XID *(LLC_SSAP)* nt *(net)*	491013	Low		This message indicates that an LLC XID packet was received from the network. The value *(LLC_SSAP)* identifies the LLC XID packet and *(net)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ETH.014 LLC TEST *(LLC_SSAP)* nt *(net)*	491014	Low		This message indicates that an LLC TEST packet was received from the network. The value *(LLC_SSAP)* identifies the LLC Test packet and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.015 unrec ctl *(LLC_Cont)* nt *(net)*	491015	Low		This message indicates that a packet was received from the network that had an illegal control field or UI. The value *(LLC_Cont)* identifies the LLC packet and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.016 VL *(selftest)* fld *(error)* nt *(net)*	491016	High		This message indicates that the self-test for the VLAN-E card has reported an error during self-test. The value *(selftest)* identifies the specific self test that has been performed, *(error)* identifies the error detected, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.017 LOOP rev *(source)->(dest)*, nt *(net)*	491017	PTrace		This message indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet was received. The value *(source)* identifies the source Ethernet address, *(dest)* identifies the destination Ethernet address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ETH.018 LOOP odd skp count, *(source)->(dest)*, nt *(net)*	491018	Medium		This alarm indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet had an odd skipcount in the packet. When this occurs the packet is discarded. The value *(source)* identifies the source Ethernet address, *(dest)* identifies the destination Ethernet address, and *(net)* identifies the network.		Generally, this indicates a hardware error with the card. **■ Note** Refer to the *IP Routing Manual* (Part Number T0100-03) and your Vanguard Installation manual for additional information.
ETH.019 LOOP func *(function)* forw, *(source)->(dest)*, nt *(net)*	491019	Medium		This message indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet did not have a *(function)* code of forward (2). When this occurs the packet is discarded. The value *(source)* identifies the source Ethernet address, *(dest)* identifies the destination Ethernet address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.020 LOOP mc fwd dst *(forw)*, *(source)->(dest)*, nt *(net)*	491020	Medium		This message indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet has a forward address that is multicast. When this occurs the packet is discarded. The value *(forw)* identifies the Ethernet address to which the packet will be forwarded, *(source)* identifies the source Ethernet address, *(dest)* identifies the destination Ethernet address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ETH.021 LOOP fwd *(source)* -> *(forw)*, nt *(net)*	491021	PTrace		This message indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet is being forwarded to the specified next hop. The value *(source)* identifies the source Ethernet address, *(forw)* identifies the Ethernet address towhich the packet will be forwarded, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.022 LOOP fwd to *(forw)* dsc, rsn *(code)*, nt *(net)*	491022	Low		This message indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet could not be forwarded to the specified address, for the reason specified by the code. The value *(forw)* identifies the Ethernet address towhich the packet could not be forwarded, *(code)* identifies the error code for this problem, and *(net)* identifies the network		Programming error in remote code.
ETH.023 LLC RSP to (dest) dsc, rsn *(code)*, nt *(net)*	491023	Low		This message indicates that an LLC response (XID or TEST) could not be transmitted to the specified address, for the reason specified by the code. The value *(source)* identifies the source Ethernet address, *(dest)* identifies the destination Ethernet address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ETH.024 MOP bd in *(actual), (claimed)*, *(source)* -> *(dest)* nt *(net)*	491024	Medium		This message indicates that a DECnet MOP packet was received with a length field that was larger than the actual length of the packet. The value *(actual)* identifies the actual length of the non-broadcast packet, *(claimed)* identifies the claimed length of the packet, *(source)* identifies the source Ethernet address, *(dest)* identifies the destination Ethernet address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.025 LOOP bd skp *(count)*, *(source)* -> *(dest)*, nt *(net)*	491025	Medium		This message indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet had a skipcount in the packet that points to beyond the end of the packet. When this occurs the packet is discarded. The value *(count)* identifies the skipCount value, *(source)* identifies the source Ethernet address, *(dest)* identifies the destination Ethernet address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.031 NP no buf fr slf-tst, nt *(net)*	491031	Low		This message indicates that a packet buffer is unavailable to do a self-test on NP600 interface. The self-test will time out and fail. The value *(net)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ETH.032 NP slf-tst cmd, nt *(net)*	491032	CTrace		This message indicates that an NP600 self-test routine is starting an internal self-test in the interface. This is done on some self-tests. The value *(net)* identifies the network.		Programming error on remote node.
ETH.033 NP diag cmd, nt *(net)*	491033	CTrace		This message indicates that an NP600 self-test routine is starting an internal diagnostics program in the interface. This is normal for the first self-test. The value *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.034 slf-tst cmd timeout, nt *(net)*	491034	High		This message indicates that an NP600 self-test running inside the interface did not complete in the required five seconds. This probably indicates a serious problem with the interface or with its network connection. The network will be declared down. The value *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.35 NP diag cmd timeout, nt *(net)*	491035	High		This message indicates that an NP600 diagnostics running inside the interface did not complete in the required 20 seconds. This probably indicates a serious problem with the interface or with its network connection. The network will be declared down. The value *(net)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ETH.36 NP fld *(mod)* diag, stat *(code)*, nt *(net)* disabled	491036	High		This message indicates that an NP600 internal diagnostic detected a hardware failure. The interface is disabled and further self-tests are cancelled. The value *(mod)* identifies the Module whose major functional diagnostics block has failed. This will be either: • EPROM checksum test • Quick DRAM test • System memory port test • Power-up state test • Ethernet address ROM test • RDR bit test • Quick DRAM test 12 The value *(code)* identifies the exact error number reported by the diagnostics and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.037 NP diags OK, ETH bad, stat *(code)*, nt *(net)*	491037	Medium		This message indicates that an NP600 diagnostic passed, but als indicates that the Ethernet network connection is faulty. The value *(code)* identifies the exact error number reported by the diagnostics and *(net)* identifies the network. **■Note** The overall self-test will continue, and probably will fail later.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ETH.038 NP load timeout, nt *(net)*	491038	High		This message indicates that the download of operational firmware by the EPROM monitor in the NP600 interface timed out. This may indicate a hardware problem, or it may be an error in DMA channel configuration. The network will be declared down. The value *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.039 NP *(command)* rst, nt *(net)*	491039	UTrace		This message indicates that the specified NP600 interface command has been cancelled by a device reset. The value *(command)* identifies one of: • load; for a firmware load • slf-tst; for an internal self-test • maint; for a maintenance command. These messages are a normal follow-on to a timeout. The value *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.040 NP slf-tst fld *(code)*, nt *(net)*	491040	High		This message indicates that the NP600 self-test command failed “status code, network.”. The value *(code)* identifies the exact error number reported by the diagnostics and *(net)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
ETH.041 NP loaded, slf-tst, nt *(net)*	491041	CTrace		This message indicates that the NP600 firmware load succeeded, so an internal self-test is being started in the interface. The value *(net)* identifies the network.		This is an information message only. No corrective actions are required.
ETH.042 Unable to get buf for ethernet packet.	491042	High		This message indicates that a buffer to set an Ethernet address, or to copy an Ethernet packet could no be obtained because of a buffer shortage.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.001 Copyright 1984 Massachusetts Institute of Technology	486001	Always		This message indicates that portions of the original code, on which this system was based, bear the following copyright notice: "*Permission to use, copy, modify and distribute this program for any purpose and without fee is hereby granted, provided that this copyright and permission appear on all copies and supporting documentation, the name M.I.T. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of M.I.T. M.I.T. makes no representation about the suitability of this software for any purpose. It is provided 'as is' without express or implied warranty.*"		This is an information message only. No corrective actions are required.
GW.002 Portable CGW *(name)* Rel *(level)* strtd	486002	Always		This message identifies the name of the router, and the release level of the software running on it. The value *(name)* identifies the router name and *(level)* identifies the software release level being used.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.003 Unus pkt len *(len)* nt *(net_id)*	486003	Always		This alarm indicates that the Vanguard router can not send or receive a specified number of bytes with the maximum packet size. The value *(len)* identifies how many bytes will not be sent or received and *(net_id)* identifies the network.		The configuration for the router has dictated a maximum packet size that the software will handle, which is smaller than the Maximum Transmission Unit (MTU) of the network. If the buffer size setting on the router has been manually set, modify or remove the buffer size setting in the router. **■ Note** If this message appears repeatedly, contact your customer service representative.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.004 Sys *(type)* q adv alloc *(adv_len)* excd *(act_len)*	486004	Always		This alarm indicates that the system has detected an insufficient number of buffers for the optimal operation. On startup, the maximum number of buffers allocated to either the permanent device input queue or the transmit device output queue had exceeded an advisable allocation of the entire buffer. The value *(type)* identifies the input queue, *(adv_len)* identifies the advisable length of the buffer pool, and *(act_len)* identifies the actual length of the buffer pool.		Perform these tasks to correct this problem: a) Ensure that the protocol routing tables are properly sized for the network configuration. The router may have been configured with overly large routing tables for some protocol and memory allocated to routing tables cannot be used for packet buffers. b) Reduce the number of network interfaces on the router. The router may have too many network interfaces for available buffer memory. If a reasonable number of interfaces are configured, or if a memory upgrade is available, consider expanding the amount of memory. c) The number of buffers has been manually set to a low number. Modify or remove the number of buffers setting in the router. Contact your customer service representative if this alarm occurs repeatedly.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.005 Bffrs: *(total)* avail *(free)* idle fair *(fair)* low *(high)*	486005	Always		The message gives information about the number of buffers created by the initialization procedure, as well as some information on parameters used by the buffer allocation system. The value *(total)* identifies the total number of buffers, *(free)* identifies the number of free buffer, *(fair)* identifies the number of buffers that can freely allocate, and *(high)* identifies the highest number of buffers.		This is an information message only. No corrective actions are required.
GW.006 Pkt frm nt *(net_id)* for uninit prt, disc	486006	Low		This message indicates that an incoming packet was in a protocol which, although recognized, did not have a handler loaded and enabled. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW.007 Ip err *(code)* nt *(net_id)*	486007	Low		This message indicates that a device input operation returned an error, along with a device-specific error code. The input error counter for that network was incremented, and any packet associated with that error was probably discarded. The value *(code)* identifies the error code and *(net_id)* identifies the network.		**Note** Refer to the IP Routing Manual (Part Number T0100-03) and your Vanguard Installation manual, for additional information on error codes.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.008 Ip ovfl nt *(net_id)*, disc	486008	Low		This alarm indicates that packets were arriving on the stated interface too quickly for the router to process them. Before the software can examine these packets they are discarded because of the overload condition. The input overflow counter for that network increments each time this occurs. This is sometimes caused by "broadcast storms." These are untoward events caused by combinations of buggy and/or out-of-date software running on network hosts which spread in a chain reaction. These typically cause a network to be consumed with back to back packets (often broadcast) for a period of seconds, or occasionally, a minute or two. The value *(net_id)* identifies the network.		To correct this problem either: a) Fix or disable the host responsible for the broadcast storm. Or: b) Consider upgrading your Vanguard to a new model with a faster CPU.
GW.009 Nt dwn ip rstrt nt *(net_id)*	486009	High		This alarm indicates that a Vanguard has attempted to queue additional input operations for the network, the network had been disabled for input. The value *(net_id)* identifies the network.		This is caused by the timing windows in the internal operation of the router; an input restart operation was requested, but when the time came to do it, input on the interface had been internally disabled. The condition is detected, and is harmless.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.010 Ip q len *(len)* no ip buf nt *(net_id)*	486010	High		This alarm indicates that the Vanguard router attempted to queue additional input operations for the network. There were insufficient free buffers available to refill the input queue to the level desired; the actual level attained is listed. The value *(len)* identifies the length of the input queue and *(net_id)* identifies the network.		If the message occurs on an occasional basis, a traffic peak is causing the router to run short of buffers. No action required. Or: The router is short of buffers for some reason. This may be because there is not enough memory on the router to provide enough buffers. If there is a shortage of memory for buffers, add memory to the router or reduce the number of network interfaces on the router. If the message persists, contact Customer Support. Or: The number of buffers may be manually set to low. Modify or remove the number of buffers setting in the router. If the message persists, contact Customer Support.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.014 Nt dwn op rstrt nt *(net_id)*	486014	High		This alarm indicates that the Vanguard router has attempted to queue additional output operations for the network. As a result, the network had been disabled for output. The value *(net_id)* identifies the network.		This is caused by timing windows in the internal operation of the router. An output restart operation was requested, but when the time came to do it, output on the interface had been internally disabled. The condition is detected and is harmless. **Note** Contact your customer service representative if this alarm appears repeatedly.
GW.017 Intfc hdw mssng nt *(net_id)*	486017	Medium		This alarm indicates that Vanguard Applications Ware has tried to initialize the network interface for the first time, the board did not respond on the bus. The board is marked Ònot presentÓ and ignored from then on. The value *(net_id)* identifies the network.		To correct this problem: a) Verify that the board is properly plugged in. If necessary refer to your Vanguard Installation Manual for the proper removal, replacement, and seating instructions. b) Verify that the device is properly configured. Refer to your Vanguard Applications Ware documentation for additional information on the configuration of hardware and software. c) Replace the board if the preceding steps do not rectify the problem.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.018 Strt nt slf tst nt *(net_id)*	486018	UTrace		This message indicates that a network self-test has been requested. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW.019 Slf tst nt *(net_id)*	486019	Low		This message indicates that a network self-test has been requested. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW.020 Nt pss slf tst nt *(net_id)*	486020	UTrace		This message indicates that a network undergoing self-test has passed the self-test. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW.022 Nt fld slf tst nt *(net_id)*	486022	UTrace		This message indicates that a network undergoing self-test has failed the self-test. The value *(net_id)* identifies the network.		The cause of this problem is dependent on the network architecture and topology. Use any trap messages printed by the network handler, along with network specific information as revealed by the CGWCON "Interface" command, to isolate the problem.
GW.023 Nt dwn nt *(net_id)*	486023	Medium		This message indicates that after failing the self test, a network that was previously up has gone down. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.025 Nt fld mnt nt *(net_id)*	486025	Medium		This message indicates that the number of maintenance checks failed in a given interval has exceeded the allowed limit. A self-test will be started on the interface; if it fails, the interface will be marked down. The value *(net_id)* identifies the network.		The cause of this problem is dependent on the network architecture and topology. Use any trap messages printed by the network handler, along with network specific information as revealed by the CGWCON "Interface" command, to isolate the problem.
GW.026 Mnt nt *(net_id)*	486026	CTrace		This message indicates that a maintenance check has been started for the indicated interface. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW.027 No pkt fr mnt nt *(net_id)*	486027	High		This alarm indicates that a buffer could not be allocated when needed by network maintenance. The value *(net_id)* identifies the network.		This may be caused by temporary traffic loads. Many other causes are possible. If the message persists, contact Customer Support.
GW.028 Snk dsc pkt prt *(type)* to *(host)*	486028	Low		This message indicates that a buffer was sent to the sink network, which discarded it. There was no indication of an error sent to the forwarder. The value *(type)* identifies the protocol and *(host)* identifies the next hop host.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.029 Int dis nt *(net_id)*	486029	Low		This message indicates that the interface in question was disabled in the configuration and will not come up. This interface can be started at any time by testing it. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW.030 *(heap)* bytes reserved by *(subsys)*	486030	Low		This message indicates that a router subsystems, at startup, has reserved too many bytes of heap memory. This will be subtracted from the router's free memory before the remainder is carved into packet buffers. The value *(heap)* identifies the number of bytes reserved in heap memory and *(subsys)* identifies the subsystem that has reserved the memory.		This is an information message only. No corrective actions are required.
GW.031 IP q alloc fl nt *(net_id)* avl *(buffers)*	486031	Always		The system has detected that there is probably an insufficient number of buffers for optimal operation. On startup, each of the fast devices is allocated a fixed number of buffers. If these buffers are not available, the particular interface may not perform well. The value *(net_id)* identifies the network and *(buffers)* identifies the number of available buffers.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.032 Op err *(code)* hst *(host)* nt *(net_id)*	486032	Low		This alarm indicates that a Vanguard device has returned an error code and a device specific error code, both identified in this alarm by the variable *(code)*. The output error counter for that network was incremented. The packet associated with that error will be retransmitted up to a network-dependent retransmission count. Usually, the value *(host)*, which indicates the Next Hop Host will be the MAC layer address of the next hop router or host that this packet is being sent to. The format of this MAC address depends on the network type. If Next Hop Host starts with an @, that network does not provide a formatted display of MAC addresses, and the following number is the hex address in router memory that the next hop host address is stored at. The value *(net_id)* identifies the network.		Refer to the *IP Routing Manual* (Part Number T0100-03) and your Vanguard Installation Manual for additional information on the appropriate interface to to identify specific error codes.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.033 Op err cnt excd hst (*host)* nt *(net_id)*	486033	Low		This alarm indicates that after the maximum allowed number of retransmissions for output error, a packet had still not been transmitted successfully. The output discard counter for that network was incremented, and the packet was discarded. Usually, the value *(host)*, which indicates the Next Hop Host will be the MAC layer address of the next hop router or host that this packet is being sent to. The format of this MAC address depends on the network type. If Next Hop Host starts with an @ (at-sign), then that network does not provide formatted display of MAC addresses, and the following number is the hex address in router memory that the next hop host address is stored at. The value *(net_id)* identifies the network.		This message may indicate hardware transmission problems if it occurs frequently. Use appropriate level 2 network management tools, such as Tokenview (for rings) or a Time Domain Reflectometer (for Ethernet) to isolate and fix the problem.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.034 Rtrns cnt excd hst (*host)* nt *(net_id)*	486034	Low		This alarm indicates that networks containing low level acknowledgments, transmission failures due to no acknowledgment do not count as output errors, but are retransmitted; the packet will be retransmitted up to a network-dependent retransmission count. If the packet in question is not accepted after that number of retransmissions, the packet is dropped. Usually, the value *(host)*, which indicates the Next Hop Host will be the MAC layer address of the next hop router or host that this packet is being sent to. The format of this MAC address depends on the network type. If next_hop_host starts with an @ (at-sign), then that network does not provide formatted display of MAC addresses, and the following number is the hex address in router memory that the next hop host address is stored at. The value *(net_id)* identifies the network.		When this message appears, it generally means that the next hop host is down or detached from the network. If the next hop host is a router, and the routers are using dynamic routing, then this message should only appear temporarily until the dead router is detected and traffic is routed around it.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.035 Nt dwn to hst (*host)* nt *(net_id)*	486035	High		This alarm indicates that when a router tried to send a packet to a given host, the network interface it had been told to send the packet over was not up. The output discard counter for that network was incremented, and the packet was returned to the protocol forwarder for attention. Usually, the value *(host)*, which indicates the Next Hop Host will be the MAC layer address of the next hop router or host that this packet is being sent to. The format of this MAC address depends on the network type. If next_hop_host starts with an @ (at-sign), then that network does not provide formatted display of MAC addresses, and the following number is the hex address in router memory that the next hop host address is stored at. The value *(net_id)* identifies the network.		This is caused by timing windows in the internal operation of the router; a packet was queued for output, but when the time came to send it, the interface was down. The condition is detected, and is harmless. Contact your customer service representative if this alarm appears repeatedly.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.036 Op ovfl to hst (*host)* nt *(net_id)*	486036	Low		This alarm indicates that when a router tried to send a packet to a given host, the network output queue was too full, and the packet was discarded. The output overflow counter for that network was incremented, and the packet was returned to the protocol forwarder for attention. Usually the value *(host)*, which indicates the Next Hop Host, will be the MAC layer address of the next hop router or host that this packet is being sent to. The format of this MAC address depends on the network type. If next_hop_host starts with an @ (at-sign), then that network does not provide formatted display of MAC addresses, and the following number is the hex address in router memory that the next hop host address is stored at. The value *(net_id)* identifies the network.		This is caused by the offered load in the network being higher than the bandwidth available in the output network. Since the router itself is keeping up with the traffic, there is little it can do; the hosts generating the traffic are simply sending more data than the output can accommodate. Increase the speed of the network in question or take measures to restrict the offered load.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.037 Nt dwn, disc pkt to hst *(host)* nt *(net_id)*	486037	Low		This alarm indicates that packets waiting for transmission on the network in question were discarded when the network went down. The discard counter for the network in question is incremented. Usually the value *(host)*, which indicates the Next Hop Host, will be the MAC layer address of the next hop router or host that this packet is being sent to. The format of this MAC address depends on the network type. If next_hop_host starts with an @ (at-sign), then that network does not provide formatted display of MAC addresses, and the following number is the hex address in router memory that the next hop host address is stored at. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW.038 User default name has logged on	486038	Low		This message indicates that a new user has logged on to the system.		This is an information message only. No corrective actions are required.
GW.039 Failed logon:ID = default name	486039	Medium		This message indicates that someone attempted to log on to the system but did not supply a correct user-name and password.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW.040 to cl dnd nt *(net_id)*	486040	Low		This message indicates that a router would like to place outbound call, but it's configuration prevents it. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW.041 in cl dnd nt *(net_id)*	486041	Low		This message indicates that a router rejected an incoming call because it's configuration does not allow inbound calls. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW.042 in cl unk addr (dial),/(subdial), rj nt *(net_id)*	486042	Low		This message indicates that an inbound call was not accepted because the caller's address did not match the configured remote. The value *(dial)* identifies the dial address, *(subdial)* identifies the subdial address, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW.043 CML state *(state)*, event *(event),* nt *(net_id)*	486043	CTrace		This message indicates that a FSM trace event has taken place. The value *(state)* identifies the state, *(event)* identifies the event which took place, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW.044 No cnfg nt *(net_id)*	486044	High		This message indicates that no SR_VRTBLK record was found in the SR_VNET block. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
GW.045 bd dl net dial_interface_id, nt *(net_id)*	486045	High		This message indicates that the dialer net configured is either not present, or not a dial net. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW.046 bd dl dst dest_dial_name, nt *(net_id)*	486046	High		This message indicates that the specified destination name was not added with the "add address" command. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW.047 idle timer exp nt *(net_id)*	486047	Low		This message indicates that the idle timer of a demand-based net expired, and the call was cleared. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
GW: Bd cnf inf nt hdr lnghts		High		This message indicates that bad configuration information in the load was detected.		Hand-configured maximum header and trailer sizes are smaller than the actual lengths of at least one network in the router. Contact your customer service representative if this alarm appears.
GW: incompatible net table vers		High		This message indicates that a load with incompatible versions of binary modules has been detected.		The version number on the network configuration table does not match that which the code was compiled with. Contact your customer service representative if this alarm appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW: incompatible P_MAX		High		This alarm indicates that a load with incompatible versions of binary modules has been detected.		The maximum number of protocols in the configuration information does not match that which the code was compiled for. Contact your customer service representative if this alarm appears.
GW: incompatible T_MAX		High		This alarm indicates that a load with incompatible versions of binary modules has been detected.		The maximum number of network types in the configuration information does not match that which the code was compiled with. Contact your customer service representative if this alarm appears.
GW: incompatible L_MAX		High		This alarm indicates that a load with incompatible versions of binary modules has been detected.		The maximum number of interface types in the configuration information does not match that which the code was compiled with. Contact your customer service representative if this alarm appears.
GW: no mem for the prot tbl		High		This alarm indicates that there is insufficient memory available for a critical system table.		Insufficient memory is available for allocation to either the installed or complete protocol table, or the per network protocol upcalls, early in initialization. Contact your customer service representative if this alarm appears.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
GW: freeing free buffer		High		This alarm indicates that a buffer-free routine detected software in the system attempting to free a buffer that has already been freed.		Software bug that frees the same buffer twice. This is a serious error. Take dump of this failure and send it to your customer service representative. If the dump is unavailable, disable the watchdog and auto-restart. Contact your customer service representative if this alarm appears. and ask that a stack backtrace be performed on the console.
GW: alloc busy buffer		High		This alarm indicates that the buffer-free routine detected software in the system attempting to locate a buffer that is already free.		The cause is a software bug. Take dump of this failure and send it to your customer service representative. If the dump is unavailable, disable watchdog and auto-restart. Contact your customer service representative and ask that a stack backtrace be performed on the console.
ICMP.001 bd cks 0xreceived_ check-sum *(checksum) (source) -> (dest)*	480001	Medium		This alarm indicates that a bad ICMP checksum was detected in an incoming ICMP message. The received checksum is displayed, together with the value that the checksum should have had. The received packet is discarded. The value *(checksum)* identifies the received checksum, *(source)* identifies the source IP address, and *(dest)* identifies the destination IP address.		Contact the manufacturer of the source host and report the problem.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ICMP.002 ech *(source) -> (dest)*	480002	Low		An ICMP Echo Request was received from the source host by the router. Note that an ICMP Echo Request is only recognized when it comes in over the interface with the address the packet is addressed to. The value *(source)* identifies the source IP address, and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
ICMP.003 ech rp *(source) -> (dest)*	480003	Low		An ICMP Echo Reply was received from the source host by the router. This is a slightly suspicious event, since the router does not normally send ICMP Echo Requests. The value *(source)* identifies the source IP address, and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
ICMP.004 unhnd typ *(type) (code) (source) -> (dest)*	480004	High		An ICMP message came in with a type that the router software does not handle. he value *(type)* identifies the ICMP type, *(code)* identifies the message code, *(source)* identifies the source IP address, and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ICMP.005 unhnd brd typ *(type) (code) (source) -> (dest)*	480005	UTrace		A broadcast ICMP message came in with a type that the router software does not handle. The value *(type)* identifies the ICMP type, *(code)* identifies the message code, *(source)* identifies the source IP address, and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
ICMP.006 bd typ *(type) (code) (source) -> (dest)*	480006	Medium		An ICMP message came in with a type that is not legal. The value *(type)* identifies the ICMP type, *(code)* identifies the message code, *(source)* identifies the source IP address, and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
ICMP.007 addr msk *(source) -> (dest)*	480007	Low		An ICMP Address Mask Request was received from the source host by the router. The value *(source)* identifies the source IP address, and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
ICMP.008 addr msk rep *(source) -> (dest)*	480008	CTrace		An ICMP Address Mask Reply was received from the source host by the router. The value *(source)* identifies the source IP address, and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
ICMP.009 no pkt or mem	480009	High		Internal resources in the router necessary to reply to the incoming message were unavailable.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ICMP.010 amb addr msk *(source)* -> *(dest)*	480010	Medium		This message indicates that an incoming address mask request on an interface which contained more than one IP source address contained a destination address which could not be localized to one of the addresses, so no reply could be generated. The value *(source)* identifies the source IP address, and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
ICMP.011 err code sndng pkt to nt *(net_id)*	480011	High		This alarm indicates that an outgoing reply packet was dropped as the result of some problem in the router. The value *(net_id)* identifies the network.		Consult logging output from the relevant network subsystem for more information.
ICMP.012 rdr *(source)* -> *(dest)* to *(new_add)*	480012	Low		This message indicates that the router is sending an ICMP Redirect, advising a source host on a directly connected network that there is a better first hop router for this traffic. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address, *(new_add)* identifies the better first hop.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ICMP.013 bd prm off *(offset) (source) -> (dest)*	480013	Low		This message indicates that the router is sending an ICMP Parameter Problem message, for an unspecified problem at the given offset. st hop router for this traffic. The value *(offset)* identifies the specified offset, *(source)* identifies the source IP address, *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
ICMP.014 snd *(type) (code) (source) -> (dest)*	480014	UTrace		This message indicates that the router is sending an ICMP packet of the specified type about a packet from the source host to the destination. The value *(type)* identifies the ICMP type, *(code)* identifies the message code, *(source)* identifies the source IP address, and *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
ICMP.015 shrt ICMP hdr *(len)* src *(source)*	480015	Medium		This message indicates that an ICMP packet's indicated header length is below the minimum possible length for an ICMP packet. The value *(len)* identifies the header length and *(source)* identifies the source IP address.		If the problem persists, examine a line trace to determine where the packet is being damaged.
ping_trans_ completed	433000		Major	This message indicates that the Ping Transaction is completed. "PING: Entry Number %d,Transaction Completed"		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ping_entry_deleted	433001		Major	This message indicates that the Ping Entry is deleted. "PING: Entry Number %d, Deleted"		This is an information message only. No corrective actions are required.
RIP.001 bd ver *(ver)* frm hst *(source)*	483001	Medium		This message indicates that the version field in the RIP header did not match the current version. The value *(ver)* identifies the RIP version number and *(source)* identifies the source IP address.		Contact the manufacturer of the source host and report the problem.
RIP.002 rq frm *(source)*	483002	UTrace		This message indicates that a RIP routing table request was received from another host. A routing table update will be sent to it. The value *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.
RIP.003 trc on tracing_file frm *(source)*	483003	Low		This message indicates that a request from a host to turn RIP tracing on to a given log file was received. The router ignores this request. The value *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.
RIP.004 trc off frm *(source)*	483004	Low		This message indicates that a request from a host to turn RIP tracing off was received. The router ignores this request. The value *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
RIP.005 rsp frm *(source)*	483005	Ctrace		This message indicates that a RIP routing table update was received. Note that it may take more than one response packet to transmit the entire routing table, especially if the routing table is large. The value *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.
RIP.006 bd cmd *(code)* frm *(source)*	483006	Medium		This message indicates that a RIP message was received with an unrecognized command code. The value *(code)* identifies the command code and *(source)* identifies the source IP address.		Contact the manufacturer of the source host and report the problem.
RIP.007 rsp frm off nt *(source)*	483007	Medium		This alarm indicates that a RIP routing update response was received from a machine which was not directly attached to the network the response came in on. The packet is discarded. The value *(source)* identifies the source IP address.		Examine audit trails and other information to determine the original source host.
RIP.008 sbnt rt *(dest)*_network non-subnt intfc hst *(hop_add)*	483008	Medium		This message indicates that an apparent subnet route (i.e., the 'rest' field of the Internet address contained non-zero data) was received over an interface that is not marked as subnetted in the router. The value *(dest)* identifies the destination IP network and *(hop_add)* identifies the next hop IP address.		Correct the incorrect configuration.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
RIP.009 dyn rt to *(dest)* frm *(hop_add)* dis	483009	UTrace		This message indicates that a dynamic route was received but is being ignored because the configuration of RIP on the router does not allow dynamic routes except for those in a table, and this route was not in that table. The value *(dest)* identifies the destination IP network and *(hop_add)* identifies the next hop IP address.		This is an information message only. No corrective actions are required.
RIP.010 nt *(dest)* unrch via *(hop_add)*, del	483010	Low		This message indicates that an incoming RIP update from the router that was previously listed as the next hop to the destination network has announced that the destination is unreachable (i.e., at metric infinity). The RIP route to that destination is being deleted. The value *(dest)* identifies the destination IP network and *(hop_add)* identifies the next hop IP address.		This is an information message only. No corrective actions are required.
RIP.011 updt nt *(dest)* hps metric via *(hop_add)*	483011	Low		This message indicates that a new (better) route to the given destination has been learned via RIP and has been installed. The value *(dest)* identifies the destination IP network and *(hop_add)* identifies the next hop IP address.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
RIP.012 snd rqst *(source)*	483012	CTrace		The router is sending a RIP request from each of the addresses associated with an interface which has just come up. The value *(source)* identifies the source IP address.		This is an information message only. No corrective actions are required.
RIP.013 snd brd to *(dest) (count) (routes)*	483013	CTrace		This message indicates that the router is sending a normal RIP broadcast update (triggered either by a timer or a change in the routing table) to the specified address. The value *(dest)* identifies the destination IP address, *(count)* identifies the packet count, and *(routes)* identifies the number of routes.		This is an information message only. No corrective actions are required.
RIP.014 snd to *(dest) (count) (routes)*	483014	Low		This message indicates that the router is sending a RIP update (triggered by a request from another host) to the specified address. The value *(dest)* identifies the destination IP address, *(count)* identifies the packet count, and *(routes)* identifies the number of routes.		This is an information message only. No corrective actions are required.
RIP.015 cnt all pkt	483015	High		This message indicates that when RIP went to allocate a packet for transmission (either for a request or reply), none was available.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
RIP.016 snd pkt *(dest)*	483016	CTrace		This message indicates that a RIP packet (either a routing table update, or when an interface first comes up, a request) was sent. The value *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
RIP.017 err *(code)* sndng pkt nt *(net)*	483017	High		This message indicates that an outgoing reply packet was dropped as the result of some problem in the router. The value *(code)* identifies the output error code and *(net)* identifies the network.		Consult logging output from the relevant network subsystem for more information.
RIP.018 nt rt to *(dest)* tmd out	483018	Low		This message indicates a route to a destination, via another router in the routing database, has not been heard from for a while and is now being marked as unreachable. The value *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
RIP.019 nt rt to *(dest)* del	483019	Low		This message indicates a route to a destination via some other router in the routing database has not been heard from for a while, has been marked unreachable, and is now being deleted. The value *(dest)* identifies the destination IP address.		This is an information message only. No corrective actions are required.
RIP.020 cannot allocate memory for transmission	483020	High		This message indicates insufficient physical memory.		Increase the physical memory, or reduce the number of interfaces running RIP.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
rip udp port not avail				This message indicates that another application has previously registered with RIP's UDP port.		Contact your customer service representative if this alarm appears.
LUA SOCKET CONNECT FAILED	451000			This alarm indicates that memory allocation failed.		Reduce SNABSC device entries and/or other node configurations.
INITIALIZATION FAILED - MOD-ULE SNABSC NOT INCLUDED	452000			Appropriate SNABSC modules did not get included in an image.		Load the image that includes the appropriate SNABSC modules
SNABSC_CM CM SYSERR	452001			Internal error during device boot, enable or disable.		Reconfigure and reboot the device. This alarm should be reported to a customer service representative.
INSUFFICIENT MEMORY TO SUPPORT SNABSC_CM CONFIGURATION	452002			This alarm indicates that memory allocation failed.		Reduce SNABSC device entries and/or other node configurations.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TKR.001 unexp *(type)* frm *(control)* fm *(source _MAC)* ssap *(source_SAP)* dsap *(dest_SAP)* nt *(net_id)*	478001	Low		This message indicates an unexpected 802.2 LLC frame type has been received. The type may be I, which is an information transfer, or S which is supervisory. **■Note** The frame was addressed to the router. The value *(type)* identifies the frame type, *(control)* identifies the LLC control, *(source_MAC)* identifies the source MAC address, *(source_SAP)* identifies the source SAP address, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
TKR.002 unexp *(type)* brd frm LLC-control frm *(source _MAC)* ssap *(source_SAP)* , dssp *(dest_SAP)* , net *(net_id)*	478002	PTrace		This message indicates an unexpected 802.2 LLC frame type has been received. The type may be I, which is an information transfer, or S which is supervisory. **■Note** The frame was a broadcast. The value *(type)* identifies the broadcast type, *(source_MAC)* identifies the source MAC address, *(source_SAP)* identifies the source SAP address, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TKR.003 unkn SNAP mfr code *(num)* fm *(source _MAC)* nt *(net_id)*	478003	Low		This message indicates that a frame with an unknown organization code (not 000000) in the SNAP header has been received. **■Note** The frame was addressed to the router. The value *(num)* identifies the SNAP manufacturers code number, *(source_MAC)* identifies the source MAC address, and *(net_id)* identifies the network.		The host is sending packets for an unknown proprietary protocol, using SNAP. **■Note** This is an information message only. No corrective actions are required.
TKR.004 unkn SNAP mfr code *(num)* fm *(source _MAC)* nt *(net_id)*	478004	PTrace		This message indicates that a frame with an unknown organization code (not 000000) in the SNAP has been received. **■Note** The frame was a broadcast. The value *(num)* identifies the SNAP manufacturers code number, *(source_MAC)* identifies the source MAC address, and *(net_id)* identifies the network.		The host is sending packets for an unknown proprietary protocol, using SNAP. **■Note** This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TKR.005 unkn SNAP type *(type)* fm *(source _MAC)* nt *(net_id)*	478005	Low		This message indicates that a frame with an unknown SNAP type (within organization code 000000) has been received. **■Note** The frame was addressed to the router. The value *(type)* identifies the SNAP type code, *(source_MAC)* identifies the source MAC address, and *(net_id)* identifies the network.		The host is sending packets for an unknown Ethernet type, using SNAP. **■Note** This is an information message only. No corrective actions are required.
TKR.006 unkn SNAP type *(type)* fm *(source _MAC)* nt *(net_id)*	478006	PTrace		This message indicates that a frame with an unknown SNAP type (within organization code 000000) has been received. **■Note** The frame was a broadcast. The value *(type)* identifies the SNAP type code, *(source_MAC)* identifies the source MAC address, and *(net_id)* identifies the network.		The host is sending packets for an unknown Ethernet type, using SNAP. **■Note** This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TKR.007 unkn SAP *(num)* fm *(source _MAC)* nt *(net_id)*	478007	Low		This message indicates that a frame with an unknown destination SAP has been received. **■Note** The message was addressed to the router. The value *(num)* identifies the SAP number, *(source_MAC)* identifies the source MAC address, and *(net_id)* identifies the network.		The host is sending packets for an unknown protocol identifier (SAP). **■Note** This is an information message only. No corrective actions are required.
TKR.008 unkn SAP *(num)* fm *(source _MAC)* nt *(net_id)*	478008	Low		This message indicates that a frame with an unknown destination SAP has been received. **■Note** The message was a broadcast. The value *(num)* identifies the SAP number, *(source_MAC)* identifies the source MAC address, and *(net_id)* identifies the network.		The host is sending packets for an unknown protocol identifier (SAP). **■Note** This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TKR.009 unexp U frm *(control)* fm *(source_MAC)* ssap *(source_SAP)* dsap *(dest_SAP)* nt *(net_id)*	478009	Low		This message indicates that an unexpected 802.2 LLC U (unnumbered) frame type has been received and only UI, XID, and TEST are supported. **■Note** The frame was addressed to the router. The value *(control)* identifies the LLC control, *(source_MAC)* identifies the source MAC address, *(source_SAP)* identifies the source SAP address, *(dest_SAP)* identifies the destination SAP address, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
TKR.010 unexp U frm *(control)* fm *(source_MAC)* ssap *(source_SAP)* dsap *(dest_SAP)* nt *(net_id)*	478010	PTrace		This message indicates that an unexpected 802.2 LLC U (unnumbered) frame type has been received and only UI, XID, and TEST are supported. **■Note** This frame was a broadcast. The value *(control)* identifies the LLC control, *(source_MAC)* identifies the source MAC address, *(source_SAP)* identifies the source SAP address, *(dest_SAP)* identifies the destination SAP address, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TKR.011 add new RIF to *(MAC_add)* (RIF header) nt *(net_id)*	478011	UTrace		This message indicates that a new RIF is added to the 802.5 MAC address to RIF translation cache. The first 32 bits of the RIF header are displayed 16 bits at a time. The value *(MAC_add)* identifies the RIP headers MAC address and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
TKR.012 xtra RIF to *(MAC_add)* dscd nt *(net_id)*	478012	CTrace		This message indicates that additional RIF responses are received for a request which has already been satisfied. The value *(MAC_add)* identifies the MAC address and *(net_id)* identifies the network.		This is a normal event when there are source routing bridges in parallel. **■ Note** This is an information message only. No corrective actions are required.
TKR.013 del RIF to *(MAC_add)* nt *(net_id)*	478013	Low		This message indicates that a RIF is removed from the 802.5 MAC address to RIF translation. The value *(MAC_add)* identifies the MAC address and *(net_id)* identifies the network.		A frame sent to the indicated node returned with the Address Recognized bit unset. **■ Note** This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TKR.014 *(selftest)* fld *(error)* nt *(net_id)*	478014	High		This message indicates that an 802.5 Token Ring card self test has reported an error. Phases include: • Initial test • Board reset • Configuration • Open: Lobe Media Test, Physical Insertion, Address Verification, Roll Call Poll, and Request Parameters • Packet Output • Packet receive. The value *(error)* identifies the error condition and *(net_id)* identifies the network.		To correct this problem identify the Token Ring card that has failed the self test and repair or replace as necessary.
TKR.015 dwn sts cls nt *(net_id)*	478015	High		This alarm indicates that the interface has automatically removed itself from the ring due to a serious error condition. The interface attempts to join the ring again and may eventually come up. This is a hardware (ring or interface) problem. The exact cause is not logged, but these errors are counted, and counters in the +interface command should indicate the problem. The value *(net_id)* identifies the network.		To correct this problem look at the interface counters for one of these indications: • Lobe wire fault - The problem is with the network. • Remove received - The problem is with a network management station that has instructed this station to leave the ring.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TKR.016 dwn adap chk *(code)* nt *(net_id)*	478016	High		This alarm indicates that an interface has been brought down because of an adapter status check. The interface will not be self-tested, and will not come back up automatically. The value *(code)* identifies the adapter check codes and is an indication of which error occurred, and *(net_id)* identifies the network.		The adapter has detected a severe unrecoverable internal failure. If the problem persists, replace the interface.
TKR.017 pkt sz *(con_size)* too big for 4 Mbps, limiting to *(size)*, nt *(net_id)*	478017	High		This alarm indicates that the user set Packet Size, for the 802.5 network, packet size has been set to a value larger than what is allowed for a 4 Mbps network. The 8144, 11407, and 17800 byte sizes are only legal on a 16 Mbps network. The value *(con_size)* identifies the configured packet size, *(max_size)* identifies the maximum packet size and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
TKR.018 16 Mbps not supp on dev, net *(net_id)*	478018	High		This alarm indicates that the network speed has been set to 16 Mbps, and the router interface does not have the capability to operate at this speed. The network will operate at the 4 Mbps speed. The value *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TKR.019 runt pkt *(len)* frm *(source),* net *(net_id)*	478019	Medium	High	This alarm indicates that a packet has been received that is too short to contain the MAC and LLC headers. The value *(len)* identifies the packet length in bytes, *(source)* identifies the source address, and *(net_id)* identifies the network.		To correct this problem check for errors that are external to this node.
TKR.020 DN bd ln *(actual) (claimed) (source) -> (dest)* nt *(net_id)*	478020	Medium	High	This alarm indicates that a DECnet packet was received with a length field that was larger than the actual length of the packet. The value *(actual)* identifies the actual length of the broadcast packet, *(claimed)* identifies the claimed length of the packet, *(source)* identifies the source MAC address, *(dest)* identifies the destination MAC address, and *(net)* identifies the network.		Contact your customer service representative if this alarm appears.
TKR.021 LOOP rev *(source) -> (dest)*, nt *(net_id)*	478021	PTrace	High	This message indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet was received. The value *(source)* identifies the source MAC address, *(dest)* identifies the destination MAC address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TKR.022 LOOP odd skp *(count)*, *(source)* -> *(dest)*, nt *(net_id)*	478022	Medium		This message indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet had an odd skipcount in the packet. When this occurs the packet is discarded. The value *(count)* identifies the packet skipcount, *(source)* identifies the source MAC address, *(dest)* identifies the destination MAC address, and *(net)* identifies the network.		To correct this problem, check for configuration errors in the remote node.
TKR.023 LOOP bd skp *(count)*, *(source)* -> *(dest)*, nt *(net_id)*	478023	Medium		This message indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet had an odd skipcount in the packet that points to beyond the end of the packet. When this occurs the packet is discarded. The value *(count)* identifies the packet skipcount, *(source)* identifies the source MAC address, *(dest)* identifies the destination MAC address, and *(net)* identifies the network.		To correct this problem, check for configuration errors in the remote node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TKR.024 LOOP func *(func)* not forw, *(source)* -> *(dest)*, nt *(net_id)*	478024	Medium		This message indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet did not have a function code of forward (2). When this occurs the packet is discarded. The value *(func)* identifies the function code, *(source)* identifies the source MAC address, *(dest)* identifies the destination MAC address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
TKR.025 LOOP mc fwd dst *(f_MAC_add)*, *(source)* -> *(dest)* , nt *(net)*	478025	Medium		This message indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet is being forwarded to the specified next hop. The value *(f_MAC_add)* identifies the MAC address to which the packet must be forwarded, *(source)* identifies the source MAC address, *(dest)* identifies the destination MAC address, and *(net)* identifies the network.		To correct this problem, check for configuration errors in the remote node.
TKR.026 LOOP fwd *(source)* -> *(dest)* , nt *(net)*	478026	PTrace		This message indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet is being forwarded to the specified next hop. The value *(source)* identifies the source MAC address, *(dest)* identifies the destination MAC address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TKR.027 LOOP fwd to *(f_Enet_add)* dsc, rsn *(code)*, nt *(net)*	478027	High		This message indicates that an Ethernet Loopback Protocol (Configuration Testing Protocol) packet could not be forwarded to the specified address, for the reason specified by code. The value *(f_Enet_add)* identifies the Ethernet address to which the packet must be forwarded, *(code)* identifies the reason code, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
TKR.028 rif table corruption for interface *(net)*	478028	High		This message indicates that the rif table has become corrupted. The value *(net)* identifies the network.		This is an information message only. No corrective actions are required.
TKR.029 rif entry is being removed entry *(hwe_add) (type)* nt *(net)*	478029	PTrace		This message indicates that the rif entry aging function is removing an entry from the rif table. The value *(hwe_add)* identifies the, hardware address, *(type)* identifies the protocol type, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
TKR.030 MAC frm typ *(MAC_frame)* unex from *(hwe_add)* nt *(net)*	478030	High		The handler received a frame with an unexpected frame type. The value *(MAC_frame)* identifies the MAC frame type, *(hwe_add)* identifies the hardware address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
TKR.031 Main rcd on nt *(net)*	478031	PTrace		The handler received a maintenance packet. The value *(net)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TKR.032 test frm *(MAC_add)*, src sap *(source_SAP)*, nt *(net)*	478032	PTrace		This message indicates that the handler has received a test message. The value *(MAC_add)* identifies the MAC address, *(source_SAP)* identifies the source SAP address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
TKR.033 xid frm *(MAC_add)* , sap *(source_SAP)*, nt *(net)*	478033	PTrace		This message indicates that the handler has received an xid message. The value *(MAC_add)* identifies the MAC address, *(source_SAP)* identifies the source SAP address, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.
TKR.034 unable to allocate buffer in handler	478034	High		This message indicates that the handler was unable to allocate a buffer.		If you encounter large numbers of these errors, there is probably a major configuration problem. The free buffer pool is getting low or there was a temporary shortage of free buffers. **Warning** The handler will attempt to recover, but this situation could be a sign of a potential problem.
TKR.035 new RIF *(rif)* for *(MAC_add)* nt *(net)*	478035	UTrace		This message indicates that a new RIF has been added to the 802.5 MAC address to RIF translation cache. The value *(MAC_add)* identifies the MAC address, *(rif)* identifies the RIF value, and *(net)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
UDP.001 pkt *(source)* #> *(dest)* port *(port n)* no srvr	482001	PTrace		This message indicates that a packet has been discarded because UDP is not installed in the router. The packet was for the broadcast address. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address, and *(port n)* identifies the port number.		This is an information message only. No corrective actions are required.
UDP.002 pkt *(source)* #> *(dest)* port *(port n)* no srvr	482002	Low		This message indicates that a packet has been discarded because UDP is not installed in the router. The packet was addressed to the router. The value *(source)* identifies the source IP address, *(dest)* identifies the destination IP address, and *(port n)* identifies the port number.		This is an information message only. No corrective actions are required.
UDP.003 dsc pkt frm *(source)* bd length (len)	482003	Medium		This message indicates that a packet has been discarded because it had a UDP length greater than its IP length. The value *(source)* identifies the source IP address and *(len)* identifies the UDP length that exceeds the IP length.		This is an information message only. No corrective actions are required.
UDP.004 bd cksm clc *(calc_csum)* rcv *(rcvd_csum)*	482004	Medium		This message indicates that a packet has been discarded because it had a bad checksum. The value *(calc_csum)* identifies the calculated checksum and *(rcvd_csum)* identifies the received checksum.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
XN.001 *(prot)* trunc pkt frm *(net)*/*(node)*, xns *(xns_len)* phys *(phys_len)*	489001	Medium		This alarm indicates that a a packet has an XNS packet length greater than the packet's physical length. The value *(prot)* identifies the protocol involved, *(net)* identifies the network source of the packet, *(node)* identifies the source node, *(xns_len)* identifies the length of the Xerox Network Core packet, and *(phys_len)* identifies the physical length of the packet.		To correct this problem, check for: a) A programming error in the remote node. If this is the case, correct the software configuration in the remote node. b) Possible truncation by network.
XN.002 *(prot)* non-zero TC frm *(net)* / *(node)* *(tc)*	489002	Medium		The reserved bits in the Transport Control field of the header were not zero. An Error (checksum) packet is sent. The value *(prot)* identifies the protocol involved, *(net)* identifies the network source of the packet, *(node)* identifies the source node, and *(tc)* identifies the Transport Control field.		This is an information message only. No corrective actions are required.
XN.003 *(prot)* bd rtng cksum frm *(net)* / *(node)*, *(rcvd_csum)* *(cmp_csum)*	489003	Medium		This message is generated when the checksum in a packet being forwarded does not match the calculated checksum for the packet. An Error (checksum) packet is sent. The value *(prot)* identifies the protocol involved, *(net)* identifies the network source of the packet, *(node)* identifies the source node, *(rcvd_csum)* identifies the received checksum, and *(cmp_csum)* identifies the compared checksum.		To correct this problem, check for: a) A programming error in the remote node. If this is the case, correct the software configuration in the remote node. b) Packet corruption on the network.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
XN.004 *(prot)* hop cnt ovflo frm *(net)* / *(node)* to *(dest)*	489004	Medium		This message is generated when a packet's hop count counts up past 15 and overflows. An Error (hop count) packet will be sent. The value *(prot)* identifies the protocol involved, *(net)* identifies the network source of the packet, *(node)* identifies the source node, *(dest)* identifies the destination network.		This is an information message only. No corrective actions are required.
XN.005 *(prot)* no gwy frm *(net)* /*(node)* to *(dest)*	489005	Medium		This message is generated when a packet cannot be forwarded because there is no gateway to the destination network. An Error (unreachable) packet will be sent. The value *(prot)* identifies the protocol involved, *(net)* identifies the network source of the packet, *(node)* identifies the source node, *(dest)* identifies the destination network.		This is an information message only. No corrective actions are required.
XN.006 *(prot)* wstd hop frm *(net)* /*(node)* to *(dest*	489006	Medium		This packet is generated when a packet is being sent out the same network interface it arrived on. This router is not the best path off that network to the destination network. The value *(prot)* identifies the protocol involved, *(net)* identifies the network source of the packet, *(node)* identifies the source node, *(dest)* identifies the destination network.		To correct this problem, check for: a) errors in the configuration of the first-hop router on the network end node. If this is the case, reconfigure the node. b) Inconsistent routing tables. If this is the case correct the routing table configurations.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
XN.007 *(prot)* dst hst 0 frm *(net)* /*(node)* to *(dest)*	489007	Medium		This message indicates that a packet is addressed to node 000000000000. This is an illegal host address. An Error (checksum) packet will be sent. The value *(prot)* identifies the protocol involved, *(net)* identifies the network source of the packet, *(node)* identifies the source node, *(dest)* identifies the destination network.		This is an information message only. No corrective actions are required.
XN.008 *(prot)* *(s_net)* /*(s_node)*-> *(d_net)* / *(d_node)*	489008	PTrace		This message indicates that a packet has been forwarded. The value *(prot)* identifies the protocol involved, *(s_net)* identifies the source network, *(s_node)* identifies the source node, *(d_net)* identifies the destination network, and *(d_node)* identifies the destination node.		This is an information message only. No corrective actions are required.
XN.009 *(prot)* pkt too lng to frwd *(p_size)* > *(m_size)* nt *(net_id)* frm *(net)* /*(node)*	489009	Medium		This message indicates that a forwarded packet cannot be sent out the required interface because it is too long. An Error (size) packet will be sent. The value *(prot)* identifies the protocol involved, *(p_size)* identifies the packet size, *(m_size)* identifies the maximum packet size, (net_id) identifies the network, *(net)* identifies the network, and *(node)* identifies the node.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
XN.010 *(type)* frm *(s_net)* /*(s_node)* for *(d_net)* /*(d_node)* dsc, rsm *(code)*	489010	Low		This message indicates that an outgoing packet was not successfully transmitted for the reason indicated by the error code. The value *(type)* identifies the protocol type, *(s_net)* identifies the source network, *(s_node)* identifies the source node, *(d_net)* identifies the source network, *(d_node)* identifies the source node, and *(code)* identifies the error code specific to this alarm.		This is an information message only. No corrective actions are required.
XN.011 *(prot)* intrfc *(net)*/*(node)* net *(net_id)* up	489011	Low		This message indicates that a specified interface has come up, and has been enabled for the specified XNS protocol. The value *(prot)* identifies the protocol type, *(net)* identifies the source network, *(node)* identifies the source node, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.
XN.012 *(prot)* del nt *(d_net)* rt via *(gw)* nt *(net_id)*	489012	Low		This alarm indicates that a specified route has been deleted because the first hop interface for that route has gone down. The value *(prot)* identifies the protocol type, *(d_net)* identifies the destination network, *(gw)* identifies the gateway, and *(net_id)* identifies the network.		To correct this problem identify which interface is down and repair the network at that location.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
XN.013 *(prot)* tbl ovrfl, dst *(d_net)*	489013	High		This message indicates that a new entry cannot be made to the routing table because it is already full. The value *(prot)* identifies the protocol type, *(d_net)* identifies the destination network.		To correct this problem increase the size of the routing table for the specified protocol.
XN.014 *(prot)* echo type *(op)* to skt socket frm *(s_net)* / *(s_node)*	489014	Low		This message indicates that an echo type packet has been received with the specified operation to the specified socket. The value *(prot)* identifies the protocol type, *(op)* identifies the operation, *(s_net)* identifies the source network, *(s_node)* identifies the source node.		This is an information message only. No corrective actions are required.
XN.015 *(prot)* bd src *(s_net)*/*(s_node)* nt *(net_id)*	489015	Medium		This message indicates that a packet was returned to the sender, but the sender's node address was a multicast address or the illegal address 000000000000. This happens when sending an Echo reply or an Error packet, or replying to other queries. This packet will be discarded. The value *(prot)* identifies the protocol type, *(s_net)* identifies the source network, *(s_node)* identifies the source node, and *(net_id)* identifies the network.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
XN.016 *(prot)* bad net 0 *(s_net)*/*(s_node)* - *(d_net)*/*(d_node)*	489016	Medium		This message indicates that a packet was being returned to the sender, and the source network was zero, but the destination network was non-zero. This happens when sending an Echo reply or an Error packet, or replying to other queries. The packet will be discarded. The value *(prot)* identifies the protocol type, *(s_net)* identifies the source network, *(s_node)* identifies the source node, *(d_net)* identifies the destination network, and *(d_node)* identifies the destination node,		This is an information message only. No corrective actions are required.
XN.017 *(prot)* no mem for err pkt	489017	High		This message indicates that there insufficient memory available to copy the offending packet into an Error packet. An Error packet will not be sent. The value *(prot)* identifies the protocol type.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
XN.018 *(prot)* short *(len)* pkt frm *(s_net)*/ *(s_node)* (?) net *(net_id)*	489018	Medium		This message indicates that a packet has a physical length shorter than the minimum XNS header length. The value *(s_net)* identifies the source network and *(s_node)* identifies the source node. These may or may not be valid packet data, depending on how severe the truncation is. The value *(prot)* identifies the protocol type, *(len)* identifies the difference in the packet's physical and minimum lengths, and *(net_id)* identifies the network.		To correct this problem, check for configuration errors in the remote node or truncation in the network.
<app_id> does not exist				The application identified by <app_id> is either not configured or not active because of improper configuration.		Make sure that the application is properly configured and is active. Boot the QCL profile.
No QoS features configured				None of the QoS features are configured.		Configure the required features and boot the QCL profile.
IpBaRmark Prof #<num> does not exist				IP BA Remarker profile (indicated by <num>) is either not configured or not booted.		Configure/boot the IP BA Remarker profile. Then boot the QCL profile.
Ingress IP ClTcQos-Map Prof #<num> does not exist				The "IP Classifier, Traffic Conditioner & QoS Mapper" profile (indicated by <num>) used for Ingress, is not configured.		Configure the "IP Classifier, Traffic Conditioner & QoS Mapper" profile with required classifiers. Boot the IP MF classifiers used in the profile (not required if they are already booted) and then boot the QCL profile.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
No classifiers in Ingress IP ClTcQos-Map Prof #<num>				All the entries of “IP Classifier, Traffic Conditioner & QoS Mapper” profile (indicated by <num>) used for Ingress, are configured with IP MF classifiers that do not exist (i.e. the IP MF classifiers are either not configured or not booted).		Configure/boot the IP MF classifiers used in the “IP Classifier, Traffic Conditioner & QoS Mapper” profile and then boot the QCL profile.
Egress IP ClTcQos-Map Prof #<num> does not exist				The “IP Classifier, Traffic Conditioner & QoS Mapper” profile (indicated by <num>) used for Egress, is not configured.		Configure the “IP Classifier, Traffic Conditioner & QoS Mapper” profile with required classifiers. Boot the IP MF classifiers used in the profile (not required if they are already booted) and then boot the QCL profile.
No classifiers in Egress IP ClTcQos-Map Prof #<num>				All the entries of “IP Classifier, Traffic Conditioner & QoS Mapper” profile (indicated by <num>) used for Egress, are configured with IP MF classifiers that do not exist (i.e. the IP MF classifiers are either not configured or not booted).		Configure/boot the IP MF classifiers used in the “IP Classifier, Traffic Conditioner & QoS Mapper” profile and then boot the QCL profile.
IPX ClTcQosMap Prof #<num> does not exist				The “IPX Classifier, Traffic Conditioner & QoS Mapper” profile (indicated by <num>) is not configured.		Configure the “IPX Classifier, Traffic Conditioner & QoS Mapper” profile with required classifiers. Boot the IPX classifiers used in the profile (not required if they are already booted) and then boot the QCL profile.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
No classifiers in IPX ClTcQosMap Prof #<num>				All the entries of “IPX Classifier, Traffic Conditioner & QoS Mapper” profile (indicated by <num>) are configured with IPX classifiers that do not exist (i.e. the IPX classifiers are either not configured or not booted).		Configure/boot the IPX classifiers used in the “IPX Classifier, Traffic Conditioner & QoS Mapper” profile and then boot the QCL profile.
TB ClTcQosMap Prof #<num> does not exist				The “TB Classifier, Traffic Conditioner & QoS Mapper” profile (indicated by <num>) is not configured.		Configure the “TB Classifier, Traffic Conditioner & QoS Mapper” profile with required classifiers. Boot the classifiers used in the profile (not required if they are already booted) and then boot the QCL profile.
No classifiers in TB ClTcQosMap Prof #<num>				All the entries of “TB Classifier, Traffic Conditioner & QoS Mapper” profile (indicated by <num>) are configured with classifiers that do not exist (i.e. the classifiers are either not configured or not booted).		Configure the “TB Classifier, Traffic Conditioner & QoS Mapper” profile with required classifiers. Boot the classifiers used in the profile (not required if they are already booted) and then boot the QCL profile.
AT ClTcQosMap Prof #<num> does not exist				The “AT Traffic Conditioner & QoS Mapper” profile (indicated by <num>) is not configured.		Check the number of “Classifier, Traffic Conditioner & QoS Mapper” channels required for all the configured “Classifier, Traffic Conditioner & QoS Mapper” profiles (each configured entry in the profile requires one channel) and appropriately configure the QoS General Parameter - “Max ClTcQosMap Channels”. Boot the node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Insuff traffic conditioners				There are not enough Traffic Conditioners to bring up the classification, traffic conditioning & QoS mapping features.		Check the number of Traffic Conditioners required for all the configured “Classifier, Traffic Conditioner & QoS Mapper” profiles (each profile entry configured for traffic conditioning requires one traffic conditioner) and appropriately configure the QoS General Parameter - “Max Conditioners”. Boot the node.
Service Prof #<number> does not exist				Service profile (indicated by <num>) is not configured to bring up queuing & scheduling feature (which services the packets as per their QoS mappings) for the application.		Configure the service profile with the required services and boot the QCL profile.
Scheduler not available				There are not enough service channels to bring up queuing & scheduling feature (which services the packets as per their QoS mappings) for the application.		Check the number of Service channels required for the configured Service profile (each entry configured in the Service profile requires one or more channels) and appropriately configure the QoS General Parameter - “Max Service Channels”. Boot the node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Insuff service channels				There are not enough service channels to bring up the queuing and scheduling feature which services the packets (QoS mappings) for the application.		Check the number of Service channels required for the configured Service profile (each entry configured in the Service profile requires one or more channels) and appropriately configure the QoS General Parameter - “Max Service Channels”. Boot the node.
Insuff Q mgmt channels				There are not enough queue management channels to bring up the queuing and scheduling feature which services the packets (QoS mappings) for the application.		Check the number of queue management channels required for the configured Service profile (each Service profile entry that uses queue management requires one channel) and appropriately configure the QoS General Parameter - “Max Q Mgmt Channels”. Boot the node.
QCL Prof #<num> ignored - Duplicate Record for <app_id>				The QCL profile (<num> is the profile number) is a duplicate record for the application identified by <app_id> (i.e. multiple QCL profiles are configured for the same application) and hence ignored.		Delete the duplicate QCL profiles and boot the one which is needed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
<n> entries of Ingress IP ClTcQosMap Prof #<num> ignored - no classifiers				The “IP Classifier, Traffic Conditioner & QoS Mapper” profile (<num> is the profile number) used for Ingress, has entries configured with IP MF classifiers that do not exist (i.e. the IP MF classifiers are either not configured or not booted). All these entries (<n> is the total number of these entries) are ignored.		Either configure/boot the IP MF classifiers or delete the entries (if not required). Boot the QCL profile.
<n> entries of Egress IP ClTcQosMap Prof #<num> ignored - no classifiers				The “IP Classifier, Traffic Conditioner & QoS Mapper” profile (<num> is the profile number) used for Egress, has entries configured with IP MF classifiers that do not exist (i.e. the IP MF classifiers are either not configured or not booted). All these entries (<n> is the total number of these entries) are ignored.		Either configure/boot the IP MF classifiers or delete the entries (if not required). Boot the QCL profile.
<n> entries of IPX ClTcQosMap Prof #<num> ignored - no classifiers				The “IPX Classifier, Traffic Conditioner & QoS Mapper” profile (<num> is the profile number) has entries configured with IPX classifiers that do not exist (i.e. the IPX classifiers are either not configured or not booted). All these entries (<n> is the total number of these entries) are ignored.		Either configure/boot the IPX classifiers or delete the entries (if not required). Boot the QCL profile.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
<n> entries of TB ClTcQosMap Prof #<num> ignored - no classifiers				The "TB Classifier, Traffic Conditioner & QoS Mapper" profile (<num> is the profile number) has entries configured with classifiers that do not exist (i.e. the classifiers are either not configured or not booted). All these entries (<n> is the total number of these entries) are ignored.		Either configure/boot the classifiers or delete the entries (if not required). Boot the QCL profile.
<n> entries of Service Prof #<num> ignored - Duplicate Records				The Service profile (<num> is the profile number) has entries with duplicate configuration (i.e. multiple entries are configured for same services). All duplicate entries (<n> is the total number of these entries) are ignored.		Delete the duplicate entries and boot the QCL profile.
FAILED TO NEGOTIATE ISAKMP PARAMETERS WITH aa.bb.cc.dd (Reason)		High		Cannot establish ISAKMP with remote IPSec peer because the proposals were rejected by the remote peer.		Contact your customer service representative.
REMOTE PEER DOES NOT RESPOND TO ISAKMP REQUEST		High		Cannot establish communication with remote peer. Either the remote is not configured for ISAKMP or the path to remote is broken.		Check configuration. Contact your customer service representative.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
FAILED TO NEGOTIATE IPSec PARAMETERS WITH aa.bb.cc.dd (Reason)		High		Fails to negotiate a set of acceptable IPSec parameters with the remote node.		Check the IPSec Profile on both nodes to ensure at least one common set of profiles exist between the nodes.
ISKAMP POLICY # xx DOES NOT EXIST		High		The specified ISAKMP profile does not exist.		Check the configuration.
IPSec PROFILE xx DOES NOT EXIST		High		The specified IPSec profile does not exist.		Check the configuration.
ESTABLISHED ISAKMP CONNECTION WITH aa.bb.cc.dd		Medium		Successfully negotiated a ISAKMP SA with the remote. The node proceeds to establish IPSec Security.		This is an informative message.
ESTABLISHED IPSec CONNECTION with aa.bb.cc.dd		Medium		Successfully established IPSec connection with the remote peer. Data passing can now start on the tunnel.		This is an informative message.
RECEIVED UN-AUTHORIZED ISAKMP REQUEST FROM aa.bb.cc.dd		High		Received unexpected requests to establish ISAKMP SA from remote node aa.bb.cc.dd. The request is ignored.		This is an informative message.
INSUFFICIENT MEMORY TO INITIALIZE IPSec MODULE		High		The system does not have enough memory to initialize the IPSec module. IPSec is disabled.		Check memory allocated.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
MBR.001, MBR - Not Enough Dynamic Memory ***for structure***		High		This message indicates that the router cannot allocate enough memory for a structure.		Reboot the system, if the problem persits, contact Customer Service.
MBR.002, MBR - ***(source ip address, group ip address)*** not created - max limit hit		High		This message indicates that the router has reached the maximum MBR routes and new route for ***(source ip address, group ip address)*** is not created. Although Multicast protocol is still active on the router, the protocol may not be able to perform proper forwarding due to insufficient memory.		Reset the Multicast Forwarding Table. If this persists, increase Multicast Forwarding Table size.
MFE.001, MFE.1 Initialization Failure - cause: ***text***		High		This message indicates that the router cannot properly initialize the Multicast Forwarding Engine. The cause is ***text***.		Reboot the system, if the problem persists, contact Customer Service.
MFE.002, MFE.2 Unable to allocate packet buffer		Medium		This message indicates that the router cannot allocate a packet buffer within the Multicast Forwarding Engine framework. Although the multicast routing protocol is still active on the router, the router is not able to duplicate and forward a multicast packet.		Investigate why the router is low on packet buffers. Try rebooting the system, if the problem persists, contact Customer Service.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PIM.001, PIM.1: Debug string		High		This debug alarm (although at HIGH priority), will never show up unless it is explicitly turned on via DEBUG menu. It is set at high priority to ease debugging a specific area of PIM at a life network.		This is debug message only. No corrective action is required. Customer Service must be contacted to enable/disable this alarm.
PIM.003, PIM.3: No mem for ***structure_1*** (in ***function_1***)		High		This alarm indicates that the router cannot allocate memory for a required PIM structure of type ***structure_1*** in ***function_1***. Although PIM protocol is still active on the router, the protocol may not be able to perform correctly due to insufficient memory.		Investigate why the router is low on memory. Try reboot the system, if the problem persists, contact Customer Service.
PIM.004, PIM.4: CRP ***ip address*** has no grp.		Medium		This alarm indicates a Candidate RP is configured but the associated group profile is not configured.		Configure the appropriate group profile or remove the corresponding candidate RP entry.
PIM.005, PIM.5: Static RP ***ip address*** has no grp		Medium		This alarm indicates a Static RP is configured but the associated group profile is not configured.		Configure the appropriate group profile or remove the corresponding static RP entry.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PIM.006, PIM.6: Inconsistent RP for ***ip address*** (us: ***ip address*** nbr ***ip address 's ip address***)		High		This alarm indicates that we receive a join prune message from a neighbour, and it has a different RP information for the group than what the router has. PIM will not work correctly with inconsistent views of RP sets.		Investigate if both routers have the same set of RP mapping. If any static RP is configured on the routers, make sure the precedence is identical on both routers. If the neighbour router is another vendor's equipment, verify if a different hash function should be used. If the problem persists, contact Customer Service.
PIM.007, PIM.7: Reg not sent for ***(IP address, IP Address)***, hit limit		Low		This indicates that the router is not forwarding the multicast packet via register to the RP because the configured register rate limit has been reached.		Investigate if the source is sending too many packets per second and if this is a desired scenario to protect the RP. Also investigate if the configured limit should be set higher (the default is no limit).
PIM.008, PIM.8: Recv ***type*** msg from non-nbr ***ip address***		Low		The router receives a PIM ***(message type)*** message from a neighbour ***(ip address)*** that it has not received its Hello message.		This is informational message only. No corrective action is required.
PIM.009, PIM.9: Reject ***type*** msg from ***ip address***. (c:***error reason*** val:***value***)		Low		The router receives a mal-formatted PIM (***message type***) message from a router (***ip address***). The error reason indicates the problems with the message and ***value*** indicates the error value.		This is an informational message only. No corrective action is required. If this problem persists, investigate if the sending router has any misconfigurations.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PIM.011, PIM.11: Recv Reg for ***ip address*** from ***ip address***, but RP is ***ip address***		High		This alarm indicates that the router receives a PIM register message for group ***ip address*** but it is not the RP, and the RP is ***ip address.***		Investigate if both routers have the same set of RP mapping. If any static RP is configured on the routers, make sure the precedence are identical on both router. Verify if both routers have the same rpsets. If the problem persists, contact Customer Service.
PIM.012, PIM.12: Recv CRP msg on ***ip address*** from ***ip address***, but BSR is ***ip address***		Medium		This alarm indicates that the router receives a PIM candidate rp advertisement message, but it is not the BSR and the BSR is ***ip address***.		Investigate if there is connectivity lost and cause BSR message not propagated throughout the PIM networks. All routers must have the consistent view of who is the BSR.
PIM.013, PIM.13: Max Route Hit, (***source ip address, group ip address***) not created		High		This alarm indicates that the router has reached the maximum PIM routes and new route for ***(source ip address, group ip address***) is not created. Although PIM protocol is still active on the router, the protocol may not be able to perform correctly due to insufficient memory.		If this problem persists, increase the PIM table size.
PIM.014, PIM.14: Recv pim msg on non-pim if ***ip address***		Low		This alarm indicates that the router is receiving PIM message on the interface that PIM is not configured.		Investigate if PIM needs to be configured on that interface. If not, remove the neighbour's PIM configuration so that the PIM message is not generated.

Chapter 10
General and Miscellaneous Alarms and Reports

Introduction

This chapter describes alarms and reports of a general or miscellaneous nature. Any documented alarm or report that you can not find in the first chapters of this manual is likely in this chapter.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
%s HAS DETECTED A STREAMING DEVICE	115002	High	Minor		115003	Contact your customer service representative if this alarm is displayed.
%s NCCP CRC ERROR	115001	High	Minor			Contact your customer service representative if this alarm is displayed.
%s STREAMING DEVICE CONDITION CLEARED	115003	High	Normal			Contact your customer service representative if this alarm is displayed.
BAD P(S)	46005	Low	Critical	This alarm indicates that a data packet, with the packet number out of sequence, has been received.	46000	Complete the following procedure to correct this alarm condition: a) Install a DataScope to monitor the line. b) Verify that your Vanguard device is operating correctly. c) Check the configuration to be sure the Packet Window sizes match at both ends.
bop_bri_sm_pck() DEFAULT : RETURN	241027	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
NO PROFILE AVAILABLE FOR *(name)*	270011	Medium	Critical	This alarm indicates that a profile with remote nodename *(name)* could not be found.		Check the configurations of the local PPP profiles, and the remote equipment for consistent configuration of names.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
##@@**Event to LCON %d, %s	157003	High	Normal			Contact your customer service representative if this alarm is displayed.
%d BYTES LOADED FROM NSO DISK	65000	High	Critical			Contact your customer service representative if this alarm is displayed.
%ld - RECEIVED INVALID PROTOCOL ID FROM THE ROUTER %d	188000	High	Minor			Contact your customer service representative if this alarm is displayed.
%s - CANNOT BE ACTIVATED. <SRC, DST, ENCAPSULATION> CONFLICTS WITH STN %d	289002	Medium	Critical			Contact your customer service representative if this alarm is displayed.
%s - CLOCK SOURCE OVERRIDE	108004	Low	Minor			Contact your customer service representative if this alarm is displayed.
%s - CONFIG ERROR - %s	156008	High	Critical			Contact your customer service representative if this alarm is displayed.
%s - CONFIG ERROR - %s %d	156000	High	Critical			Contact your customer service representative if this alarm is displayed.
%s - CONFIG ERROR - %s %s	156009	High	Critical			Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
%s - DATA LOST FROM DATA QUEUE	232000	High	Major			This is an information message only. There are no corrective actions necessary.
%s - DATA LOST FROM DATA QUEUE	233000	High	Major			This is an information message only. There are no corrective actions necessary.
%s - DATA LOST FROM DATA QUEUE	289000	High	Major			Contact your customer service representative if this alarm is displayed.
%s - DATA LOST FROM DATA QUEUE	290000	High	Major			Contact your customer service representative if this alarm is displayed.
%s - DATA LOST FROM Rx DATA QUEUE	292000	High	Major			Contact your customer service representative if this alarm is displayed.
%s - DATA LOST FROM Tx DATA QUEUE	292001	High	Major			Contact your customer service representative if this alarm is displayed.
%s - DPAD '%s' IS NON RESPONDING	116000	High	Major			Contact your customer service representative if this alarm is displayed.
%s - ERRONEOUS BOOLEAN PARAMETER: %s	108003	Medium	Minor			Contact your customer service representative if this alarm is displayed.
%s - EXCEEDING MAXIMUM RANGE ALLowED	156010	High	Critical			Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
%s - INVALID ENCAPSULATION	233001	Medium	Minor			This is an information message only. There are no corrective actions necessary.
%s - INVALID ENCAPSULATION	271000	Medium	Major			Contact your customer service representative if this alarm is displayed.
%s - INVALID ENCAPSULATION	271001	Conn	Minor	This alarm indicates that an invalid encapsulation type has been used.		Check the local and remote port configurations and reconfigure as required using a valid encapsulation type.
%s - INVALID ENCAPSULATION	289001	Medium	Minor			Contact your customer service representative if this alarm is displayed.
%s - INVALID ENCAPSULATION	290001	Medium	Minor			Contact your customer service representative if this alarm is displayed.
%s - LAN CONNECTION BOOTED	156005	High	Normal			Contact your customer service representative if this alarm is displayed.
%s - LAN CONNECTION BOOT FAILURE - %s	156006	High	Normal			Contact your customer service representative if this alarm is displayed.
%s - LAN CONNECTION CREATION FAILURE - %s	156007	High	Critical			Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
%s - LAN CONNECTION CREATION FAILURE - %s	157001	High	Critical			Contact your customer service representative if this alarm is displayed.
%s - LAN CONNECTION CREATION FAILURE - %s	189000	High	Critical			Contact your customer service representative if this alarm is displayed.
%s - LAN CONNECTION DISABLE FAILURE - %s	156003	High	Normal			Contact your customer service representative if this alarm is displayed.
%s - LAN CONNECTION DISABLED	156001	High	Warning		156002	Contact your customer service representative if this alarm is displayed.
%s - LAN CONNECTION ENABLE FAILURE - %s	156004	High	Normal			Contact your customer service representative if this alarm is displayed.
%s - LAN CONNECTION ENABLED	156002	High	Normal			Contact your customer service representative if this alarm is displayed.
%s - NO HEARTBEAT	292002	High	Critical			Contact your customer service representative if this alarm is displayed.
%s - NS INVALID CONFIGURATION	229005	High	Critical			Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
%s - PACKET RECEIVED WITH INVALID RFC1294 ENCAPSULATION	191000	High	Minor			Contact your customer service representative if this alarm is displayed.
%s - PACKET TYPE NOT SUPPORTED FOR ENCAPSULATION	234000	Low	Minor			This is an information message only. There are no corrective actions necessary.
%s - PORT ERROR COUNT > THRESHOLD	40000	Medium	Warning			Contact your customer service representative if this trap is displayed.
%s - PORT ERROR COUNT > THRESHOLD	41000	Medium	Warning			Contact your customer service representative if this trap is displayed.
%s - RECEIVED INVALID FORWARDER ID FROM THE WAN LINK %d	159001	High	Warning			Contact your customer service representative if this alarm is displayed.
%s - RECEIVED INVALID FORWARDER ID FROM THE WAN LINK %d	188001	High	Major			Contact your customer service representative if this alarm is displayed.
%s - SNMP Manager is Restarting	152000	High	Major			Contact your customer service representative if this trap is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
%s - STPE BAD HELLO THRESHOLD EXCEEDED	159000	High	Warning			Contact your customer service representative if this alarm is displayed.
%s - UNSUP-PORTED SPEED: OPERATING AT %d BITS PER SECOND	108001	Medium	Minor			Contact your customer service representative if this alarm is displayed.
%s - UNSUP-PORTED RECEIVE BYTE COUNT: OPERATING WITH %d RX BYTE COUNT	108002	Medium	Minor			Contact your customer service representative if this alarm is displayed.
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	40001	Medium	Minor			Contact your customer service representative if this trap is displayed.
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	41001	Medium	Minor			Contact your customer service representative if this trap is displayed.
%s - WSL BOOT COMPLETE	157000	High	Normal			Contact your customer service representative if this alarm is displayed.
%s CONNECTED TO MAIN CHANNEL	152002	High	Normal			Contact your customer service representative if this trap is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
%s CONNECTED TO PMS CHANNEL	152004	High	Normal			Contact your customer service representative if this trap is displayed.
%s DUPLICATE NCCP DEVICE ent #%d	116002	High	Critical			Contact your customer service representative if this alarm is displayed.
%s FAILED MAIN CHANNEL CONNECT	152001	High	Major			Contact your customer service representative if this trap is displayed.
%s IS NOT MONITORED BY BOD, NO PARALLEL LCON CREATED	157002	Medium	Major			Contact your customer service representative if this alarm is displayed.
%s LOST MAIN CHANNEL CONNECTION	152003	High	Major		152002	Contact your customer service representative if this trap is displayed.
%s LOST PMS CHANNEL CONNECTION	152005	High	Major		152004	Contact your customer service representative if this trap is displayed.
%s NCCP PROTOCOL ERROR	116006	High	Warning			Contact your customer service representative if this alarm is displayed.
%s STATE SEARCH ABORTED %s	115007	High	Major			Contact your customer service representative if this alarm is displayed.
%s-<%d> %s THRESHOLD EXCEEDED	283004	Medium	Warning			Contact your customer service representative if this alarm is displayed.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
%s-<%d> - Warning - Illegal T1/E1 clock mode - Both ports configured for 'REC' timing	283009	High	Critical			Contact your customer service representative if this alarm is displayed.
(#) BYTES LOADED FROM EXTENDED FLASH MEMORY	211001	High	Warning	This message indicates the size of the image that has been successfully loaded. The value *(#)* identifies the number of bytes loaded into FLASH.		This is an information message only. No corrective action is required.
(cause) - NON-RECOVERABLE INBOUND ERROR	125005	High	Major	This alarm indicates that a serious protocol violation occurred while waiting for data from a local device or local host. This alarm can be caused by exhausting the configured number of retries. The value *(cause)* indicates one of the following errors: • time-out • bad CRC • overflow • received NAK • received EOT - host terminated Poll/Select • in some cases, received a legal protocol response that is was misplaced	125000	To correct any of these problems, boot the port and check the line integrity.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
(cause) - NON-RECOVERABLE OUTBOUND ERROR	125006	High	Major	This alarm indicates that a serious protocol violation occurred while waiting for a response to previously sent data from a local device or local host. The value *(cause)* can indicate one of these causes for the alarm: • exhausting number of retires caused by time-out • in some cases, received a legal protocol response that was misplaced • received EOT - host terminated Poll/Select	125000	If this alarm occurs, boot the port and check the integrity of the line.
(entity) - BOOT COMPLETE	176000	Conn	Normal	This message indicates that an ALC entity has successfully been booted. The value *(entity)* identifies the ALC line, Interchange Address or Terminal affected.		This message is for information-purposes only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
(entity) - BOOT FAILURE *(cause)*	176001	High	Normal	This alarm indicates that an ALC entity has failed to boot successfully. The value *(entity)* identifies the ALC line, Interchange Address or Terminal affected, while *(cause)* identifies one of these possible reasons for the failure: a) No Port Record b) Port is Disabled c) No Interchange Record d) Port Record is not ALC e) Interchange is disabled f) Port Subtype change requires node boot g) Terminal is not defined. h) No connection defined i) Connection disabled j) # buffer change requires node boot k) Max component per frame change requires node boot l) Max frame size change requires node boot. m) # leading pad chars change requires node boot n) # trailing pad chars change requires node boot		To correct this problem, complete the corrective actions for the *(cause)* indicated: a) Configure a port in the Port record. b) Enable the port. c) Configure an Interchange Record for the port. d) Reconfigure the port as an ALC port. e) Enable the interchange. f) Boot the node. g) Configure a terminal entity if one is required h) Configure a connection type for the appropriate entity. i) Enable the connection. j) Boot the node after changing this parameter. k) Boot the node after changing this parameter. l) Boot the node after changing this parameter. m) Boot the node after changing this parameter. n) Boot the node after changing this parameter.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
(entity) - BUFFER DISCARDED *(cause)*	178000	Medium	Minor	This alarm indicates that an ALP PAD module failure has occured and that buffered data has been discarded. The value *(entity)* identifies the ALC line, Interchange Address or Terminal affected while *(cause)* indicates one of these possible reasons for the failure: a) ALC QUEUE FULL: The queue towards ALC is full. b) X.25 QUEUE FULL: The queue towards X.25 is full. c) ALC BAD WRITE: A write request to ALC has failed. d) X.25 BAD WRITE: A write request to X.25 has failed. e) ENTITY OFFLINE: The connection was off line f) BAD HEADER: The received header was invalid. g) BAD ADDRESS: The received ALC address was invalid.		Perform the corrective actions that respond to the (cause) indicated: a) Increase the amount of bandwidth assigned to ALC. b) Increase the amount of bandwidth assigned to X.25. c) Check all node connections and verify that the network configuration is correct. d) Check all node connections and verify that the network configuration is correct. e) Verify that the entity is online. If it is not, check cause for that entities failure. f) Check the networks configuration and correct as necessary. g) Check the networks configuration and correct as necessary.
(entity) - DISABLE FAILURE	176003	High	Normal	This alarm indicates that an entity has been failed to become disabled because it was already disabled. The value *(entity)* identifies the ALC line, Interchange Address or Terminal affected.		This message is for information purposes only. No corrective actions are required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
(entity) - DISABLED	176002	High	Warning	This message indicates that an entity has been disabled. The value *(entity)* identifies the ALC line, Interchange Address or Terminal affected.	176004	This message is for information purposes only. No corrective actions are required.
(entity) - ENABLE FAILURE	176005	High	Normal	This message indicates that an entity has failed to be enabled because it was already enabled. The value *(entity)* identifies the ALC line, Interchange Address or Terminal affected.		This message is for information purposes only. No corrective actions are required.
(entity) - ENABLED *(cause)*	176004	High	Normal	This message indicates that an entity has been enabled. The value *(entity)* identifies the ALC line, Interchange Address or Terminal affected.		This message is for information purposes only. No corrective actions are required.
(entity) - FLOW CONTROL IMPOSED	177002	Medium	Warning	This alarm indicates that the network is congested and Flow Control has been imposed to prevent the ALC PAD from forwarding traffic to the network. The value *(entity)* identifies the ALC line, Interchange Address or Terminal affected.	177003	To correct this problem, increase the available network bandwidth.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
(entity) - FLOW CONTROL RELEASED	177003	Medium	Normal	This message indicates that the ALC PAD has received an indication, from the network, that Flow Control has been removed. The ALC PAD will restart sending data to the network. The value *(entity)* identifies the ALC line, Interchange Address or Terminal affected.		This is an information message only. No corrective action is required.
(entity) - HOST TIMEOUT	177011	Medium	Minor	This alarm indicates that the ALC Handler has not received a poll for the specified entity within the time specified by the host timeout. The value *(entity)* identifies the ALC line, Interchange Address or Terminal affected.	177012	Check all connections to the host and correct as necessary.
(entity) - MESSAGE DISCARDED, NO CONNECTION	177013	Medium	Minor	This alarm indicates that there is no connection available. A message has been received on ALC entity, but no connection is associated with that entity. The value *(entity)* identifies the ALC line, Interchange Address or Terminal affected.		Verify that the correct entries are configured on the ALC PAD.
(entity) - X.25 CALL FAILED	178001	High	Major	This message indicates that the X.25 call setup has failed. The value *(entity)* identifies the ALC line, Interchange Address or Terminal affected.		To correct this problem, check the Called Address and reconfigure the Routing Table.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
(entity) -HOST HAS STARTED POLLING	177012	Medium	Normal	This message indicates that the host has polled an interchange for the first time after that interchange was reset or the host timed out.		This is an information message only. No corrective action is required.
(IA) - IA ENTERING FAST POLL	177004	High	Normal	This message indicates that the interchange is responding to polls and has been moved from the slow poll list to the fast poll list. This results in the Interchange Address being polled more frequently. The value *(IA)* identifies the Interchange Address.		This is an information message only. No corrective action is required.
(IA) - IA ENTERING SLOW POLL	177005	High	Warning	This alarm indicates that the interchange is not responding to polls and has been moved to the slow poll list. The value *(IA)* identifies the Interchange Address.	177004	Check the connections to the affected interchange.
(IA) - RESET DISCARDED	177007	Low	Warning	This alarm indicates that ALC has received a RESET command for a specified Interchange Address (IA) and the IA is not configured to handle RESET commands. The value *(IA)* identifies the Interchange Address.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
(IA) - STOPPED POLLING IA	177006	High	Minor	This alarm indicates that the ALC PAD has stopped polling the interchange because the network has imposed Flow Control. The ALC PAD is configured to stop polling whenever it is unable to forward traffic to the network. The value *(IA)* identifies the Interchange Address		To correct this problem, increase the available network bandwidth.
(IA) - T1 TIMEOUT	177008	Medium	Warning	This alarm indicates that ALC Handler has sent a poll on a specified line and has failed to receive the start of a response within the configured T1 Timeout. The value *(IA)* identifies the Interchange Address.		Increase the configured value for the T1 Timeout parameter.
(IA) - T2 TIMEOUT	177009	Medium	Warning	This alarm indicates that ALC Handler has sent a poll on a specific line and has failed to receive a complete response within the configured T2 Timeout. The value *(IA)* identifies the Interchange Address.		To correct this problem: a) Increase the configured value for the T1 Timeout parameter. b) Increase the link speed.
(l) - DEDICATED LINK - NOT CONFIGURED	270006	High	Critical	This alarm indicates that the dedicated link *(l)*, referenced in a PPP profile record, has not been configured cannot be allocated for the PPP connection.		Ensure that the referenced dedicated link is configured and in operation, or remove it from the PPP profile record.
(n) GOOD ISAKMP PRESHARED KEYS FOUND IN CMEM	425021	Medium	Normal	Indicates number of valid Pre-Shared keys found.		This is an informative message.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
(n) BAD ISAKMP PRESHARED KEYS FOUND IN CMEM	425022	High	Major	Invalid ISAKMP Pre-Shared keys found in CMEM.		Ensure node keys are set properly.
RE-ESTABLISHED ISAKMP CONNECTION WITH ***aa.bb.cc.dd***	425024	Connect	Normal	ISAKMP connection has been successfully re-negotiated with the peer.		This is an information message only. There are no corrective actions necessary.
RE-ESTABLISHED IPSEC CONNECTION WITH ***aa.bb.cc.dd***	425025	Connect	Normal	IPSec connection has been successfully r-negotiated with the peer.		This is an information message only. There are no corrective actions necessary.
RECEIVED ENCR. NOTIFY MSG OR MALFORMED PACKET FROM ***aa.bb.cc.dd***	425026	High	Major	Encrypted ISAKMP notify messages are being received before the ISAKMP SA has been established. Possibly also receiving corrupted ISAKMP packets.		Ensure that IPSec configuration is valid on the node and on the peer also.
ISAKMP DETECTED DEAD PEER ***aa.bb.cc.dd***	425027	High	Major	Connection to the peer has been severed or the peer has gone down.		Ensure that the path to the peer is operational, and ensure the peer is operating normally.
(s) - CONNECTION UP	329010	High	Normal	This message indicates that the TCP connection between the TPA-TCP and the remote host is up. The value *(s)* indicates the slot affected.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
(s) CLEARING CALL, UNEXPECTED Q-BIT PACKET *(q)*	315002	High	Major	This alarm indicates that Q-bit data is not being accepted once a connection exists between a SDLC TPAD and a TPA-SDLC. The value *(s)* indicates the TPA-SDLC slot number affected, while *(q)* identifies the Q-Bit packet code.		This is an information message only. There are no corrective actions necessary.
(s) CONNECTION DOWN	315001	High	Major	This message indicates the connection between a TPA-SDLC and a SDLC TPAD does not exist. The value *(s)* indicates the TPA-SDLC slot number affected.	315000	To correct this problem: a) Check the routing table information. b) Check for the Autocall address in SDLC TPAD device configuration.
(s) CONNECTION UP	315000	High	Normal	This message indicates that an active connection exists between a TPA-SDLC and a SDLC TPAD. The value *(s)* indicates the TPA-SDLC slot number affected.		This is an information message only. There are no corrective actions necessary.
(s) INVALID CP PACKET *(header)*	315013	Low	Minor	This message indicates that an invalid PU frame has been recognized by the PU2/LU0 of TPA-SDLC. The value *(s)* identifies the TPA-SDLC slot number affected, while the value *(header)* shows the transmit or receive header from the PU2/LU0 frame.		This is an information message only. There are no corrective actions necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
(s) INVALID LU PACKET *(header)*	315014	Low	Minor	This message indicates that an invalid LU frame has been recognized by the PU2/LU0 of TPA-SDLC. The value *(s)* identifies the TPA-SDLC slot number affected, while the value *(header)* shows the transmit or receive header from the PU2/LU0 frame.		This is an information message only. There are no corrective actions necessary.
(s) OUT OF SEQUENCE PACKET, Event Code *(n)*	315015	Low	Warning	This message is displayed when the unexpected PU messages received after the PU session is up.The value *(s)* identifies the TPA-SDLC slot number affected and the value *(n)* shows the event code corresponds to the out of sequence PU message.		There is a problem with the terminal. Have this device checked.
(s) RECEIVED -VE RESPONSE,SENSE DATA- *(d)*	315007	Low	Normal	This report indicates that a '-ve' response has been received for the PU2/LU0 message. Possible causes for this message to be displayed include: • PU2/LU0 terminal does not understand out implementation. • Unacceptable value within the Pu2/LU0 message. The value *(s)* identifies the TPA-SDLC slot number, while *(d)* indicates the sense data that is detected.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
(s) RETRIES OVER FOR SENDING BIND	315016	Medium	Minor	This message is sent before a LU-LU session is activated. If a response is not received, the same BIND message will be retried for the configured retry times. If the number of retries is exhausted, the LU-LU session is cleared. The value *(s)* identifies the TPA-SDLC slot number affected.		The cause of this problem is likely that the terminal is not active.
(xx) TABLES BOOTED	425015	High	Normal	An IPSec Profile, ISAKMP Policy or IPSec Transform table has been booted. The value *(xx)* identifies a configured name or value.		This is an informative message.
(xxxx) AUTHENTICATION WAS REJECTED BY PEER	270015	Medium	Warning	This alarm indicates that this end is configured as a PAP and/or CHAP authentication server, and the peer has refused to authenticate itself. The authentication protocol(s) in question are given by *(xxxx)*.		Reconfigure this end or the remote equipment for compatible authentication.
ABNORMAL CALL TERMINATION - xxx PROTOCOL : xx STATES : xxxx EVENT : x	90000	Low	Major	This alarm indicates that an internal error has occurred.		Advise your customer service representative of the problem. There are no corrective actions you can perform when this alarm is displayed.
ABNORMAL NS COMMAND, CMD	379008	Medium		This alarm should never be displayed.		Contact your customer service representative if this alarm is displayed.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
ADDRESS ERROR *(h)*	42003	Medium	Warning	This alarm indicates that the address byte of the received frame is in error. The value *(h)* identifies the hexadecimal value of the received address.	42007	Check that the correct device is connected.
ADDRESS ERROR *(h)*	43003	Medium	Warning	This alarm indicates that the address byte of the received frame is in error. The value *(h)* identifies the hexadecimal value of the received address.	43007	Check that the correct device is connected.
ADDRESS ERROR *(h)*	195003	Medium	Warning	This alarm indicates that the address byte of the received frame is in error. The value *(h)* identifies the hexadecimal value of the received address.		Check that the correct device is connected.
ADDRESS ERROR *(hh)*	68005	Medium	Warning	This message indicates that the address byte of the received frame is in error. The hh is the hexadecimal value of the received address.		Check the frame address.
ALL PRIORITY QUEUES UNBLOCKED	46013	Medium	Normal	This message indicates that all queues, regardless of traffic priority level, are now unblocked.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ap2_ *(cause)*	236002	Low		This alarm indicates that a one of the following problems, identified by the value *(cause)*, has occurred: a) NULL; a Null function has been called for use as a place holder. b) No Buffs; This alarm indicates that AppleTalk cannot get a buffer from the buffer pool. c) Cannot n_send; The node cannot send an AppleTalk packet over a network interface. d) Cannot Append; The AppleTalk module could not append characters to a existing AppleTalk packet.		Perform the corrective action indicated for the appropriate cause: a) Contact your customer service representative if this alarm message is displayed. b) Increase memory allocated for buffers and boot the node. c) One of the AppleTalk interfaces could be down. Check to ensure that all AppleTalk interfaces are up. d) Contact your customer service representative if this alarm message is displayed.
ap2_net_change: Got netdown twice in a row	236003	Medium		This message indicates that the AppleTalk module has received a duplicate indication of the interface going down.		This is an information message only. No corrective action is required.
APPN_CM SYSERR *(counter)*	383000	Medium		This alarm indicates that an SNA protocol software Retry Counter error has occurred.		Record the report exactly as it appears on screen, and report it to Customer Service.
ATM-*3000* - AAL5 CPCS FRAME TRANSMIT ERROR		Medium		This alarm indicates that a packet could not get queued fro transmission *(port ID is ATM-3000)* because either the SAR driver was disabled, or the transmit queue was full.		This message prints out based on the node's configured "Threshold Alarm Timer". This keeps repetitive reports from flooding the system.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
AUTOCALL RETRIES EXHAUSTED	308041	High	Minor	This alarm indicates that the number of Autocall retries, to a remote PAD, has exceeded the configured value.	308000	Check the link, Mnemonic table and route selection table configuration.
BACKUP LINK ACTIVATED	43010	High	Major	This alarm indicates that the backup link is active and that all alternate links are down.	43007	Check that the alternate links are properly configured.
BACKUP NAME IN SWITCHED SERVICE ENTRY	242009	High	Critical	This message indicates that the backup port name of a SS entry has been changed and the tables booted.		Boot the node to correct this problem.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
bad adv/ovflo: (*ls_type, dest_addr, adv_source*)	386	Medium	Medium	This OSPF 51 alarm indicates that a received link state advertisement is badly formatted. This route is installed in the database, without parsing, and is marked as unusable for the purpose of route calculation. This alarm is displayed whenever the Link State Advertisement does not fall into one of these categories. • Router links advertisement. (Value 1) • Network links advertisement. (Value 2) • Summary link advertisement. (Value 3) • Summary to ASBR. (Value 4) • AS external link advertisement. (Value 5) • Group-membership-LSA. (Value 6) The value *ls_type* identifies the type of advertisement (by Value number), *dest_addr*: identifies the destination, and *adv_source*: indicates the source of advertisement.		If the Link State Advertisement Type is not listed in the alarm description, the neighboring router must be sending some Link State Advertisement Type that is not supported by a Vanguard router. Check the configuration of that router. If the Link State Advertisement Type is supported by a Vanguard router, there is insufficient memory for the internal OSPF routing table. Increase the memory size for the OSPF routing table.
BAD FRAME LENGTH *(b)*	42004	Medium	Minor	This alarm indicates that a frame was received with an incorrect length. The value *(b)* identifies the length of the received frame.	42007	Configure the attached device to send smaller frames.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
BAD FRAME LENGTH *(b)*	43004	Medium	Minor	This alarm indicates that a frame was received with an incorrect length. The value *(b)* identifies the length of the received frame.	43007	Configure the attached device to send smaller frames.
BAD FRAME LENGTH *(b)*	195004	Medium	Minor	This alarm indicates that a frame was received with an incorrect length. The value *(b)* identifies the length of the received frame.		Configure the attached device to send smaller frames.
BAD FRAME LENGTH *(bbbb)*	68009	Medium	Minor	This message indicates that a frame had an incorrect length; *(bbbb)* is the length of the received frame.		Configure the attached device to send smaller frames.
BAD FRAME TYPE *(h)*	42002	Low	Minor	This alarm indicates that a frame has been received with an unrecognizable receive control byte. The value *(h)* identifies the hexadecimal value of the byte.	42007	Check the link configuration, and verify that the Frame Sequence value is the same at both ends of the link.
BAD FRAME TYPE *(h)*	43002	Low	Minor	This alarm indicates that a frame has been received with an unrecognizable receive control byte. The value *(h)* identifies the hexadecimal value of the byte.	43007	Check the link configuration, and verify that the Frame Sequence value is the same at both ends of the link.
BAD FRAME TYPE *(h)*	195002	Low	Minor	This alarm indicates that a frame has been received with an unrecognizable receive control byte. The value *(h)* identifies the hexadecimal value of the control byte.		Check the link configuration, and verify that the Frame Sequence value is the same at both ends of the link.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
BAD FRAME TYPE *(hh)*	68003	Low	Minor	This message indicates that a frame has been received with an unrecognizable receive control byte. The value *(hh)* identifies the hexadecimal value of the byte.		Check link configuration, and that Frame Sequence is the same at both ends of the link.
BAD IPSEC PROFILE CMEM RECORD *(xx)*	425003	High	Major	The IPSec profile indicates an invalid Policy Number or an invalid Transform Set number. The value *(xx)* identifies a configured name or value.		Configure valid Transform or Policy numbers in the IPSec Profile.
BAD IPSEC TRANSFORM SET CMEM RECORD *(n)*	425004	High	Major	Invalid Transform record. The following Transform set record number has an incorrect configuration. Another possible reason for this alarm is the DIMM/ SIMM does not support the ESP encryption algorithm.		Ensure the IPSec Transform configuration is correct. Also, verify that the hardware supports the ESP algorithm specified in the transform record.
BAD ISAKMP PRESHARED KEY RECORD *(n)*	425005	High	Major	Invalid ISAKMP Pre-Shared key record. This alarm may be generated if the node key has changed.		Ensure that the ISAKMP preshared keys have been reconfigured correctly.
BAD ISAKMP POLICY CMEM RECORD *(n)*	425006	High	Major	Invalid Policy record. The following policy set record number has an incorrect configuration.		Ensure the IPSec Policy record configuration is correct.
BAD N(R) *(hh/hh)*	68008	Low	Minor	This message indicates that a frame has been received with a bad N(R). The first *hh* is the received N(R) and the second is the expected N(R).		Check the other end of the link to make sure it is the same port type. If the port types are the same, check the hardware and cables. Check K Level 2 Windows.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
BAD P(R)	46004	Low	Minor	This alarm indicates that a bad acknowledgment number has been received.	46000	Complete the following procedure to correct this alarm condition: a) Install a DataScope to monitor the line. b) Verify that your Vanguard device is operating correctly. c) Check the configuration to be sure the Packet Window sizes match at both ends.
BAD PACKET LENGTH *(bbbb)*	46008	Medium	Minor	This alarm indicates that a received is either too long or too short. The value *(bbbb)* indicates the length of the received packet.	46000	Check the link configuration. The P Packet window must be the same at both ends of the link.
BAD PACKET TYPE *(h)*	46009	Low	Minor	This alarm indicates that a packet with an invalid packet type (PTI) has been received. The value *(h)* is the received PTI.	46000	Check the link configuration. The packet sequence must be the same at both ends of the link.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
Bad Param in *(message)*	236000	High	Critical	This alarm is generated with many different messages, indicated by the value *(message)* and described below: a) AP2_connect - The interface number is not in the current range of interfaces b) ap2_net_change: Got netup twice in a row - Received a duplicate indication for network interface coming up. c) Could not bring down port - The specified port could not be brought down, and hence would be marked as failed. d) Could not complete bring up of port - The specified port could not come up, and is marked as failed. e) ap2_catch_timer - Appletalk encountered an incorrect timer number. f) GetSystemMemory got bad size - The system requested a memory size which is not supported.		Perform the corrective actions appropriate to the alarm message displayed. a) Change the interface number and reboot the node. b) This is an information message only. No corrective action is required. c) The node would have to be restarted for the port to be activated again. d) The node would have to restarted for the port to be activated again. e) This is an information message only. No corrective action is required. f) This situation should never arise. If this alarm is encountered restart the node.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
Bad Param in (*message)* (Cont'd)	236000	High	Critical	g) Restart the node. The interface number configured is out of range (more than 36). h) CMEM: No default zone for interface - A duplicate zone has been configured for the same interface i) ap2_Module_Init: init too many times j) CMEM: Duplicate interface - Duplicate entry for the same interface was encountered, the second instance is skipped. k) CMEM: Illegal Port Type for interface - AppleTalk cannot be run on the specified port. l) CMEM: AppleTalk not supported on Token Ring - AppleTalk not support on a token ring port.		g)Reconfigure the interface number to fit in the range of 1 to 36. h)Delete one of the duplicate zone configurations. i) Reboot the node to restart AppleTalk. j) Delete one of the duplicate interfaces. k)Reconfigure the interface number to an AppleTalk compatible port. l) This is an information message only. There are no corrective actions necessary.
BASE KEY CHANGED: *(base_key_name)*	379011	High		This indicates that a new Base Key has been entered or the existing Base Key changed. The value *(base_key_name)* identifies the current Base Key.		This report is a record of critical encryption action taking place in the node. If this activity has been performed by an authorized individual, no further action is required, otherwise, a security breach may have occurred. You should check physical security of the nodes and the configuration to identify and plug any security hole

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
BILLING RECORDS EXCEED LIMIT - BILLING RECORD LOST	32000	Medium	Critical	This message indicates that the a new Billing Record need to be attached to the queue which needs to be printed with the printer mnemonic, when the Call Establishment to this billing printer mnemonic has failed 60 times and the queue has already got elements which is equal to the Maximum Billing Record Threshold parameter in the Node Record.		To correct this problem: a) Check to see if the node is congested. b) Check the physical connections. c) Check the values in the mnemonic table, route selection table and the billing printer mnemonic. There may be an incorrect mnemonic or address configured.
BOOTED ENCRYPTION PROFILE: *(profile_name)*	379018	High		This message indicates that a specified Encryption Profile, identified by the *(profile_name),* has been booted on-line. In this case the profile will be effective for the next call.		This report is a record of critical encryption action taking place in the node. If this activity has been performed by an authorized individual, no further action is required, otherwise, a security breach may have occurred. You should check physical security of the nodes and the configuration to identify and plug any security hole

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
BOOTED ENCRYPTION KEY: *(base_key_name)*	379017	High		This message indicates that a specified Base Key, identified by the *(base_key_name),* has been booted on-line via CTP command. In this case the profile will be effective for the next call.		This report is a record of critical encryption action taking place in the node. If this activity has been performed by an authorized individual, no further action is required, otherwise, a security breach may have occurred. You should check physical security of the nodes and the configuration to identify and plug any security hole
bop_bri_sm_pck() ALLRIGHT+ CLOSED : RETURN	241026	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
bop_bri_state_machine : CS=%d, STIM=%d, RES=%d, NS=%d	241034	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
BR-%d BRIDGE ID MISMATCH	136001	High	Critical	The Bridge Identifier of this Bridge Link does not match the Bridge Identifier.		Check the configuration of the Bridge Link and the remote vanguard bridge link. Verify that the bridge Identifier of the Bridge Link matches the Bridge Identifier of the Remote Vanguard Bridge Link.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
BR-%d DUPLICATE RBR TRIPLET	136002	High	Critical	There are two sources of the Report with the Source Route Bridge Network. The first, the source Route Bridge Forwarder detected a duplicate Ring number in the Source Route Bridge Network. The second, the source Route Bridge Forwarder has two Bridge Links configured with the same bridge identifier where both bridge links provide a path that leads to the same ring.		Check the configuration of the ring numbers configured in the token ring port records within the Source Route Bridge network. Each ring number must be unique. Where both Bridge Links provide multiple paths that lead to the same ring, configure the Bridge Identifier in the Bridge Link configuration to be unique for each of the bridge links.
BR-%d INCOMPATIBLE LINK MODE	136003	High	Critical	The source Route Bridge Forwarder detected that the Bridge Link Configuration of the remote Vanguard has a Bridge Link Configuration with Link Mode not set to Normal.		Configure the Bridge Link Parameter and Link Mode of this Vanguard and the remote Vanguard to a consistent value.
BR-%d ONE TRANS LINK ALLowED PER NODE	136004	High	Critical	This report indicates that only one Bridge Link per Vanguard is allowed to have it's Link Mode Parameter set to TRANS.		Configure only one Bridge Link to have a Link Mode set to TRANS.
TR-%d PORT DUPLICATE TOKEN RING NUMBERS	136005	High	Warning	This report indicates that more than on Token Ring Port is configured with the Ring Number Parameter set to the same value. This is a serious problem if the Parameter in the Bridge Parameters Record called Local Bridge Identifier is not set to 0.		Configure the Token Ring Ports with a different Ring Number and attach them to different rings. or Change the Local Bridge Identifier in the Bridge Parameters Record to 0.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
BR-%d RING NUMBER MISMATCH LOCAL=%d REMOTE=%d	136000	High	Critical			Contact your customer service representative if this alarm is displayed.
BRI - LINK DOWN, CAUSE =DIAG	241014	High	Major	This alarm indicates that a BRI link (Layer 2) is down.		Evaluate the cause and diagnostic codes to determine why.
BRI - *PORT (p)* - BRI TX BUFFERS CONGESTED	241011	Low	Warning	This alarm indicates that the transmission buffers for a BRI port are congested. The value *PORT (p)* identifies the port affected.		Contact your customer service representative if this alarm message is displayed.
BRI - *PORT (p)* - CALL CONNECTED	241001	Medium	Normal	This message indicates that an ISDN call established to a BRI port. The value *PORT (p)* identifies the port number.		This is an information message only. No corrective action is required.
BRI - *PORT (p)* - CALL DISCONNECT FAILED. REASON CODE = *(n)*	241005	High	Critical	This alarm indicates that an attempt to disconnect the called failed. The value *PORT (p)* is the Reason Code for this error.		Evaluate the reason code to determine why the called failed.
BRI - *PORT (p)* - CALL SETUP FROM %s FAILED. REASON CODE	241004	High	Major	This alarm indicates that an ISDN call from the specified location could not be established. The value *PORT (p)* is the Reason Code for this error.		Evaluate the reason code to determine why the called failed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
BRI - *PORT (p)* - CALL SETUP FROM REJECTED. REASON CODE = *(n)*	241007	Medium	Major	This alarm indicates that a call request to this node was rejected. The value *PORT (p)* identifies the port number that failed while *(n)* gives the Reason Code for this error.		Evaluate the reason code to determine why the call was rejected.
BRI - *PORT (p)* - CALL SETUP TO DISCONNECTED BEFORE CON-NECTION COMPLETED. REASON CODE = *(n)*	241006	Medium	Major	This alarm indicates that during call establishment a 'disconnect' was received. The value *PORT (p)* identifies the port number that failed while *(n)* gives the Reason Code for this error.		Evaluate the reason code to determine why the 'disconnect' was generated.
BRI - *PORT (p)* - CALL SETUP TO FAILED. REASON CODE = *(n)*	241003	High	Major	This alarm indicates that an ISDN call to the specified location could not be established. The value *PORT (p)* is the Reason Code for this error.		Evaluate the reason code to determine why the called failed
BRI - *PORT (p)* - INITIALIZATION INCOMPLETE. REASON CODE = *(n)*	241008	High	Critical	This alarm indicates that a BRI port failed to initialize. The value *PORT (p)* identifies the port number that failed while *(n)* gives the Reason Code for this error.		Evaluate the reason code to determine why the port failed initialization. If the Reason Code *(n)* is: e01 = A different SPID was already assigned e02 = Physical link failure e03 = Network problems e04 = Network refused the SPID identification

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
BRI CARD FAILURE	241013	High	Critical	This message indicates that an internal error has caused the BRI card to fail.		Evaluate the reason code to determine the type of failure.
BRI INT. %d %s CONNECTED TO %s	278008	Conn	Normal	ISDN call connected.		This is an information message only. There are no corrective actions necessary.
BRI INTERNAL ERROR	241015	High	Critical	This alarm indicates an internal error has occurred on the BRI driver.		Contact your customer service representative if this alarm message is displayed.
BRI- *PORT (p)* - CALL DISCONNECTED REASON CODE = *(n)*	241002	Medium	Normal	This alarm indicates that an ISDN call was unexpected disconnected. The value *PORT (p)* is the Reason Code for this error.		If the call was disconnected abnormally evaluate the reason code to determine why.
BRIDGE INITIALIZATION FAILURE *(xx)*	134000	High	Critical	This message indicates that the LAN forwarder initialization has failed during node restart. The value *(xx)* identifies the ASCII description of the failure.	134001	This is an information message only. There are no corrective actions necessary.
BRIDGE IS NOT THE ROOT	137002	Low	Normal	While running the spanning tree protocol, the Vanguard is not the root of the spanning tree.		The node is receiving BPDUs (Bridge Protocol Data Unit). Not being the root of the spanning tree is a normal function.
BRIDGE IS THE ROOT	137001	Low	Normal	While running the spanning tree protocol, the Vanguard has become the root of the spanning tree.		The node is the only node in the network or it is not receiving BPDUs (Bridge Protocol Data Unit). It is the node that is sending BPDUs. Being the root of the spanning tree is a normal function.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
BRIDGE LINK BOOT COMPLETE	134001	High	Normal	This message indicates that a bridge link has been restarted.		This is an information message only. There are no corrective actions necessary.
BRIDGE LINK BOOT FAILURE *(xx)*	134002	High	Warning	This alarm indicates that a bridge link can not be booted. The value *(xx)* identifies the ASCII description of the failure.	134001	This is an information message only. There are no corrective actions necessary.
BRIDGE LINK DISABLE COMPLETE	134004	High	Warning	This message indicates that a bridge link has been successfully disabled.	134003	This is an information message only. There are no corrective actions necessary.
BRIDGE LINK ENABLE COMPLETE	134003	High	Normal	This message indicates that a bridge link has been successfully enabled.		This is an information message only. There are no corrective actions necessary.
BRIDGE PARAMETERS BOOT FAILURE %s	134006	High	Normal	This alarm indicates that a request was made to update a bridge link configuration, and that request was not successfully completed.		To correct this problem: • Review the changes that have been made to the parameters. • Check to ensure that they are all within the parameter range and entered properly.
BRIDGE PARAMETERS BOOT COMPLETE	134005	High	Normal	This message indicates that a bridge link configuration has successfully updated. Parameters that do not require a node boot to take affect, have been changed.		This is an information message only. There are no corrective actions necessary.
BYTES COPIED TO FLASH MEMORY	105001	High	Warning	This message indicates that the specified number of bytes has been copied to FLASH memory.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Called bop_bri_sm_shutdown() from bop_bri_sm_pck() rnt_cod = 0x%x	241043	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
Called state machine in the disabled state	241045	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
CAN'T GET FACILITY FOR DCP	91001	Low	Minor	This alarm indicates that an internal error has occurred.		Advise your customer service representative of the problem. There are no corrective actions you can perform when this alarm is displayed.
CANNOT READ FROM NSO DISK, SLOT %d	65001	High	Normal			Contact your customer service representative if this alarm is displayed.
Channel %d state variable is at location 0x%x	241061	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
CHECKSUM ERROR	308022	Low	Warning	This alarm indicates that a Checksum error has occurred and a frame has been discarded.	308000	Correct the software in the remote node OR packet was corrupted on the network.
CLI Error	303000	High	Normal	This alarm indicates that either a CLI initialization or memory allocation error has occurred.		Contact Technical Support if this alarm is displayed.
CMEM SIMM REINITIALIZED	106000	High	Critical			Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
COMPRESSION NEGOTIATION FAILED	270004	Medium	Warning	This alarm indicates that the Compression Control Protocol was unable to converge upon a mutually acceptable data compression protocol with the peer.		Adjust the configurations of the local and/or remote equipment so that they accept a common data compression protocol, or disable data compression.
Configuration error - *(err_msg)*	403001	High	Critical	This message indicates that, after booting, there is an invalid configuration. The value *(err_msg)* indicates the exact error message.		Change or delete the entry with bad configuration.
CONNECTED TO *(destination)*	16000	CONN	Normal	This message is generated when a call is connected to its destination; identified by the value *(destination)*.		This is an information message only. No corrective action is required.
COPY COMPLETE	105002	High	Normal	This message indicates that the FLASH-to-FLASH copy is complete.		This is an information message only. No corrective action is required.
COPYING SOFTWARE TO FLASH MEMORY	105000	High	Critical	This message indicates that software is being loaded into FLASH memory.	105002, 105005, 105014	This is an information message only. No corrective action is required.
COPYING SOFTWARE FROM LOCAL FLASH TO FLASH	105013	High	Warning	This message indicates that a local FLASH copy has started.		This is an information message only. No corrective action is required.
Could not bring up interface	236010	Medium		This alarm indicates that the specified port could not come up, and is marked as failed.		The node would have to be restarted for the interface to be activated again.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
CPU UTILIZATION > THRESHOLD ON CARD *(c)*	17002	Medium	Warning	This alarm indicates that CPU utilization is above the specified threshold limit. The value *(c)* identifies the card number.		To correct this problem: a) Remove or reduce the number of active ports. b) Reduce the port speed. c) Delete any unnecessary processes.
CTP - at wrong task, TCB =	5000	High	Warning	This message is displayed only when the DEBUG function is turned on. It indicates that other tasks are busy and the CTP task was not running at that particular moment; the current CTP operation has been terminated.		Contact your customer service representative if this alarm is displayed.
CTP HELP MESSAGE ARRAY OVERFLOW	5001	High	Warning	This message is displayed only when the DEBUG function is turned on. It indicates that the length of help messages exceed the maximum character length.		This is an information message only. No corrective action is required.
CVS - %s	373007	High		This message indicates that the Centralize Voice Switching Table did not complete. The reason for this failure will be identified in the message.		Identify the cause of the failure from the alarm message and correct as required.
CVS - Centralized Voice Switching disabled	373005	High		This message indicates that the CVS operation has been disabled by the operator.		This is an information message only. There are no corrective actions necessary.
CVS - Centralized Voice Switching enabled	373006	High		This message indicates that the CVS operation has been enabled by the operator.		This is an information message only. There are no corrective actions necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
CVS - CVS Table Copy Complete	373008	High		This message indicates that the Centralize Voice Switching Table copy was successfully completed without error.		This is an information message only. There are no corrective actions necessary.
CVS - Invalid Execution, Line No. %d	373004	Low		This message indicates a situation where an unexpected operation occurred in the CVS state machine.		If this problem persists, contact your customer service representative for assistance.
CVS - No digit value matching *(value)* found, calling address: *(add)*	373002	Low		This message indicates that the software can not find a match to the received digit value from the calling voice port. The value *(value)* identifies the received data value while *(add)* identifies the calling address.		There are no corrective actions required if the wrong number has been dialed. However, if the number is correct, update the Voice Switching Table with an entry that matches the number dialed.
DATA LOST FROM OUTBOUND *(xxxx)* QUEUE	270005	High	Major	This alarm indicates that data bound for transmission on the PPP link has instead been discarded by the network protocol *(xxxx)*.		Check connections and cables, and the status of the remote equipment.
DC SIMM, MOTHERBOARD & T1E1 INCOMPATIBLE - DATA COMPRESSION DISABLED		High		This alarm indicates that a revision M or lower motherboard along with a DC simm and a 2Mbit T1E1 card is incompatible.		Upgrade the motherboard when using a DC SIMM and a data/ voice card.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DCCM-%d: DC Communication Lost		High		This message indicates that DCCM has determined that the DC has become un responsive. DC assumed non-functioning and will be reset. %d = DCCM port number		This is an information message only. No corrective action is required.
DCCM-%d: Board Recovery Timeout (Ready Check)		High		This message indicates the DC was reset but did not return to a 'Ready' state. DC will be reset again. %d = DCCM port number		This is an information message only. No corrective action is required.
DCCM-%d: Board Timeout (Reset Check)		High		This message indicates an unexpected DC reset was detected by node, board recovery is initiated. %d = DCCM port number		This is an information message only. No corrective action is required.
DCCM-%d: Board Recovery Complete		High		This message indicates board recovery successful. %d = DCCM port number		This is an information message only. No corrective action is required.
DEDICATED LINK *(l)* ALREADY ALLOCATED	270007	High	Critical	The dedicated link *(l)*, referenced in a PPP profile record, is already associated with another PPP connection.		The dedicated link is referenced in more than one PPP profile. Remove it from all but one PPP profile.
DELETED ALL ENCRYPTION KEYS	379019	High		This message indicates that all encryption Base Keys, and the Node Key, in the node have been deleted via CTP command.		To correct this alarm, you must re-enter Base Keys and Node Key. **■Note** Refer to the *Data Encryption Feature Protocol Manual* (Part Number T0103-09) for additional configuration information.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DESTINATION NAME IN SWITCHED SERVICE ENTRY	242007	High	Critical	This message indicates that the destination name of a SS entry has been changed and tables have been booted.		Boot the node to correct this problem.
DEVICE BOOT COMPLETE	57016	High		This message indicates that the Device Record was successfully booted.		This is an information message only. No corrective action is required.
DEVICE BOOT FAILURE	57017	High		This message indicates that the Device Record boot failed.		Save the device record.
DEVICE NOT RESPONDING	308032	Medium	Major	This alarm indicates that a device is not responding to POLLs.	308000	Check the device.
DEVICE_STATUS %d	116001	High	Normal			Contact your customer service representative if this alarm is displayed.
DIAL IN NOT ALLOWED	6019	Medium	Warning	This message indicates that a Dial In condition was detected on a port not configured for this condition.		If Dial In is desired, ensure that the configuration allows it, otherwise, ignore this message.
DIAL OUT NOT ALLOWED	6020	High	Warning	This message indicates that a Dial Out condition was detected on a port not configured for this condition.		If Dial Out is desired, ensure that the configuration allows it, otherwise, ignore this message.
DISABLED state detected in bop_bri_rx_isr()	241060	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
DISC RECEIVED	42001	High	Major	This alarm indicates that a DISC Frame has been received and the link has been disconnected.	42007	Wait for the link to come back up and try to call again.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DISC RECEIVED	43001	High	Major	This alarm indicates that a DISC Frame has been received and the link has been disconnected.	43007	Wait for the link to come back up and try to call again.
DISC RECEIVED	195001	High	Major	This alarm indicates that a DISC Frame has been received and the link has been disconnected.		Wait for the link to come back up and try to call again.
DISCARDING *(n)* FRAMES	270008	Low	Minor	This alarm indicates that *(n)* Multilink frames have been discarded due to a missing segment.		This alarm, if generated infrequently, is normal (due to occasional bit errors) and no corrective action is required. If it occurs frequently, check for an excessive bit error rate on the link*(s)*.
DISCONNECTED FROM *(destination)*	16001	CONN	Normal	This message is generated when a call is cleared. The value *(destination)* indicates the destination to which the call was made. This message is not an indication of sub-system problems.		Check to see if the Call Clear was expected. If it was not expected, you should investigate possible causes, such as the link has gone down.
DLSV Loader: ATTEMPTING TO DOWNLOAD	33000	High	Warning	This message indicates that the download server is attempting a download.	33005 33008	This is an information message only. No corrective action is required.
DLSV Loader: CANNOT WRITE FLASH	33014	High	Critical	This alarm indicates that a defective FLASH SIMM needs replacement.	33005, 33008	To correct this problem, replace the FLASH SIMM. **■Note** SIMM installation instructions can be found in your products Installation Manual or the Vanguard Daughtercard Installation Manual.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DLSV Loader: CANNOT ERASE FLASH	33012	High	Critical	This alarm indicates that the FLASH SIMM is defective and needs replacement.	33008	To correct this problem: a) Replace the FLASH SIMM. b) SIMM installation instructions can be found in your products Installation Manual or the Vanguard Daughtercard Installation Manual.
DLSV Loader: COPYING SW TO FLASH	33021	High	Warning	This message indicates that a node has started transferring the image.	33005, 33008	This is an information message only. No corrective action is required.
DLSV Loader: DOWNLOAD COMPLETE	33005	High	Normal	This alarm indicates that the Download Server has completed a download.		This is an information message only. No corrective action is required.
DLSV Loader: FAILED TO COPY SOFTWARE	33016	High	Critical	This alarm indicates that Software was not copied correctly.	33005, 33008	Two activities should be performed to correct this problem: a) Check if connections are up. b) Check if load server has software.
DLSV Loader: FLASH HAS BEEN CORRUPTED	33023	High		This alarm indicates that, after a transfer was completed, the FLASH checksum test result was incorrect.		These activities should be performed to correct this problem: a) Ensure there were no network problems or errors during the transfer. b) A possible hardware problem may exist. Contact your customer service representative.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DLSV Loader: INCOMPATIBLE IMAGE LOAD ADDRESS	33011	High	Critical	This message, generated by the loader, is displayed if the called server is not a Vanguard node. Loading from 2.1x nodes is prohibited.	33005	This is an information message only. No corrective action is required.
DLSV Loader: MNEMONIC NOT CONFIGURED	33022	High	Critical	This alarm indicates that the Mnemonic is not configured.	33005, 33008	Configure a mnemonic in network services.
DLSV Loader: NO CONFIGURED SERVER	33013	High	Critical		33005, 33008	Contact your customer service representative if this alarm is displayed.
DLSV Loader: RECEIVED AN INVALID RECORD TYPE	33001	High	Critical	This alarm indicates that the Download Server has received an invalid record type.	33005 33008	Contact your customer service representative if this alarm is displayed.
DLSV Loader: RECEIVED NO RECORDS	33002	High	Critical	This alarm indicates that the Download Server has not received any records.	33005 33008	To correct this problem: a) Check the software options configured in you device and verify that they are correct. b) Reset the node and download software again. **■ Note** If this alarm is displayed repeatedly, contact your customer service representative.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DLSV Loader: RECEIVED RECORD WITH BAD CHECKSUM	33004	High	Critical	This alarm indicates that the Download Server received a record with a bad checksum.	33005 33008	Download the software again, if it fails, contact your customer service representative. **Note** Do not cold boot or power cycle the node.
DLSV Loader: RECEIVED RECORD WITH BAD LENGTH	33003	High	Critical	This alarm indicates that the Download Server received a record with a bad length.	33005 33008	Download the software again, if it fails, contact your customer service representative. **Note** Do not cold boot or power cycle the node.
DLSV Loader: SW DOWNLOAD ALREADY IN PROGRESS	33018	High	Warning	This alarm indicates that a download was requested while one was already in progress.	33005, 33008	Wait until the first download is complete before starting the second one.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DLSV Server: *(cause)*	33010	High	Critical	This message indicates that the Download Server received a load request from a node with a different CPU type. The value *(cause)* will identify: a) INCOMPATIBLE CPU TYPE - This alarm indicates that a RAM-to-RAM transfer was started between a CPU and CPU+ b) INCOMPATIBLE PRODUCT TYPE - This indicates that a FLASH-to-FLASH transfer was started between different nodes, i.e., a transfer between a Vanguard 6520 and a Vanguard 6560.		Depending on the displayed (cause) of this problem, perform one of these activities: a) No corrective action is required when an incompatible CPU type message is displayed; the server will clear the call. b) If the alarm is the result of incompatible products, ensure that the FLASH-to-FLASH transfer is being performed between the same type of nodes.
DLSV Server: CANNOT READ FLASH	33015	High	Critical	This alarm indicates that a defective FLASH SIMM needs replacement.	33005, 33008	To correct this problem, replace the FLASH SIMM. **■ Note** SIMM installation instructions can be found in your products Installation Manual or the Vanguard Daughtercard Installation Manual.
DLSV Server: CONNECTION IDLE TOO LONG	33006	High	Critical	This alarm indicates that the Download Server connection was idle too long.	33005 33008	Reset the node and download software again. If this alarm is repeated, try again later.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DLSV Server: DOWNLOAD COMPLETE TO	33008	High	Normal	This alarm indicates that the Download Server has completed sending data to the calling address.		This is an information message only. No corrective action is required.
DLSV Server: F2F FLASH BANK UNAVAILABLE	33019	High	Critical	This alarm indicates that a Loader, from another node, has tried to load from a nonexistent bank.	33005, 33008	Check the download status.
DLSV Server: FAILED TO SEND SOFTWARE	33017	High	Critical	This alarm indicates that a node could not send the software.	33005, 33008	Two activities should be performed to correct this problem: a) Check if the network connection is up. b) Check the parameters used to initiate the software transfer.
DLSV Server: LOADING TO ADDRESS	33009	High	Warning	This message indicates that the Download Server is in the process of loading to the specified address.	33005, 33008	This is an information message only. No corrective action is required.
DLSV Server: REQUEST WITH INVALID ADDRESS	33007	High	Critical	This alarm indicates that the Download Server detected a request with an invalid address.	33005, 33008	Verify that the configured download address is correct.
DLSV Server: SW DOWNLOAD ALREADY IN PROGRESS	33020	High	Normal	This alarm indicates that a node has attempted to load from this server node while 5 other loads were in progress. Note that up to 5 nodes can be served at any one time.		Wait until one of the downloads is complete, then try again.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DORM - *(address)* DORA FAILURE - REMOVED FROM DORM TABLE	253004	Medium	Minor	This report indicates that the address specified is no longer a valid Dial Out Agent address. The value *(address)* identifies that X.25 address.		There are no corrective actions necessary. This happens if some configuration was changed in the network such that the specified address is no longer valid. This can be verified with the network operator.
DORM - DIAL-OUT REQ *(E.164)* ABANDONED - DOR FAILURE	253003	Low	Minor	This alarm indicates that the dial out request for the specified E.164 address (the value *E.164*) could not be forwarded to any of the Dial Out Agents.		Usually , since this could be a temporary problem (e.g. all agents are busy), there are no corrective actions necessary. **■Note** Contact your customer service representative if this occurs frequently.
DORM - DORM COMMUNICATION ESTABLISHED	253002	Low	Normal	This report indicates that the connection between the two DORMs in the network has been established.		Usually, since this could be a temporary problem such as all agents are busy, there are no corrective actions required. **■Note** Contact your customer service representative if this alarm occurs frequently.
DORM - DORM LINK FAILURE	253001	Medium	Major	This report indicates that the connection to the Other DORM is down because of network problems.	253002	This is an information message only. There are no corrective actions necessary.
DORM - TABLE OVERFLOW	253005	Medium	Major	This report indicates that registration information has been received for an X.32 port when all the table entries are occupied.		Increase the “Number of X.32 Ports” parameter in the Node Record.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DORM CONFIGURATION - *(add)*	253000	Medium	Critical	This report indicates that the "Other DORM Address" configured in incorrect or unreachable. The value *(add)* identifies the bad DORM address.		Correct the Other DORM Address configured in the Node Record.
DSPM CRASH REASON - %s PC=%x ADD=%x	281009	High	Normal	This report indicates that a DSPM card has failed a background diagnostic test. This report provides the information needed to investigate the cause of the failure.		Record the information reported for this alarm and contact Customer Service if the problem persists.
DSPM FIRST RECOVERY SUCCESSFUL	281010	High	Normal	This report indicates that a DSPM card was successfully downloaded, after a background diagnostic failure. **■Note** This report only appears if this is the first background diagnostic failure to have occurred during the previous hour of operation.		This is an information message only. No corrective action is required.
DSPM SECOND RECOVERY SUCCESSFUL	281011	High	Normal	This report indicates that a DSPM card was successfully downloaded, after a background diagnostic failure. **■Note** This report only appears if this is the first background diagnostic failure to have occurred during the previous hour of operation.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
DSPM SOFTWARE DOWNLOAD COMPLETED	281004	Low	Normal	This message indicates that the DSPM card software was successfully download.		This is an information message only. No corrective action is required.
DSPM SOFTWARE DOWNLOAD FAILED	281005	High	Critical	This message indicates that the DSPM card software download failed.		Re-insert the DSPM card in question and power up the node again. If the problem persists replace the card.
DUPLICATE FIX TEI %d DETECTED FOR PKT D ON BRI INTERFACE %d	278015	High	Critical			Contact your customer service representative if this alarm is displayed.
Duplicate static path to *(net)* - in entry *(p)*	202000	High	Critical	This alarm indicates that the IPX Static (RIP/SAP) Table has a duplicate entry for the provided network (*(net)* value) at the mentioned position *(p)* value.		Delete one of the duplicate entries.
DVMRP.1 dvmrp_init called with NULL rfcm Context Block\r\n,	328001	High	Normal	This message should never be displayed.		Contact your customer service representative if this message appears.
DVMRP.10 Too many routing types from remote end, lcon %d	328010	DEBUG	Low	This debug message indicates the route overflow condition.		This is an information message only. There are no corrective actions necessary.
DVMRP.11 Unknown Net %s indication on interface %d	328011	DEBUG	Low	This debug message indicates that multiple net is down and netup indicated by this debug alarm.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DVMRP.12 Unknown LCON %s indication with number %d	328012	DEBUG	Low	This DEBUG alarm indicates multiple lcon down and lcon up.		This is an information message only. There are no corrective actions necessary.
DVMRP.13 %s	328013	DEBUG	Low	All debug information, as indicated below, is identified in this message: • Like Packet truncation, • Prune for unknown group • Graft for unknown group • Route report received • Prune received • Unexpected packet • Fwdinf the Packet • Route not Found.		This is an information message only. There are no corrective actions necessary.
DVMRP.3 Memory allocation for failed	328003	DEBUG	Low	This debug information is generated when a DVMRP attempts to copy all CMEM parameters to DRAM, and there is insufficient DRAM available.		To correct this problem, add additional DRAM to the router to ensure that DVMRP has enough memory to initialize itself.
DVMRP.4 DVMRP is not active in	328004	DEBUG	Low	This is an information message indicating that a DVMRP packet has arrived with DVMRP globally disabled.		There are no corrective actions required if the DVMRP packets do not have to be processed. However, if those packets have to be received and processed, you must enable DVMRP in the router.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
DVMRP.5 %s called with a NULL DVMRPCB	328005	DEBUG	Low	This debug alarm indicates that a particular function has been called but DVMRP control block is not allocated. This happens when DVMRP module is not up and Router tries to forward a multicast packet.		Configure DVMRP and check to ensure that the router has enough memory for DVMRP to initialize
DVMRP.6 DVMRP not up in lcon %d - dropping the packet	328006	DEBUG	Low	This debug information is generated when a DVMRP packet arrives on a particular interface that has the DVMRP disabled.		This alarm can be ignored if DVMRP packets are not to be received on the LCON ignore the report. If these packets are to be received on that interface/LCON enable the appropriate DVMRP.
DVMRP.7 Bad format packet received, lcon %d	328007	DEBUG	Low	This message indicates that a DVMRP packet has been received and it is in a non-standard format.		This is an information message only. There are no corrective actions necessary.
DVMRP.8 getbuf failed in %s	328008	DEBUG	Low	This message indicates the memory allocation debug report indicating that there is insufficient memory in the router.		Add more memory to the router, so that it has enough buffers available
DVMRP.9 Unsupported packet type with code %d on circuit %d	328009	DEBUG	Low	This message indicates that the DVMRP has received packets other than prunes, grafts, probes, route reports and graft ack.		This is an information message only. There are no corrective actions necessary.
E1-<%d> - <%s> - %s	283006	High	Normal			Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
EIA HANDSHAKE COMPLETE	6002	Medium	Normal	This message acknowledges the correction, by manual or automatic means, to the EIA HANDSHAKE INCOMPLETE condition.		This is an information message only. No corrective action is required.
EIA HANDSHAKE INCOMPLETE	6001	Medium	Minor	This alarm indicates that a handshake time-out occurred during EIA handshaking.	6002	Ensure that the attached device's EIA configuration matches that of the port.
ENCRYPTION MIS-CONFIGURED, %s IS A NETWORK PROTOCOL	379015	High		This message indicates that encryption is configured between two access ports.		To correct this, reconfigure encryption between an access and network port.
END of bop_bri_boardParams	241047	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
END of bop_bri_boardRestart	241046	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
END of bop_bri_Call Connected() : RETURN	241019	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
END of bop_bri_cd_ost_req uest() : RETURN	241024	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
END of bop_bri_eia_reject() : RETURN	241016	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
END of bop_bri_sig_response() : RETURN	241025	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
END of bop_bri_sm_pck() : RETURN	241028	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
END of bop_bri_sm_restart() : RETURN	241023	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
END of bop_bri_sm_shutdown() : RETURN	241022	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
END of bop_bri_trans_response () : RETURN	241037	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
END of bop_bri_tx_callsetup () : RETURN	241017	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
END of bop_bri_tx_disconn_msg() : RETURN	241021	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
END of bop_bri_tx_E_EiaShutdown() : RETURN	241020	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
END of bop_bri_validate_call () : RETURN	241018	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
END of bop_bri_x25_response() : RETURN	241035	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
END of sdrvc_traitetbenrep()	241039	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
Enet %d - Excessive RX Error Condition Set	174009	Medium	Warning	This alarm indicates that the Ethernet Driver is experiencing a high rate of Receive Errors.	174102	Complete this procedure to correct this alarm: a) Check, via the Ethernet Port Statistics, what errors the port is receiving. b) Check the Ethernet for a bad connection or excessive traffic.
Enet - 82596 Hardware Failure *(cause)*	174017	Medium	Critical	This alarm indicates that the Ethernet Driver encountered a failure when programming the ELAN Card. The value *(cause)* identifies the cause of this alarm.		To correct this problem, replace the ELAN Card.
Enet - Adding to the Transmit queue failed	174006	Medium	Critical	This alarm indicates that the Ethernet Driver was unable to place a transmit frame on the Ethernet transmit queue, because the transmit queue is filled.		Complete this procedure to correct this alarm: a) Confirm, via Ethernet Port Statistics, that the port is transmitting and that the port has not lost its carrier. b) Check the Ethernet connection for a bad clock or bad connection.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Enet - Excessive RX Error Condition CLR	174012	Medium	Normal	This message indicates that the Ethernet Driver is no longer experiencing a high rate of Receive Errors.		This is an information message only. No corrective action is required.
Enet - Excessive TX Error Condition CLR	174010	Medium	Normal	This message indicates that the Ethernet Driver is no longer experiencing a high rate of Transmit Errors.		This is an information message only. No corrective action is required.
Enet - Excessive TX Error Condition Set	174007	Medium	Warning	This alarm indicates that the Ethernet Driver is experiencing a high rate of transmit errors.	174010	Complete this procedure to correct this alarm: a) Check, via the Ethernet Port Statistics, what errors the port is receiving. b) Check the Ethernet connection and Ethernet for a bad connection or excessive traffic.
Enet - Loss of Carrier Condition Set	174008	Medium	Major	This alarm indicates that the Ethernet Driver is not able to detect a valid transmit clock.	174011	Check the Ethernet connection and Ethernet for a bad connection.
Enet - Loss of Carrier Condition CLR	174011	Medium	Normal	This message indicates that the Ethernet Driver is able to detect a valid transmit clock.		This is an information message only. No corrective action is required.
Enet - RX List Error *(f)*	174018	Medium	Minor	This message indicates that the Ethernet Driver encountered an error when receiving an Ethernet Packet. The Ethernet Driver will recover automatically from this error. The value *(f)* is the failure code.		This is an information message only. No corrective action is required.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
Enet - The 82596 failed to suspend operation	174005	Medium	Critical	This alarm indicates that the Ethernet Driver encountered a failure when programming the ELAN Card to suspend an operation.		To correct this problem, replace the ELAN Card. Refer to the Vanguard 6520/6560 *Installation Guide* (Part Number T0126) for additional information.
Enet - The Configuration command timed out	174004	Medium	Critical	This alarm indicates that the Ethernet Driver encountered a timeout when programming the ELAN Card.		To correct this problem, replace the ELAN Card. Refer to Vanguard 6520/6560 *Installation Guide* (Part Number T0126) for additional information.
Enet - The Configuration command failed	174002	Medium	Critical	This alarm indicates that the Ethernet Driver encountered a failure when programming the ELAN card.		To correct this problem, replace the ELAN Card. Refer to the Vanguard 6520/6560 *Installation Guide* (Part Number T0126) for additional information.
Enet - The Individual address command failed	174003	Medium	Critical	This alarm indicates that the Ethernet Driver encountered a failure when programming the ELAN Card MAC Address.		To correct this problem, replace the ELAN Card. Refer to the Vanguard 6520/6560 *Installation Guide* (Part Number T0126) for additional information.
Enet - TX List Error *(f)*	174019	Medium	Minor	This alarm indicates that the Ethernet Driver encountered a software error when transmitting an Ethernet Packet. The value *(f)* is the failure code.		Contact your customer service representative if this alarm is displayed.
Enet%d - Invalid driver state, should be disabled, function not performed.	174014	Medium	Critical			Contact your customer service representative if this trap is displayed.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
Enet%d - Invalid driver state, should be enabled, function not performed.	174013	Medium	Normal			Contact your customer service representative if this trap is displayed.
Enet%d - The loopback Configuration command failed.	174015	Medium	Warning			Contact your customer service representative if this trap is displayed.
Enet%d - The Time Domain Reflectometry command failed.	174016	Medium	Warning			Contact your customer service representative if this trap is displayed.
Enet- Bus Throttle Timers wouldn't load.	174000	Medium	Major	This alarm indicates that the Ethernet Driver bus timer was unable to be started.		To correct this problem, replace the ELAN Card. Refer to the Vanguard 6520/6560 Installation Guide for additional information.
Enet13 - Diag Check *(cause)*	174020	Medium	Critical	This message indicates that the Ethernet Driver encountered an error condition in the Hardware Accelerator module. The Ethernet Driver will recover automatically from this error. The value *(cause)* identifies the reason for this alarm.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
FAILED TO NEGOTIATE ISAKMP PROPOSAL WITH *(aa.bb.cc.dd) (yy**)*	425007	High	Major	Cannot establish ISAKMP with remote IPSEC peer because the proposals were rejected by the remote peer. Reason yy for failed negotiation is displayed in the alarm. *(yy**)* Reason String in Failed to negotiate parameters in ISAKMP or IPSEC Report: 1) Mal-formed packet 2) Invalid payload 3) Invalid packet length 4) Invalid DOI 5) Invalid SPI 6) Invalid Protocol ID 7) No proposal chosen 8) No supported attribute 9) Authentication failed 10) Bad packet syntax 11) Invalid Key information 12) Invalid Hash *(aa.bb.cc.dd)* refers to an IP address *(yy**)* refers to possible reason strings. **■Note** For pre-shared key configurations ensure that pre-shared keys are the same on both nodes.		Based on reason, make corrective changes to IPSec Configuration and ensure that the remote peer's IPSec configuration is valid. Reason String in Failed to negotiate parameters in ISAKMP or IPSEC Report Meanings: 1) Packet is Mal-formed, it fails the consistency check. This normally occurs when the remote peer does not have the correct pre-shared key configured. 2) The payload presented in the ISAKMP packet is not supported. 3) The packet length of the ISAKMP packet is of unexpected length. 4) The “Domain of Interpretation” field of the security Association payload is invalid. It must be IKE. 5) The security parameter index found in the packet is not valid. 6) The ISAKMP message has an unknown Protocol ID. 7) None of the proposals received from the remote peer are acceptable. Check your configuration.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
FAILED TO NEGOTIATE ISAKMP PROPOSAL WITH (*aa.bb.cc.dd) (yy**)* *(Continued)*	425007					8) The proposal contains an unknown or unsupported attribute. 9) Failure to authenticate the remote peer. The pre-shared keys of both nodes are not the same. 10) The ISAKMP packet format is not correct. 11) The Diffie-Hellman public values sent by the remote node has the wrong size. 12) The hash in the incoming ISAKMP message does not match the expected values. 13) For RSA signature configurations, verify certificate configurations.
FAILED TO NEGOTIATE IPSEC PROPOSAL WITH (*aa.bb.cc.dd) (yy**)*	425009	High	Major	Fails to negotiate a set of acceptable IPSEC parameters with the remote node. Check the IPSEC profile on both node to ensure at least one common set of profile exist between the nodes. (*aa.bb.cc.dd)* refers to an IP address (*yy**)* refers to possible reason strings, see Trap No. 425007.		Check the IPSec Profile on both nodes to ensure at least one common set of profiles exist between the nodes.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
CERTIFICATE FOR IPSEC PROFILE xx DOES NOT EXIST	4250028	High	Major	The node does not contain a CA certificate and the corresponding ID certificate needed fo IPSEC authentication. This alarm is only displayed when one of the policies within the IPSEC profile uses RSA signatures and not certificates are present.		Ensure that there is a CA certificate and an ID certificate are present in the node.
MSG_TX_LIST_PUT_FAILED	413006	Medium	Critical	This alarm indicates that the Ethernet Driver was unable to place a transmit frame on the Ethernet transmit queue, because the transmit queue is filled.		Complete this procedure to correct this alarm: a) Confirm, via Ethernet Port Statistics, that the port is transmitting and that the port has not lost its carrier. b) Check the Ethernet connection for a bad clock or bad connection.
MSG_EXCESSIVE_TX_ERRORS	413007	Medium	Warning	This alarm indicates that the Ethernet Driver is experiencing a high rate of transmit errors.		Complete this procedure to correct this alarm: a) Check, via the Ethernet Port Statistics, what errors the port is receiving. b) Check the Ethernet for a bad connection or excessive traffic.
MSG_LOSS_OF_CARRIER	413008	Medium	Major	This alarm indicates that the Ethernet Driver is not able to detect a valid transmit clock.		Check the Ethernet connection.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
MSG_EXCESSIVE RX_ERRORS	413009	Medium	Warning	This alarm indicates that the Ethernet Driver is experiencing a high rate of Receive Errors.		Complete this procedure to correct this alarm: a) Check, via the Ethernet Port Statistics, what errors the port is receiving. b) Check the Ethernet connection and Ethernet for a bad connection or excessive traffic.
MSG_EXCESSIVE_ TX_CLEAR	413010	Medium	Normal	This message indicates that the Ethernet Driver is no longer experiencing a high rate of Transmit Errors.		This is an information message only. No corrective action is required.
MSG_LOSS_OF_ CARRIER_CLEAR	413011	Medium	Normal	This alarm indicates that the Ethernet Driver is able to detect a valid Transmit Clock.		This is an information message only. No corrective action is required.
MSG_EXCESSIVE_ RX_CLEAR	413012	Medium	Normal	This message indicates that the Ethernet Driver is no longer experiencing a high rate of Receive Errors.		This is an information message only. No corrective action is required.
MSG_FPGA_INIT_ FAILED	413021	Medium	Critical	This alarm indicates that the Ethernet Driver encountered a failure when programming the 100BT card. The value (*step*) identifies the cause of this alarm.		To correct this problem replace the 100BT card.
EPx task rescued from possible deadlock	9001	Low	Debug	This message indicates that the software detected a rare situation of a possible deadlock. The condition was automatically corrected.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
EPx rescued msg 1 n1/n2/n3:n4n5	9002	High	High	This message indicates that the software has been rescued from a crash condition and that the problem has been auto-corrected.		Capture the node CMEM, software .des file, all node statistics, and the Alarm Log. Contact your representative for identification and resolution of the problem.
EPx rescued msg n0 n1/n2:n3/n4:n5/ n6:n7/n8:n9/n10	9003	High	High	This alarm indicates that one of the processors was in need of a rescue, and the process was restarted.		This is an information message only. No corrective action is required.
ESTABLISHED ISAKMP CONNECTION WITH *(aa.bb.cc.dd)*	425012	Connection	Normal	Successfully negotiated a ISAKMP SA with the remote. The node now proceeds to establish IPSEC Security Association. The value *(aa.bb.cc.dd)* identifies an IP Address.		This is an informative message.
ESTABLISHED IPSEC CONNECTION WITH *(aa.bb.cc.dd)*	425013	Connection	Normal	Successfully established IPSEC connection with the remote peer. Data passing can now start on the tunnel. The value *(aa.bb.cc.dd)* identifies an IP Address.		This is an informative message.
EXCEEDING MAXIMUM RANGE ALLowED	134007	High	Critical	This alarm indicates that a bridge link number, stored in configuration memory, is not within the allowable range.		To correct this problem: • Check the Token Ring and Ethernet LAN port configuration. • Confirm that the bridge link configuration is between 1 and 5.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
EXCEEDING THE MAXIMUM NUMBER OF INTERFACES ALLOWED	210003	Low	Critical	This alarm indicates that the number of configured interfaces exceeds the maximum number of interfaces.		To correct this problem: a) Increase the value of Maximum IPX Interfaces parameter. b) Reduce the number of interfaces configured.
EXCEEDS MAXIMUM NUMBER OF LINKS FOR THIS BUNDLE	270017	Medium	Critical	This alarm indicates that a new call has attempted to join an existing MLPPP bundle, but was rejected to conform to the configured Maximum Number of Switched Links.		To correct this problem: a) Increase the value configured for the Maximum Number of Switched Links, or b) Configure the remote equipment to limit the number of links in a bundle.
FAILED KEY EXCHANGE	379004	High		The connection can not establish data encryption session - authentication failure.		Check whether end points are properly configured for data encryption. Check whether they use the same base key and the same key length.
FAILED KEY EXCHANGE, NO RESPONSE	379005	High		The connection can not establish data encryption session - no response has been received from the remote end.		Check whether link is operational. Check if end points are properly configured.
FAILED TO COPY SOFTWARE	105003	High	Critical	This alarm indicates that the FLASH-to-FLASH copy has failed.	105002, 105005, 105014	To correct this problem: a) Ensure no network errors occurred. b) Ensure the correct FLASH to FLASH option was chosen.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
FAILED TO UPDATE SOFTWARE	105006	High	Critical	This alarm indicates that a RAM-to-RAM transfer has failed.	105002, 105005, 105014	To correct this problem: a) Ensure no network errors occurred. b) Ensure the correct FLASH to FLASH option was chosen.
FLASH CHECKSUM ERROR	105010	High	Critical	This alarm indicates the contents of FLASH memory are corrupted.		Installing a valid image will correct this problem.
FLASH CHECKSUM ERROR, SLOT *(s)*	105007	High	Critical	This alarm indicates that there is a checksum error on one the configured slots. The value *(s)* identifies the slot number on which the error occurred.		Installing a valid image will correct this problem.
FLASH CHECKSUM ERROR, *(b) (e) (a)*	1003	High	Critical	This message indicates that a checksum mismatch has been detected while doing a background FLASH checksum. The value *(b)* identifies the FLASH bank involved, *(e)* indicates the expected checksum value, and *(a)* indicates actual checksum value.	1004	This is an information message only. No corrective action is required.
FLASH CHECKSUM OK, *(b) (e) (a)*	1004	High	Normal	This message indicates that a recalculation of the FLASH checksum has produced successful results after previously having failed. The value *(b)* identifies the FLASH bank involved, *(e)* indicates the expected checksum value, and *(a)* indicates actual checksum value.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Flow *(src addr -dst addr), (protocol), (src port -dst port)* dropped	403003	Debug	Warning	This message indicates that a packet belonging to a flow is dropped because none of the nexthops configured in corresponding flow entry are active.		Reconfigure the policy so at least one of the nexthops configured is currently active.
FOUND *(n)* BAD BASE KEYS IN CMEM	379007	High		This message indicates that the node has found a number of non-valid Base Keys in CMEM. The value *(n)* identifies how many keys have been found.		To correct this problem, change the Node Key to the value used for encrypting Base Keys.
FOUND *(n)* GOOD BASE KEYS IN CMEM	379012	High		This message indicates that the node has found a number of valid Base Keys in CMEM. The value *(n)* identifies how many keys have been found.		This is an information message only. There are no corrective actions necessary.
FRAME DROPPED AFTER MAX RETRY	308031	Medium	Minor	This alarm indicates that a device has not acknowledging the receipt of a previous frame, and that frame has been dropped.	308000	Check the device.
FRAME RECEIVED WITH BAD LENGTH: DLCI *(n)*	187002	Medium	Minor	This alarm indicates that a frame larger than the allowed maximum has been received from the link. The value *(n)* identifies the DLCI number.		Configure the remote equipment to send frames less than or equal to the allowed maximum.
FRAME TOO LONG	308023	Low	Minor	This alarm indicates that the frame size is more than 1024 bytes and that a frame has been discarded.	308000	Correct the software in the remote node OR packet was corrupted on the network.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
FRMR *(hh/hh/hh)*	68004	Low	Minor	This message indicates that a FRMR has been received on an X25 link running normal sequencing. The first *hh* is the rejected frame control field, the second is the current V(S) and V(R) of the end sending the FRMR, and the last is the WXYZ bits.		Verify that other end is running X.25 in normal sequencing. If problem persists, hardware at both ends should be checked.
FUNCTION NAME: %s, SIG_STATE: %d	283026	High				Contact your customer service representative if this alarm is displayed.
H323 Node Wide Parameters Boot Complete	392001	High		This message indicates that the H323 Node Wide Parameters were successfully installed.		This is an information message only. No corrective action is required.
H323 NODE WIDE PARAMETERS NOT INSTALLED - Out of memory.	392000	High		This alarm indicates that the node ran out of memory and the Node Wide parameters were not installed.		To correct this problem, either: • Install additional memory. • Install a smaller image.
IGMP.1 RFCM Context Block NULL in function Name.	327001	DEBUG	Low	This is error condition. The IP Router is not active.		Ensure that the IP Router is included and configured in the Multicast image
IGMP.10 Multicast not enabled, IGMP shall not come up	327010	DEBUG	Low	This debug alarm is generated whenever IGMP packets with Multicast disabled globally this alarm is generated.		To enable IGMP enable the global Multicast parameter.
IGMP.11	327011	DEBUG	Low	This is a general debug alarm generated when packet allocation failure occurs in the null IGMP control block.		This is an information message. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IGMP.12	327012	DEBUG	Low	This debug alarm indicates that a router has received packet with a checksum error.		Isolate the device that is sending the packets with a bad checksum.
IGMP.13 IP Context Block NULL	327013	DEBUG	Low	This debug information is generated when a IGMP tries to access a NULL IP data base.		Configure IP or check IP configuration and reports.
IGMP.14 IGMP Packet received on %d IGMP Circuit	327014	DEBUG	Low	This debug message indicates the arrival of an IGMP packet on an IGMP interface.		This is an information message. No corrective action is required.
IGMP.3 Memory allocation for %s failed	327003	DEBUG	Low	This alarm is generated during memory allocation for each group entries (Dynamic heap).		To correct this problem: a) Add memory to the dynamic heap in the router. b) This can be done through the debug menu. c) Add additional DRAM to increase total available memory.
IGMP.4 IGMP Module not up	327004	DEBUG	Low	This alarm is generated when the IGMP module is disabled on a particular interface.		Enable IGMP to handle the IGMP packets being received by the node.
IGMP.5 Packet %s Error	327005	DEBUG	Low	This debug message indicates that an improperly sized packet and Checksum error is reported.		This is an information message. No corrective action is required.
IGMP.6 Getbuff failure	327006	DEBUG	Low	This debug alarm is generated whenever a buff_allocation fails.		Add additional memory to the node to increase the number of existing buffers.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IGMP.7 Failure to insert a group	327008	DEBUG	Low	This debug alarm is generated whenever new groups join and the router fails to put them into the IGMP data base.		Add memory to the router.
IGMP.9 IGMP Packet dropped for IGMP NOT Active on 5	327009	DEBUG	Low	This debug alarm is generated whenever the IGMP receives a packet from a disabled interface on an IGMP.		If IGMP packets received on the interface have to be processed then enable IGMP on that interface.
INACTIVITY TIME OUT	308044	Medium	Major	This message indicates that there is no activity on the connection. The connection will be terminated.	308000	This is an information message only. There are no corrective actions necessary.
INCOMPATIBLE %s DETECTED FOR ISDN	278003	High	Minor			Contact your customer service representative if this alarm is displayed.
INCOMPATIBLE DESTINATION	6024	Medium	Warning	This message indicates that an X.32 Port configuration does not match the destination configuration.		Check the source and destination configuration and modify them so they match.
(p) changed from LHHHHHHHLH to HHHHHHHHLH	6032	Medium		This message indicates CSU/DSU alarm capturing.		This is an informational message.
INCONSISTENT LINK NEGOTIATION	270012	Medium	Major	This alarm indicates that a new link joining an existing MLPPP bundle has attempted to negotiate parameters inconsistent with other operating links in the bundle.		Reconfigure the remote equipment so that it will negotiate a consistent set of parameters.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
INCORRECT LOGIN	270002	Medium	Warning	This alarm indicates that the peer failed to provide a valid account/ password during authentication.		Verify that the remote user or equipment has been provided with a valid account and password.
INPUT BUFFER OVERRUN	46011	Medium	Major	This alarm indicates that an X.25 port output queue has overflowed and that data has been lost.	46000	Check flow control parameters on the adjacent port.
INSUFFICIENT MEMORY TO INITIALIZE IPSec MODULE	425000	High	Major	The system does not have enough memory to initialize the IPSec module. IPSec is disabled.		Check memory allocated.
INSUFFICIENT MEMORY TO SUPPORT APPN CONFIGURATION	383001	High		This alarm indicates that the SNA protocol software did not have enough memory to start-up properly.		To correct this problem, add additional RAM to your Vanguard product.
INSUFFICIENT MEMORY TO SUPPORT TN3270 CONFIGURATION	419000	High		The Remote TN3270 Server Subsystem cannot allocate enough memory to initialize.		Check the configuration of the Local Dynamic Port Creation Heap Size in the node record. Back-up the contents of the Configuration memory and then increase the Local Dynamic Port Creation Heap Size. Note that a Node Boot is required for changes to the Local Dynamic Port Creation Heap to take effect.
INSUFFICIENT RESOURCES TO COMPLETE IPSEC EXCHANGE	425020	High	Major	When attempting to complete IPSec Exchange, node resources have been exhausted.		Reduce the configuration and reboot the node. If the problem persists, call your service representative.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
INTER CHARACTER TIMEOUT	308021	Low	Minor	This alarm indicates that an Inter-Character Timeout Error has occurred and that a frame has been discarded.	308000	Check the port speed to ensure it is set to the correct value.
INVALID PHB *(phb)*, PCK TREATED WITH DEFAULT OF Q'ING & SCH'ING PROF # *(n)*	402001	Low		This alarm indicates that a packet has to receive treatment as per the PHB *(phb)*, where *(phb)* is one of PHB1-PHB15 or CS1-CS7. The packet was mapped to this PHB by classification features, but it is not configured for the Queuing & Scheduling profile. The packet receives treatment as per the DEFAULT PHB configured for the Queuing & Scheduling profile.		To correct this problem: a) Complete one of these actaions: – Change the PHB mapping of the classification features to one of the PHBs configured for the Queuing & Scheduling profile. – Configure the PHB for the Queuing & Scheduling profile. b) Boot the (application).
IPSEC MODULE CANNOT RUN: ENCRYPTION MODULE IS DOWN OR MISSING	425001	High	Major	The encryption module is down or is not operating correctly in the node.		Ensure that the encryption module is installed correctly. Contact customer service if this problem repeats itself.
IPSEC PROFILE *(xx)* DOES NOT EXIST	425011	High	Major	The specified IPSEC profile does not exist. The value *(xx)* identifies a configured name or value.		Ensure the corresponding IPSec profile record exists.
IPX Disabled - memory allocation failure during init	202002	High		This alarm indicates that IPX has failed to obtain memory for critical data structures during initialization and has been Disabled.		To correct this problem you must add additional DRAM to your Vanguard 6520/6560.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPXWAN.1 ipxwan_init called with NULL rfcm Context Block	293000	High	Normal	This alarm indicates that an internal software error has occurred. This problem involves IPXWAN being initialized without the ROUTER module, and that the IPXWAN initialization has failed.		There are two possible solutions to this problem: a) Ignore the alarm if IPXWAN is not being used. b) Ensure that all the LAN SAKs, if IPXWAN is used, are included and boot the node.
IPXWAN.10 Rcvd Tmr Req - option len not 1 for routing type option, lcon %d	293009	Conn	Normal			Contact your customer service representative if this trap is displayed.
IPXWAN.11 Rcvd Tmr Req - wnode id non-zero with extended node id option set, lcon %d	293010	Conn	Warning			Contact your customer service representative if this trap is displayed.
IPXWAN.12 Rcvd Tmr Req - option len not 4 for extended node id, lcon %d	293011	Conn	Warning			Contact your customer service representative if this trap is displayed.
IPXWAN.13 Rcvd Tmr Req - configuration error, lcon %d	293012	Conn	Critical			Contact your customer service representative if this trap is displayed.
IPXWAN.14 Rcvd Tmr Req - no common routing type, lcon %d	293013	Conn	Major			Contact your customer service representative if this trap is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPXWAN.15 Rcvd Tmr Resp - wnode id zero, lcon %d	293014	Conn	Warning			Contact your customer service representative if this trap is displayed.
IPXWAN.16 Rcvd Tmr Resp - multiple routing types marked yes, lcon %d	293015	Conn	Warning			Contact your customer service representative if this trap is displayed.
IPXWAN.17 Rcvd Tmr Resp - could not set the routing type, lcon %d	293016	Conn	Minor			Contact your customer service representative if this trap is displayed.
IPXWAN.18 Rcvd Tmr Resp - routing type not supported, lcon %d	293017	Conn	Critical			Contact your customer service representative if this trap is displayed.
IPXWAN.19 Rcvd Tmr Resp - option len not 1 for routing type option, lcon %d	293018	Conn	Critical			Contact your customer service representative if this trap is displayed.
IPXWAN.2 IPXWAN Module Aborted; not enough RAM	293001	High	Critical	This alarm indicates that IPXWAN initialization has failed due to an insufficient amount of DRAM.		There are two possible solutions to this problem: a) Ignore the alarm if IPXWAN is not being used. b) Increase memory, if IPXWAN is used, to startup IPXWAN.
IPXWAN.20 Rcvd Tmr Resp - header compression not supported, lcon %d	293019	Conn	Warning			Contact your customer service representative if this trap is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPXWAN.21 Rcvd Tmr Resp - no routing type option with yes, lcon %d	293020	Conn	Critical			Contact your customer service representative if this trap is displayed.
IPXWAN.22 Rcvd Info Req - rcvd wnode id zero, lcon %d	293021	Conn	Warning			Contact your customer service representative if this trap is displayed.
IPXWAN.23 %s - bad info exchange option, lcon %d	293022	Conn	Minor			Contact your customer service representative if this trap is displayed.
IPXWAN.24 %s - no info exchange option, lcon %d	293023	Conn	Minor			Contact your customer service representative if this trap is displayed.
IPXWAN.25 %s - zero netno proposed for numbered RIP/ SAP, lcon %d	293024	Conn	Critical			Contact your customer service representative if this trap is displayed.
IPXWAN.26 %s - non-zero netno proposed for an unnumbered protocol, lcon %d	293025	Conn	Critical			Contact your customer service representative if this trap is displayed.
IPXWAN.27 %s - the proposed netno is not equal to active netno, lcon %d	293026	Conn	Critical			Contact your customer service representative if this trap is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPXWAN.28 Rcvd Info Resp - rcvd wnode id is incorrect, lcon %d	293027	Conn	Critical			Contact your customer service representative if this trap is displayed.
IPXWAN.29 Rcvd Info Resp - the proposed netno is already active, lcon %d	293028	Conn	Major			Contact your customer service representative if this trap is displayed.
IPXWAN.3 Memory allocation for %s failed\r\n	293002	Conn	Critical			Contact your customer service representative if this trap is displayed.
IPXWAN.30 Rcvd Info Resp - could not set the active netno, lcon %d	293029	Conn	Critical			Contact your customer service representative if this trap is displayed.
IPXWAN.31 getbuf failed in %s	293030	Conn	Major			Contact your customer service representative if this trap is displayed.
IPXWAN.32 Event %d ignored in state %d, lcon %d	293031	Conn	Warning			Contact your customer service representative if this trap is displayed.
IPXWAN.33 Old State:%d, Event:%d, New State:%d, lcon %d	293032	Conn	Normal			Contact your customer service representative if this trap is displayed.
IPXWAN.34 Too many routing types from remote end, lcon %d	293033	Conn	Major			Contact your customer service representative if this trap is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
IPXWAN.4 IPXWAN is not active in %s\r\n	293003	Conn	Critical			Contact your customer service representative if this trap is displayed.
IPXWAN.5 IPX not active in %s\r\n	293004	Conn	Critical			Contact your customer service representative if this trap is displayed.
IPXWAN.6 %s called for a LAN interface	293005	Conn	Normal			Contact your customer service representative if this trap is displayed.
IPXWAN.7 %s called with a NULL IPXWANCB	293006	Conn	Minor			Contact your customer service representative if this trap is displayed.
IPXWAN.8 IPX not up in lcon %d - dropping the packet	293007	Conn	Minor			Contact your customer service representative if this trap is displayed.
IPXWAN.9 Bad format packet received, lcon %d	293008	Conn	Minor			Contact your customer service representative if this trap is displayed.
ISDN BRI CORE BOOT COMPLETED	278005	High	Normal			Contact your customer service representative if this alarm is displayed.
ISDN BRI INTERFACE %d IS ACTIVE	278000	High	Normal			Contact your customer service representative if this alarm is displayed.
ISDN BRI INTERFACE %d IS INACTIVE	278001	High	Normal			Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ISDN BRI INT. %d %s DISCONNECTED FROM %s, CAUSE: %d	278009	Conn	Normal	ISDN call cleared.		This is an information message only. There are no corrective actions necessary.
ISDN BRI INT. %d BOOT COMPLETED	278014	High	Normal			Contact your customer service representative if this alarm is displayed.
ISDN BRI SWITCH CONFIGURED OVERRIDE	278010	High	Normal			Contact your customer service representative if this alarm is displayed.
ISDN Config Error	278016	High	Critical	This alarm indicates that you have configured phone numbers in ISDN and defined them in Switched Services, or PPP. The numbers defined in Switched Services, or PPP, are dialed by ISDN.		To correct this problem, reconfigure your ISDN.
ISDN LOOP TEST %s %s %s	278002	Low	Warning			Contact your customer service representative if this alarm is displayed.
ISAKMP POLICY *(n)* DOES NOT EXIST	425010	High	Major	The specified ISAKMP policy does not exist.		Ensure the corresponding ISAKMP policy record exists.
ISAKMP PRESHARED KEY *(xx)* HAS BEEN CHANGED	425016	High	Normal	The Pre-Shared key value has changed for the specified key name. The value *(xx)* identifies a configured name or value.		This is an informative message.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
ISAKMP PRESHARED KEYS TABLE BOOTED	425017	High	Normal	ISAKMP Pre-Shared key table has been booted.		This is an informative message.
IV USAGE FORCED BY REMOTE ENCRYPTION PEER	379021	High		This message indicates that while IV (initialization Vector) usage has not been requested in the encryption profile, IV will be used since the remote end requested it.		This is an information message only. There are no corrective actions necessary.
LCON RX DISCARD - NO NEXT HOP TO %s	188003	High	Warning			Contact your customer service representative if this alarm is displayed.
LCON RX DISCARD - NO ROUTE TO %s	188002	High	Warning			Contact your customer service representative if this alarm is displayed.
LCON TX DISCARD - UNKNOWN NEXT HOP %s	188004	High	Minor			Contact your customer service representative if this alarm is displayed.
link %d - UNKNOWN STP BPDU received	137000	Medium	Minor			Contact your customer service representative if this alarm is displayed.
LINK DOWN	42000	High	Major	This alarm indicates that a link is inoperative. This alarm occurs when the number of attempts to connect (as set during configuration) is exceeded.	42007	Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
LINK DOWN	43000	High	Major	This alarm indicates that a link is inoperative. This alarm occurs when the number of attempts to connect (as set during configuration) is exceeded.	43007	Check cables and hardware for possible failure. If these are OK, check the transmission media.
LINK DOWN	308040	High	Major	This message indicates that a connection between PAD (HPAD and TPAD) is down.	308000	This is an information message only. There are no corrective actions necessary.
LINK IS LOOPED BACK	270016	High	Major	This alarm indicates that a unique end-point discriminator, generated locally, as been received during link negotiation.		Check all PPP links for possible circuit loops to correct this problem.
LLC LT: INVALID FRAME *(t)* RCVD FROM *(w)* LOC MAC/SAP *(a)(p)*, REM MAC/SAP *(a)(p)*	155000	Medium	Warning	The initial frame must be XID or SABME to properly initiate an LLC session. The value *(t)* identifies the frame type, *(w)* identifies where the invalid frame was received from, *(a)* identifies the MAC Address, and *(p)* identifies the Service Access Point.		This is an information message only. No corrective action is required.
LOCAL FLASH COPY COMPLETE	105014	High	Normal	This message indicates that a local FLASH copy is finished.		This is an information message only. No corrective action is required.
LOCAL FLASH COPY FAILED	105015	High	Critical	This alarm indicates that a failure occurred while copying local FLASH memory.	105002, 105005, 105014	Verify that all input parameters are correct.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
LOG CLEARED	15001	Low	Warning	A record of all alarms is kept in an Alarm Log. Periodically this log is cleared of all previously recorded alarms.		This alarm distributed to the Alarm log only. **■Note** This is an information message only. No corrective action is required.
LOGIN OK	270003	Medium	Normal	This alarm indicates that the peer successfully passed authentication.		This message is for information only. No corrective actions are necessary.
LOST *(n)* MESSAGES IN 60 SECONDS	178002	Medium	Major	This message indicates that (n) messages have been lost during a 60 second period.		This is an information message only. No corrective action is required.
MASTER POLLED EARLY	68006	High	Minor	This message indicates that an MX25 slave detected that the master has polled another slave prior to it going off line.		Reconfigure the poll timer to a larger value.
MESSAGES LOST	308033	High	Warning	This alarm indicates that a message received, from a remote PAD is out of sequence. Normally happens during the initial connection establishment.	308000	If this message is displayed while a connection is being established, no action is required. Otherwise, check the connection between the PAD ports (HPAD and TPAD).
MONITORED NAME IN SWITCHED SERVICE ENTRY	242008	High	Critical	This message indicates that the name of one of the monitored ports of a SS entry has been changed and the tables booted.		Boot the node to correct this problem.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
NO BUNDLES AVAILABLE	270013	Medium	Critical	This alarm indicates that a call has been received which requires a new PPP bundle to be established, but the maximum number of operating bundles has already been reached.		Increase the number of PPP profiles/connections available by configuring new PPP Profile Records and booting the node.
No Ethernet SAK	236004	High		This message indicates that AppleTalk configured for an Ethernet port and the Ethernet SAK has not been entered.		Enter the Ethernet SAK and reboot the node. **Note** Refer to the Vanguard *Basics Manual* (Part Number T0113) for instructions on entering SAKs.
NO H323 NODE RECORDS FOUND - Installing Defaults	392002	High		This alarm indicates that the node wide records were not found in CMEM. The defaults are being installed.		To correct this problem, either: • Use the defaults. • Configure the H232 Node Wide Parameters.
NO MEMORY - TFTP UPLOAD TO SCRIPT FAILED	4003	High	Critical			Contact your customer service representative if this alarm is displayed.
NO ROOM IN FACILITY FOR DCP	91000	Low	Minor	This alarm indicates that an internal error has occurred.		Advise your customer service representative of the problem. There are no corrective actions you can perform when this alarm is displayed.
NODE BOOT COMPLETE	19002	High	Normal	This alarm indicates that a Node Boot has been successfully completed in response to a CTP command.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Node boot required. The number of MNEM table entries in CMEM does not match the active number.	21000	High	Critical	This alarm indicates that the active size is different from the CMEM size at table boot time.		Perform a node boot for the entry to take effect.
Node boot required. The number of PVC table entries in CMEM does not match the active number.	16005	High	Critical	This alarm indicates that the active number, of PVC table entries, is different from the configured maximum number of PVC entries at table boot time.		Perform node boot for the entry to take effect.
Node boot required. The number of ROUT table entries in CMEM does not match the active number.	16004	High	Critical	This alarm indicates that the active memory size is different from the CMEM size when the Table Boot occurs.		Perform a Node boot for the entry to take effect.
NODE COLDSTARTED	19005	High	Normal	This message indicates that the node has been cold started; diagnostics will be run as part of the startup procedure.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
NODE KEY CHANGED	379010	High		This indicates that a new Node Key has been entered or the existing Node Key changed.		This report is a record of critical encryption action taking place in the node. If this activity has been performed by an authorized individual, no further action is required, otherwise, a security breach may have occurred. You should check physical security of the nodes and the configuration to identify and plug any security hole
NODE KEY NOT CONFIGURED	379006	High		This alarm indicates that the Encryption Node Key is invalid. In this case the system will temporarily use the default Node Key.		To correct this problem, change the value of the Node Key to prevent it from becoming a security hazard.
NODE RECORD BOOT FAILED, *(cause)*	173000	High	Warning	This alarm indicates that a node record could not be booted. The value *(cause)* identifies the reason for the failure.		Use the *(cause)* to identify where the problem is. Once identified, correct the problem and then boot the port.
NODE RESET DUE TO CRASH	19003	High	Normal	This alarm indicates that a node reset occurred because of a system crash.		This is an information message only. No corrective action is required.
NODE RESET DUE TO DEBUGGER COMMAND	19004	High	Normal			Contact your customer service representative if this alarm is displayed.
NODE RESET DUE TO WATCHDOG TIMER TIMEOUT	19001	High	Critical	This alarm indicates that a 65xx watchdog timer has expired causing a node to boot.		Contact your customer service representative for additional information.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
NODE RESET WITH DEFAULT PASSWORD	19018	High	Critical			Contact your customer service representative if this alarm is displayed.
NODE WARMSTARTED	19006	High	Normal	This message indicates that the node has been warm started; diagnostics will not be run during startup.		This is an information message only. No corrective action is required.
Not enough memory - *(err_msg)*	403000	High	Critical	This message indicates that not enough memory (permanent or dynamic) is available for PBR objects. The value *(err_msg)* specifies the consequence of memory allocation failure.		To correct this problem, either: • Add more DRAM in the node. • Disable some of the features not being used.
NS RUN TIME ERROR- NO FEATURES	229000			This message indicates that a software module tried to register with Switched Services but the image did not contain the Switched Service Module.		This is an information message only. No corrective action is required.
NS RUN-TIME ERROR - DATA STRUCTURE IN ERROR	229002	Low	Critical			Contact your customer service representative if this alarm is displayed.
NS RUN-TIME PARAMETER ERROR	229000	High	Critical			Contact your customer service representative if this alarm is displayed.
NULL REPORT	68000	Low	Normal			Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
OUTER,ETH PORT,TKR PORT subsystems SRAM related high priority traps	162000	High	Major			Contact your customer service representative if this trap is displayed.
OUTER,ETH PORT,TKR PORT subsystems SRAM related low priority traps	162002	Low	Warning			Contact your customer service representative if this trap is displayed.
OUTER,ETH PORT,TKR PORT subsystems SRAM related medium priority traps	162001	Medium	Minor			Contact your customer service representative if this trap is displayed.
PACKET LEVEL RESTART	246000	Low	Normal	This message indicates that X25 layer 3 has received a RESTART packet.		This is an information message only. There are no corrective actions necessary.
PERMANENT LINKS MUST CONFIGURED AS A DEDICATED LINK IN A PROFILE	270018	High	Critical	This alarm indicates that a permanent link (non-switched link) has been configured, but is not referenced as a Dedicated Link in any PPP profile and thus is unusable.		To correct this problem: a) Configure the link as a Dedicated Link in a PPP profile record, or b) Delete the link from the configuration.
PHONE NUMBER BUSY	6022	Medium	Warning	This message indicates that the desired destination number was busy.		Try later, or supply another number.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PORT (n) - BAD CCC RECEIVED	177010	Low	Warning	This alarm indicates that a message was received with a bad checksum (CCC). This indicates a line error. The value *PORT (n)* identifies the port affected.		Check all connections on the node and correct as necessary.
PORT (n) - PORT ENABLED	129004	High	Normal	This message indicates that a port has been enabled via the CTP port. The value *PORT (n)* identifies the port affected.		This is an information message only. No corrective action is required.
POSSIBLE DATA LOSS	59000	High	Major	This alarm indicates that one of the following problems has occurred: a) Node congestion. b) Errors on the network side. c) Request for disconnect from the remote device (network side).		To correct these problems: a) Check the network connection. b) Check the data buffer usage in node stats. c) A hardware upgrade maybe required.
POSSIBLE DATA LOSS	125012	High	Major	This alarm indicates that the remote end of a connection has been disconnected or there has been a network failure.	125000	Check the network connections and the remote device.
Precedence Array Assignments = %d %d %d %d	156012	High	Critical			Contact your customer service representative if this alarm is displayed.
PRESHARED KEY *(xx)* FOR IPSEC PROFILE *(xx)* DOES NOT EXIST	425002	High	Major	The Pre-Shared key specified in the IPSec profile does not exist. The value *(xx)* identifies a configured name or value.		Configure a Pre-shared key for the key name specified in the IPSec profile.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
PRI-%d - %s CALL %s %s ON	283033	Medium	Normal			Contact your customer service representative if this alarm is displayed.
PRI-%dB%d - INCOMING CALL TO %s FROM %s CONNECTED ON PORT %d	283011	Medium	Normal	ISDN PRI Call in.		Contact your customer service representative if this alarm is displayed.
PRI-%dB%d - INCOMING CALL TO %s FROM %s FAILED, %s	283025	Medium				Contact your customer service representative if this alarm is displayed.
PRIORITY QUEUE BLOCKED	46012	Medium	Warning	The queue for packets of the mentioned traffic priority level is blocked.	46000	This is an information message only. No corrective action is required.
Process Msg: PID: *(n)* Event: *(n)* x25cause: *(n)* x25diag: *(n)* Stat	242015			This is DEBUG report and only appears when the DEBUG option is enabled. Used for tracing call events through software modules.		Contact your customer service representative for additional information.
Protocol Priority Profile Entry %d in LCON-%d not found	156011	High	Critical			Contact your customer service representative if this alarm is displayed.
Proxy %d Ignored. Has duplicated IP address or Mac Address	347002	High	Minor			Contact your customer service representative if this alarm is displayed.
Proxy %d Ignored.IP interface not available	347001	High	Major			Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Proxy specifying interface %d Mac Address is deactivated	347003	High	Critical			Contact your customer service representative if this alarm is displayed.
QFRMR RECEIVED	76003	Low	Minor	This message indicates that a received QLLC was not recognized by the current QLLC implementation. This is probably due to a QFRMR being sent. Control received address bits are: • 0 = undefined control field • 1 = invalid information field		Verify that the ends are running primary to secondary QLLC and contact your customer service representative.
QLLC BAD PACKET LENGTH *(l)*	76001	Low	Minor	This message is displayed when a QLLC packet, that was either too long or short, has been received. The value *(l)* indicates the length of the packet.		Verify that the ends are running primary to secondary QLLC and contact your customer service representative.
QLLC ILLEGAL PKT DETECTED	76002	Low	Minor	This message indicates that a received QLLC was not recognized by the current QLLC implementation. This is probably due to a QFRMR being sent. Control received address bits are: • 0 = undefined control field • 1 = invalid information field		Verify that the ends are running primary to secondary QLLC and contact your customer service representative.
QLLC PROTOCOL ERROR *(x) (y)*	76000	Low	Warning	This message indicates that an invalid sequence of QLLC packets has been received. The value *(x)* identifies the current statistics and *(y)* identifies the illegal message received.		Verify that the ends are running primary to secondary QLLC and contact your customer service representative.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
QOS : INITIALIZATION FAILURE - NOT ENOUGH MEMORY	387001	High	Critical	This alarm is logged during node initialization if there is not enough memory to bring up the protocol priority feature for the node.		To correct this problem: a) Add more memory and/or configure the QoS General parameters appropriately. b) Boot the node.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
QOS : NOT OPERATIONAL AS CONFIGURED FOR *(application)* - *(cause)*	387000	High	Critical	a) PROFILE DOES NOT EXIST - Some or all profiles specified for the *(application)* are not configured in Protocol Priority Profile Table. b) IP FLOWS EXCEEDED THE LIMIT - The IP flow across all specified protocol priority profiles for the *(application)* have exceeded the configured limit. c) IPX FLOWS EXCEEDED THE LIMIT - The IPX flow across all specified protocol priority profiles for the *(application)* have exceeded the configured limit.		a) If this cause is indicated: • Configure the profiles in Protocol Priority Profile Table and/or configure the appropriate profile numbers for the *(application)*. • Boot the *(application)*. b) If this cause is indicated, there are two possible procedures you can follow: • Reduce the IP flows in the profiles specified for the *(application)*, and then boot the *(application)*. • Configure appropriate value for the QoS General parameter - "Maximum Number of IP Flows", and then boot the node. c) If this cause is indicated, there are two possible procedures you can follow: • Reduce the IPX flows in the profiles specified for the *(application)* and then boot the *(application)*. • Configure appropriate value for the QoS General parameter - "Maximum Number of IPX Flows" and then boot the node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
QOS : NOT OPERATIONAL AS CONFIGURED FOR *(application)* - *(cause) (Cont'd)*	387000			d) NO SERVICE CHANNEL e) NOT ENOUGH SERVICE QUEUES		d) Contact your customer service representative if this alarm is displayed. e) Contact your customer service representative if this alarm is displayed.
QOS : TOTAL PERCENTAGE > 100 FOR *(application)* - NORMALIZED TO 100%	389000	High	Critical	This alarm is generated for an application (for example LCON-1) when the total percentage of less than 100% classes, among all the profiles specified, has exceeded 100%. The percentage assignments of these classes are normalized to 100% and are listed in the application statistics.		To correct this problem, identify the percentage assignments of the classes in the applications statistics, and: a) If these are not the correct values, configure the proper percentages in the Protocol Priority Profile Table so that less than 100% classes add to 100%. b) Boot the *(application)*.
QOS : TOTAL PERCENTAGE < 100 FOR *(application)* - PERCENTAGE ASSIGNMENT FOR DEFAULT CLASS OF PROFILE *(x)* CHANGED TO *(value)*	389001	Medium	Major	This alarm is generated for an application (for example LCON-1) when the total percentage of less than 100% classes, among all the profiles specified, does not add to 100%. The difference is added to the DEFAULT class of the last profile *(x)* so that the new assignment for it is *(value)*.		If the *(value)* is not the intended one: a) Configure the proper percentages in the Protocol Priority Profile Table so that all less than 100% classes add to 100%. b) Boot the*(application)*.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
QOS: DISABLED FOR *(application)* - *(cause)*	400001	High		This message indicates that QoS can not be brought up for *(application)* because of *(cause)*. The value *(application)* indicates the application identifier value (for example, LCON1) while *(cause)* is one of: • QCL PROF # *(n)* NOT CONFIGURED (The QCL profile is not configured.) • NO QCL CHANNEL (The QCL channel is unavailable.)		To correct this problem, complete one of these actions: • Configure the QCL profile and boot the application. • Configure appropriate value for the QoS General Parameter Maximum Number of QCL Channels and boot the node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
QOS: DISABLED FOR *(application)* *(cause)*	401000	High		This report is generated when QoS features can not be brought up for the *(application)* because of *(cause)*. The value *(application)* indicates the application identifier value (for example, LCON1) while *(cause)* is one of: a) IP C'FIER PROF # *(n)* NOT CONFIGURED (IP Classifier profile is not configured.) b) NO IP C'FIER CHANNEL (IP Classifier channel is not available.) c) DS MF C'FIER & MARKER PROF # *(n)* NOT CONFIGURED (DiffServ MF Classifier & Marker profile is not configured.) d) NO DS MF C'FIER & MARKER CHANNEL (DiffServ MF Classifier & Marker channel is not available.) e) DS BA C'FIER & REMARKER PROF # *(n)* NOT CONFIGURED (DiffServ BA Classifier & Remarker profile is not configured.)		Perform the corrective action that corresponds to the cause indicated. a) Configure the IP Classifier profile and boot the application. b) Configure appropriate value for the QoS General Parameter Maximum Number of IP Classifier Channels. Boot the node. c) Configure the DiffServ MF Classifier & Marker profile and boot the application. d) Scheduling profile and boot the application. e) Configure appropriate value for the QoS General Parameter - Maximum Number of Service Channels. Boot the node

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
QOS: DISABLED FOR *(application) - (cause) (Cont'd)*	401000	High		f) RNO DS BA C'FIER & REMARKER CHANNEL (DiffServ BA Classifier & Remarker channel is not available.) g) IPX C'FIER PROF # *(n)* NOT CONFIGURED (IPX Classifier profile is not configured.) h) NO IPX C'FIER CHANNEL (IPX Classifier channel is not available.)		f) If Custom PHBs are not required, configure % Bandwidth for Custom PHBs with zero and delete Custom PHB records, if any. g) If Custom PHBs are required, configure % Bandwidth for Custom PHBs with appropriate value. Configure the Custom PHBs appropriately, so that the total bandwidth adds to the value configured for Custom PHBs. Boot the application. h) Reduce the number of queues needed by appropriately configuring the required PHBs (DiffServ Class Selector PHB Group and Custom PHBs) for the Queuing & Scheduling profile and boot the application. Or configure appropriate value for the QoS General Parameter - Maximum Number of Queues and boot the node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
QOS: DISABLED FOR *(application)* - *(cause)*	402000	High		This report is generated when QoS features can not be brought up for *(application)* because of *(cause)*. The value *(application)* identifies the application (for example, LCON1) while *(cause)* is one of: a) Q'ING & SCH'ING PROF # *(n)* NOT CONFIGURED (This means that the Queuing & Scheduling profile is unconfigured.) b) NO SERVICE CHANNEL (This means that the Service channel for Queuing & Scheduling is unavailable.) c) Q'ING & SCH'ING PROF # *(n)* - CUSTOM PHB ERROR (This means that the Custom PHB configuration error which is one of the following: Bandwidth for Custom PHBs is configured, but no Custom PHBs are configured, Total bandwidth of all configured Custom PHBs does not match the value configured for Custom PHBs.)		Perform the corrective action that corresponds to the cause indicated. a) Configure the Queuing & Scheduling profile and boot the application. b) Configure appropriate value for the QoS General Parameter - Maximum Number of Service Channels. Boot the node. c) If Custom PHBs are not required, configure % Bandwidth for Custom PHBs with zero and delete Custom PHB records, if any. If Custom PHBs are required, configure % Bandwidth for Custom PHBs with appropriate value. Configure the Custom PHBs appropriately, so that the total bandwidth adds to the value configured for Custom PHBs. Boot the application.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
QOS: DISABLED FOR *(application)* - *(cause)* (Cont'd)	402000	High		d) NOT ENOUGH QUEUES FOR Q'ING & SCH'ING PROF # *(n)* (This means that there are insufficient queues for the PHBs associated with the Queuing & Scheduling profile. The maximum number of queues for an application is 16 and the total number of queues for PHBs across all enabled applications should not exceed the value configured for QoS General Parameter - Maximum Number of Queues.)		d) Reduce the number of queues needed by appropriately configuring the required PHBs (DiffServ Class Selector PHB Group and Custom PHBs) for the Queuing & Scheduling profile and boot the application. Or configure appropriate value for the QoS General Parameter - Maximum Number of Queues and boot the node.
QOS: INITIALIZATION FAILURE - NOT ENOUGH MEMORY	400000	High		This message indicates that is a failure was logged during node initialization when there was not enough memory to bring up the QoS features for the node.		Add more memory or configure the QoS General parameters appropriately. Boot the node.
QOS: IP FLOW # *(n)* USED IN DS C'FIER & MARKER PROF # *(n)* IGNORED FOR *(application)*	401003	Low		This alarm indicates that a warning was generated for *(application)* when the IP Flow used in DiffServ MF Classifier & Marker profile is not configured in IP Flow Table. The value *(application)* identifies the application identifier value (for example, LCON1). The corresponding DiffServ MF Classifier & Marker profile entry is ignored.		To correct this problem: a) Configure the IP Flow in IP Flow Table or configure the DiffServ MF Classifier & Marker profile appropriately. b) Boot the *(application)*.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
QOS: IP FLOW # *(n)* USED IN IP C'FIER PROF # *(n)* IGNORED FOR *(application)*	401001	Low		This message indicates that a warning was generated for *(application)* when the IP Flow used in IP Classifier profile is not configured in IP Flow Table. The value *(application)* is the application identifier value (for example, LCON1). The corresponding IP Classifier profile entry is ignored.		Configure the IP Flow in IP Flow Table or configure the IP Classifier profile appropriately. Boot the *(application)*.
QOS: IPX FLOW # *(n)* USED IN IPX C'FIER PROF # *(n)* IGNORED FOR *(application)*	401002	Low		This message indicates that a warning was generated for *(application)* when the IPX Flow used in IPX Classifier profile is not configured in IPX Flow Table. The value *(application)* is the application identifier value (for example, LCON1). The corresponding IPX Classifier profile entry is ignored.		Configure the IPX Flow in IPX Flow Table or configure the IPX Classifier profile appropriately. Boot the (application).
Received a E_Disconnect from BRI_PORT	241044	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
RECEIVED INVALID CC TPDU	91004	Low	Minor	This alarm indicates that an invalid code was encountered in the DCP facility in a Call Connected packet.		A non-DCP call was inadvertently routed to the local DCP service. Check the X.25 call routing configuration.
RECEIVED INVALID CR TPDU	91003	Low	Minor	This alarm indicates that an invalid code was encountered in the DCP facility in a Call Request packet.		A non-DCP call was inadvertently routed to the local DCP service. Check the X.25 call routing configuration.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
RECEIVED INVALID TPDU HEADER LENGTH	91006	High	Warning	This alarm indicates that the length of the TPDU trailer in a DCP data packet was invalid.		A non-DCP call was inadvertently routed to the local DCP service. Check the X.25 call routing configuration.
RECEIVED INVALID TPDU TYPE	91007	High	Warning	This alarm indicates that an invalid TPDU type was encountered in a DCP data packet.		A non-DCP call was inadvertently routed to the local DCP service. Check the X.25 call routing configuration.
RECEIVED MULTILINK FRAME WITH INVALID FORMAT	270009	High	Minor	This alarm indicates that an MLPPP protocol encapsulated frame has a corrupted Multilink header.		Check the configuration of the remote equipment with respect to multilink operation.
RECEIVED NULL POINTER	91002	Low	Minor	This alarm indicates that an internal error has occurred.		Advise your customer service representative of the problem. There are no corrective actions you can perform when this alarm is displayed.
RECEIVED NULL POINTER	92001	Low	Minor	This alarm indicates that an internal error has occurred.		Contact your customer service representative of the problem. There are no corrective actions you can perform when this alarm is displayed.
RECEIVED OUTBOUND PACKET OF UNSUPPORTED PROTOCOL	270000	Medium	Minor	This alarm indicates that an attempt was made to transmit a packet in which the network protocol is not supported.		Ensure that the application attempting to send data on the PPP link is only using one supported network protocol, such as IP or IPX.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
RECEIVED UNAUTHORIZED ISAKMP REQUEST FROM (*aa.bb.cc.dd)*	425014	High	Major	Received unexpected requests to establish ISAKMP SA from remote node *aa.bb.cc.dd.* The request is ignored. The value *(aa.bb.cc.dd)* identifies an IP Address.		Ensure a valid IPSec configuration exists. If IPSec services are not required from this remote peer, check for intrusion.
RECEIVED UNKNOWN PACKET TYPE INDICATOR	91005	Low	Minor	This alarm indicates that an internal error has occurred.		Advise your customer service representative of the problem. There are no corrective actions you can perform when this alarm is displayed.
RECEIVED UNKNOWN PACKET TYPE INDICATOR	92000	Low	Minor	This alarm indicates that an internal error has occurred.		Contact your customer service representative of the problem. There are no corrective actions you can perform when this alarm is displayed.
record : Attempt to add duplicate record	210004	Low		This alarm indicates that a duplicate record was encountered in the specified table at the entry number.		The specified table cannot have duplicate entries, delete one of the duplicate entries and reboot the table.
REMOTE CONNECTION ESTABLISHED	222004	CONN	Normal	This message indicates that a connection has been established.		This is an information message only. There are no corrective actions necessary.
REMOTE PEER (*aa.bb.cc.dd)* DID NOT RESPOND TO ISAKMP REQUEST	425008	High	Major	Cannot establish communication with remote peer. Either the remote is not configured for ISAKMP or the path to remote is down. (*aa.bb.cc.dd) refers to an IP Address*		Ensure that the path to the remote node is active and that the remote peer is configured to receive IPSec connections.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
REMOTE PPP IS SILENT	270010	Medium	Major	This alarm indicates that the peer, expected to initiate exchanges on a dial-in connection, has remained silent.		Verify that the remote equipment is functioning.
REQUIRED MODULE *(name) (#)* NOT FOUND	176006	High	Critical	This alarm indicates that the system does not contain a software module that is necessary for the configuration of ALC. The values *(name)* and *(#)* identify the software modules name and number.		Contact Customer Service if this alarm is displayed.
RESET FROM REMOTE ENCRYPTION PEER	379013	High		This message indicates that a remote peer could not recognize the SPI. This may indicate that the remote node has crashed.		This is an information message only. There are no corrective actions necessary.
ROUT MAIN: Command: *(event)* from *(n)*	16019			This is a DEBUG report and only appears when the DEBUG option is enabled. Used for tracing call events through software modules.		Contact your customer service representative for additional information.
ROUTER,ETH PORT,TKR PORT subsystems high priority traps	154000	Conn	Major			Contact your customer service representative if this trap is displayed.
ROUTER,ETH PORT,TKR PORT subsystems low priority traps	154002	Conn	Warning			Contact your customer service representative if this trap is displayed.
ROUTER,ETH PORT,TKR PORT subsystems medium priority traps	154001	Conn	Minor			Contact your customer service representative if this trap is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
rtn_msg: lg_refapp = 0x%x, refapp.S0 = 0x%x	241042	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
RX MESSAGE QUEUE OVERFLOW	130001	Medium	Major	This message indicates that the speed at which the receiving device is operating, does not match that at which the originating device is transmitting. The result of this mismatch in device speeds is that the message queue on the receiving end overflows and the WAN link becomes congested.		Reconfigure congestion parameters as required.
RX_ISR : DEFAULT : CODRET	241032	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
RX_ISR : DEFAULT-2 : CODRET	241033	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
RX_ISR : P_CONNSDR : CODRET	241030	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
RX_ISR : P_DISCSDR : CODRET	241031	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
RX_ISR : P_SETUPSDR : CODRET	241029	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
sdrvc_traitetbenrep(): loop timed out	241040	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
sdrvr_disc(rtn_msg): returned	241041	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
Select Condition: Chain: *(n)* PID: *(n)* TbleAddr: *(n)* SETUP: *(n)*	242014			This is a DEBUG report and only appears when the DEBUG option is enabled. Used for tracing call events through software modules.		Contact your customer service representative for additional information.
Select Destination: *(n)*	242013			This is a DEBUG report and only appears when the DEBUG option is enabled. Used for tracing call events through software modules.		Contact your customer service representative for additional information.
SNAP: SYSERR *(counter)*	384000	High		This alarm indicates that an SNA protocol software Retry Counter error has occurred.		Record the report exactly as it appears on screen, and report it to Customer Service.
SNMP AGENT - AUTHENTICATION FAILURE	151006	High	Major	This alarm indicates that an SNMP operation, requested by the manager, is not authorized.	151000, 151001	Correct the 'SNMP Communities' configuration and boot the Tables and Node records for the change to take effect. **■ Note** Refer to the Vanguard *Basic Protocols Manual* (Part Number T0106) for additional information.
SNMP AGENT - CONNECTED TO MAIN CHANNEL	151002	High	Normal	This message indicates that a connection to the Main UDP channel has been successfully established.	151000, 151001, 151002	This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
SNMP AGENT - LOST MAIN CHANNEL CONNECTION	151003	High	Major	This alarm indicates that a connection to the Main UDP channel has been lost. The SNMP Agent will attempt to recover on it's own although, if this fails, a Node boot will be required.		Boot the node if the SNMP Agent is unable to recover. **■Note** Refer to the Vanguard *Basic Protocols Manual* (Part Number T0106) for additional information.
SNMP AGENT - SNMP Agent Cold Start	151000	High	Normal	This message indicates that an SNMP Agent has been started up after a Node Boot. Note that diagnostics are run as part of the cold start process.		This is an information message only. There are no corrective actions necessary. **■Note** Refer to the *SNMP Feature Manual* (Part Number T0106-04) for additional information.
SNMP AGENT - SNMP Agent Warm Start	151001	High	Normal	This message indicates that an SNMP Agent has been started up after a Warm Boot operation. The value *(a)* indicates the Agent affected.		This is an information message only. There are no corrective actions necessary.
SNMP CONNection FLow CONTROL (cannot get DBUFFER)	153003	High	Critical	This alarm indicates an internal memory conversion failure.		Boot the node to correct this alarm condition.
SNMP CONNection FLow CONTROL (cannot get IORB)	153002	High	Critical	This alarm indicates an internal memory conversion failure.		Boot the node to correct this alarm condition. **■Note** Refer to the Vanguard *Basic Protocols Manual* (Part Number T0106) for additional information.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
SNMP CONNection FLow CONTROL (cannot get memory)	153001	High	Critical	This alarm indicates that packets, being received from the SNMP Manager, cannot be processed due to a failure in memory allocation.		Boot the node to correct this alarm condition. **■Note** Refer to the Vanguard *Basic Protocols Manual* (Part Number T0106) for additional information.
SNMP CONNection is Restarting	153000	High	Major	This message indicates that an SNMP connection module has been warm booted.		This is an information message only. There are no corrective actions necessary.
SOFTWARE FAILURE LOGGED	25000	High	Critical	This alarm indicates that a fatal error report is logged during system startup.		Display the Fatal Error Reports and send the results to Customer Service.
SOFTWARE FAILURE LOGGED	9000	High	Warning	This alarm indicates that a software crash occurred. The text in the alarm log may provide information generated by the module that detected the failure.		Contact you customer service representative if this alarm appears.
SOFTWARE FAILURE LOGGED	25000	High	Critical	This alarm indicates that an error report was logged during system startup		Display the Fatal Error Reports and send the results to Customer Service.
SOFTWARE LOADED FROM ALTERNATE FLASH	106001	High	Normal			Contact your customer service representative if this alarm is displayed.
SOFTWARE UPDATE COMPLETE	105005	High	Normal	This message indicates that a RAM-to-RAM transfer has finished.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
SOLICIT ABORT	308037	High	Major	This alarm indicates that a POLL has been received in solicited state by the HPAD port, and that the Solicited state has been aborted.	308000	Check the device.
SOTCP Init failed Software absent	331001	High	Critical	This alarm indicates that a software module (IDCM, TCP, TGO) is absent in the software bundle used to create the image. SOTCP needs these modules and cannot function without them.		Create a new image with these modules included and down load the new image into the node.
SOTCP Voice Total SVC Decrement Failed				This alarm indicates that Total Voice SVCs could not be further decremented.		Contact your customer service representative if this alarm appears.
SOTCP Voice Num SVC Decrement Failed				This alarm indicates that the number of Voice SVCs for scb could not be further decremented.		Contact your customer service representative if this alarm appears
SOTCP Data Total SVC Decrement Failed				This alarm indicates that Total Data SVCs could not be further decremented.		Contact your customer service representative if this alarm appears
SPFM #%d - CONFIGURATION MISMATCH ON REMOTE SPFM	285009	Low	Critical			Contact your customer service representative if this alarm is displayed.
SPFM #%d - CONNECTION ACTIVE %s -> %s	285005	Low	Normal			Contact your customer service representative if this alarm is displayed.
SPFM #%d - CONNECTION INACTIVE %s -> %s	285006	Low	Normal			Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
SPFM #%d - DISABLED, DUPLICATE SLOT ON SPFM #%d	285003	Low	Critical			Contact your customer service representative if this alarm is displayed.
SPFM #%d - DISABLED, MISCONFIGURED OPTION	285004	Low	Critical			Contact your customer service representative if this alarm is displayed.
SPFM #%d - PVC CONNECTED %s -> %s	285002	Low	Normal			Contact your customer service representative if this alarm is displayed.
SPFM #%d - PVC CONNECTION FAILED ON %s	285001	Low	Minor		285002	Contact your customer service representative if this alarm is displayed.
SPFM #%d - SPFM HEADER FORMAT ERROR	285008	Low	Minor			Contact your customer service representative if this alarm is displayed.
SPFM #%d ENTRY BOOT COMPLETE	286001	High	Normal			Contact your customer service representative if this alarm is displayed.
SPFM #%d ENTRY BOOT FAILED	286002	High	Warning			Contact your customer service representative if this alarm is displayed.
SPFM - RX DATA ON UNKNOWN DLCI SLOT %s(%d)	285007	Low	Warning			Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
SS incoming call on already active link	242005	High	Minor	This message is generated as a part of Calling ID validation of incoming ISDN calls, i.e., Switched Services find that the link is already active then it generates this report.		There is confusion on the link state between Switched Services and the ISDN. Boot the node, or the ISDN port, to correct this problem.
SS RUN-TIME PARAMETER ERROR	242004	High	Critical	This alarm is generated only when DEBUG is on. It warns that Switched Services has received a parameter from NS that it does not recognize.		Corrective actions for this alarm depend what is causing this parameter error. Typically this could happen if the stack or memory is corrupted.
START of bop_bri_tx_ callsetup() : chan_num	241036	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
START of sdrvc_traitetbenrep ()	241038	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
State set to DISABLED in bop_bri_sm_shutdow n3()	241058	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
State set to DISABLED in bop_bri_sm_shutdow n4()	241059	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
State set to DISABLED in bop_ bri_cd_rr_disconn_m sg()	241055	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
State set to DISABLED in bop_bri_setup_rr_disconn_msg()	241054	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
State set to DISABLED in bop_bri_sm_shutdown()	241056	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
State set to DISABLED in bop_bri_init_chan_cbs()	241048	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
State set to DISABLED in bop_bri_sm_shutdown2()	241057	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
State set to DISABLED in bop_bri_tx_callsetup()	241049	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
State set to DISABLED in bop_bri_tx_disconn_msg()	241053	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
State set to DISABLED in bop_bri_tx_E_EiaShutdown()	241052	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
State set to DISABLED in bop_bri_validate_call ()	241050	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
State set to DISABLED in bop_bri_validate_call 2()	241051	Low	Normal	This message should never be displayed.		Contact your customer service representative if this alarm message is displayed.
STATION (n) - POSSIBLE DATA LOSS - *(controller address) (station address)*	110012	High	Major	This alarm indicates that packets, coming from the network, may have been lost. This could be caused either by a network failure or by the device failing to respond properly. The value *STATION (n)* identifies the station affected while *(controller address) (station address)* identify the hexadecimal addresses.		To correct this problem: a) Check the network connection, or b) Verify that the device is working correctly.
SW56K CALL DISCONNECTED	6016	Medium	Normal	This message indicates that a call was successfully disconnected.		This is an information message only. No corrective action is required.
SW56K FAILED TO DISCONNECT	6013	High	Critical	This message indicates that the RX circuit has failed to disconnect.	6007, 6008, 6010, 6016	Ensure that the RX circuit is correctly configured.
SW56K LINE IN SERVICE	6015	High	Normal	This message indicates that the RX circuit is available.		This is an information message only. No corrective action is required.
SW56K LINE NOT IN SERVICE	6014	High	Major	This message indicates that the RX circuit is not available.	6015	Ensure that the RX circuit is configured properly and is available.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
T1-<%d> - %s ALARM %s	283005	High	Major			Contact your customer service representative if this alarm is displayed.
T1E1DRV-<%d>: %s - %x hex	283010	Low	Major			Contact your customer service representative if this alarm is displayed.
T1E1DRV-<%d>: ERROR: CAUSE-%s	283002	High	Major			Contact your customer service representative if this alarm is displayed.
T1E1DRV-<%d>: L3L4mERROR FROM T1/E1 CARD, Cause : %d	283001	High	Major			Contact your customer service representative if this alarm is displayed.
T1E1DRV: INVALID EXECUTION. Line # %d	283027	Medium				Contact your customer service representative if this alarm is displayed.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
Telnet-Error: *(cause)*	257001	High		This alarm indicates that a Telnet error has occurred. The problem is identified in the *(cause)* value, as identified below: a) Invalid number of atcif sessions, connecting to CTP - ATCIF failure. b) Insufficient memory, atcif create failed - Not enough memory in the node. c) atcif module create failed - telnet failed to create the ATCIF module. d) Insufficient memory, telnet client create failed - Not enough memory in the node. e) Cannot allocate memory for Tel net-telnet_Init - Not enough memory in the node. f) Abort failed.exitting-tel_client - there is not enough memory in the node. g) Memory allocation failure-tel_client - there is not enough memory in the node.		If any of these alarm messages are displayed, reset the node, wait a short period of time, and retry the connection.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
Telnet-Error: *(cause)* (Cont'd)	257001	High		h) Bad negotiation-TNR_SB - an unsupported negotiation command arrived from the remote side. If this alarm is ignored, Telnet malfunctions. i) Bad negotiation-TNR_TTYTYPE - an unsupported negotiation command arrived from the remote side. If this alarm is ignored, Telnet malfunctions. j) Couldnt post a receive to TCP-tel_sig_cread - a TCP failure has occurred. k) Bad negotiation-TNR_DONT - an unsupported negotiation command arrived from a remote site. If this alarm is ignored, Telnet will continue to malfunction. l) Couldnt post a receive to TCP-tel_cpost_buf - a TCP failure has occurred. m) Memory allocation failure. Operation aborted - Not enough memory in the node. n) Couldnt post a receive to TCP-telcommon - TCP failure.		If any of these alarm messages are displayed, wait a short period of time and retry the connection.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
Telnet-Error: *(cause)* (Cont'd)	257001	High		o) Memory allocation failed in tel_addtsk - Not enough dynamic memory in the node. p) Cannot route to CTP-tel_start a ROUT failure has occurred. q) Packet allocation failed-tel_sread - there is not enough buffers in the node. r) Bad negotiation-TNC_SB/TNC_SE - an unsupported negotiation command arrived from the remote side. If this alarm is ignored, Telnet malfunctions. s) Server not up because of addtsk failure - Not enough dynamic memory in the node.		If any of these alarm messages are displayed, wait a short period of time and retry the connection.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
Telnet-Internal Error: *(cause)*	257000	Low	Warning	This alarm indicates that a Telnet error has occurred. The problem is identified in the *(cause)* value, as identified below: a) listQ full-telnet_Packet - The packet queue is full, releasing the new packet. b) Client, Couldnt do a tcp_send - The client is unable to send data, aborting. c) Client, Couldnt do a tcp_sendbuf - The client is unable to send data, aborting. d) Bad state in tcp_crdata - Wrong state encountered by the client while processing data character, aborting. e) Ring Buffer Full-tel_crdata - Ring buffer became full while processing command character, aborting. f) Reached cabort in a CLOSED state - Already in CLOSED state while aborting the connection. g) Reached cfclose in a CLOSED state - Local host is already in CLOSED state while foreign host is closing the connection.		If any of these alarm messages are displayed, wait a short period of time and retry the connection.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
Telnet-Internal Error: *(cause)* (Cont'd)	257000	Low	Warning	h)pck_Append_Char failed-tel_srdata - Cannot append the character to the end of packet while processing data character, aborting. i) Reached ctmo in a CLOSED state - Already in CLOSED state while processing the timeout upcall. j) Local queues full in Telnet - Local queue full, cannot add the element 'data' in the queue. k)tcp_listen() failed-tel_sattempt - Server failed attempting to listen for incoming connections. This might be due to insufficient memory. l) Server, Couldnt do a tcp_send - The server is unable to send data, aborting. m)Server, Couldnt do a tcp_sendbuf - The server is unable to send data, aborting.		If any of these alarm messages are displayed, wait a short period of time and retry the connection.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
Telnet-Internal Error: *(cause)* (Cont'd)	257000	Low	Warning	n) tnp->temp_packet != NULL - No space free for saving the packet while CTP is in flow control, aborting. o) Bad state in tcp_srdata - Wrong state encountered by the server while processing data character, aborting. p) Bad negotiation received-tel_srdnt - Bad negotiation received, aborting.		If any of these alarm messages are displayed, wait a short period of time and retry the connection.
TERMINAL (%d) INITIALIZATION ON BRI INT. %d COMPLETED	278011	Medium	Normal			Contact your customer service representative if this alarm is displayed.
TERMINAL (%d) INITIALIZATION ON BRI INT. %d FAILED: %d	278004	Medium	Critical			Contact your customer service representative if this alarm is displayed.
TFR - CONNECTION ESTABLISHED WITH OTHER TFR	298002	Low	Normal	This message indicates that the TFR has established a connection with the other TFR in the network.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TFR - CONNECTION FAILURE WITH OTHER TFR *(cause)*	298003	Medium	Major	This alarm indicates a TFR connection has failed. The cause of this failure is identified by the *(cause)*. Causes may include: • The connection that was in place, with the other TFR, has been broken. • All attempts to establish a connection with the other TFR have failed.		Complete the necessary procedure to correct this alarm: • If this alarm has been generated because the TFR-TFR connection has come down, contact the net work operator to investigate the cause of the failure. • If this alarm has been generated because all connection attempts have failed, check if the 'Other TFR Address' configured in the TFR Record is valid. Also con tact the network operator to investigate if any network problems exist.
TFR - FRAME DISCARDED	298005	Low	Warning	This alarm indicates that a TNPP data frame, with the Source and Destination Addresses specified could not be forwarded to any connection.		Verify that the Destination Address is valid and is configured in the Paging Destination Table. **■ Note** If the problem occurs frequently, there could be an issue with the link/node capacity. Contact your customer service representative.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TFR - QUEUE OVERFLow	298006	Low	Major	This report is generated only when DEBUG is on. It indicates that queue used to store TNPP data frames before processing is overflowing.		Complete these steps to clear the alarm: a) Increase the Queue Size in the TFR record to correct this alarm condition. b) Contact your customer service representative if the problem persists.
TFR - RECEIVED INCOMPLETE FRAME	298007	Low	Warning	This report indicates that an incomplete TNPP data frame was received and has been discarded.		This is an information message only. No corrective action is required.
TFR - UNKNOWN CALLER	298004	Medium	Minor	This message indicates that the TFR received a call request with an invalid Protocol Identifier.		There are no specific corrective actions to clear the cause of this message. This problem may be caused by an incorrect configuration in some other node.
TFR BOOT FAILURE	298001	High	Normal	This alarm indicates that a TFR record boot cannot be performed. This failure will have occurred because either the record does not exist or a parameter requiring node boot has been modified.		Complete these steps, to correct this alarm: a) Configure a TFR record if no record exists and then boot. b) Perform a node boot if a parameter requiring node boot has been modified.
TFRI - CONNECTION ESTABLISHED WITH TFR FOR THE PT *(n)*	299003	Low	Normal	This message indicates that an X.25 connection between a TFRI and a TFR is active for the paging terminal number configured in TDLC port record. The value *(n)* identifies the Paging terminal number.		This is an information message only. There are no corrective actions necessary.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TFRI - CONNECTION FAILURE WITH TFR FOR PT *(n)* - *(cause)*	299004	Medium	Major	This message indicates that an X.25 connection between a TFRI and TFR has failed for the Paging terminal. The value *(n)* identifies the Paging terminal number and the *(cause)* of this alarm is also displayed.		To correct this problem perform one of these activities: a) Check for the Autocall Mnemonic. b) Check the integrity of the X.25 connection. c) Check the routing table entry to ensure that the correct routing information is available.
TFRI - FRAME DISCARDED *(s)* - *(d)*	299005	Low	Warning	This message indicates that TNPP frames are being rejected. This can occur when: a) the X.25 connection is not up b) the TNPP frame format is incorrect The value *(s)* indicates the source address and *(d)* indicates the destination address.		To correct this problem, check the integrity of the X.25 connection. **Note** Refer to the *X.25 Configuration Basics Manual* (Part Number T0107) for additional information.
TFRI - INSUFFICIENT MEMORY - INITIALIZED WITHOUT DCP	299001	High	Critical	This is a warning message indicating that memory is not available to allocate Data Connection Protection (DCP), and that DCP is not available.		To correct this problem perform one of these activities: a) Reduce the number of TFRI connections. b) Reduce the size of the image. c) Increase the amount of memory in the node (provided that the Vanguard device supports this).

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TFRI - INSUFFICIENT MEMORY - INITIALIZATION FAILED	299000	High	Critical	This message indicates that no memory is available for use in allocating the context of a TNPP Frame Router Interface (TFRI).		To correct this problem perform one of these activities: a) Reduce the number of TFRI connections. b) Reduce the size of the image. c) Increase the amount of memory in the node (provided that the Vanguard device supports this).
TFRI - SOCKET REGISTRATION FAILED	299006	High	Warning	This message indicates that TDLC Port and TFRI registration have failed.		This is an information message only. There are no corrective actions necessary.
TFRI BOOT FAILURE *(cause)*	299002	High	Normal	This message indicates that you have modified the configured value of a parameter requiring a Node-boot. The *(cause)* of this alarm will also be displayed. **■ Note** Parameters requiring a node boot after modification are identified in the appropriate Feature Protocol Manuals.		To correct this situation a) Boot the Node. b) Recover the old value for the Node boot parameter.
TFTP:	198010	High	Normal	This alarm indicates that a file is either too big or the wrong file type. It can also indicate that the file is of a type which you are unauthorized to load.		Check error and correct accordingly.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TFTP: CMEM access failure\r\n%s	198001	High	Major	This alarm indicates a failure to access CMEM during TFTP transfer operation. This is probably due to insufficient buffers available to hold CMEM record in the node.	198000	To correct this problem: a) Reduce current node activity or completely stop node to increase available buffers. b) Add more DRAM to node.
TFTP: Error in software image file	198007	High	Critical	This alarm indicates that an image was received that does not match its correct size.		To correct this problem: a) Check image format. b) Check that image have been created correctly.
TFTP: failure	198012	High	Critical	This alarm indicates that a command line TFTP transfer failure.		To correct this problem: a) Check IP address b) Check ethernet cable. c) Free up node resources and restart operation
TFTP: Flash erasure failure	198008	High	Critical	This alarm indicates that a timer expired before FLASH was erased.		This is a system problem that must be reported to Customer Service.
TFTP: Flash write failure	198009	High	Critical	This alarm indicates that a timer expired before FLASH could be written.		This is a system problem that must be reported to Customer Service.
TFTP: Local transfer failure\r\n%s\r\nError text = %s\r\nError code = %d	198002	High	Major	This alarm indicates a failure in flash to flash local transfer.	198000	Reduce node activity and restart TFTP operation. If this problem persists, contact your customer service representative.
TFTP: Operation successful	198000	High	Normal	This message indicates that a TFTP command has been successfully executed.		This is an information message only. No corrective actions are necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TFTP: partial success	198011	High	Normal	This alarm indicates that a transfer was partially completed via the command line interface.		This is an information message only. No corrective actions are necessary.
TFTP: Remote transfer failure\r\n%s\r\nError text = %s\r\nError code = %d	198003	High	Major	This alarm indicates a failure in flash to flash remote transfer.	198000	To correct this problem: a) Check IP addresses. b) Check ethernet connection. c) Free up node resources and restart
TFTP: Software download already in progress	198006	High	Normal	This alarm indicates that you have tried to download software in the middle of download operation.		Wait for download to finish.
TFTP: System failure\r\n%s	198004	High	Major	This alarm indicates that a Disconnect was received in the middle of software download operation.	198000	Boot the node and restart operation.
TFTP: UDP registration failure\r\n%s	198005	High	Major	This alarm indicates that a UDP port can not be registered. Possible causes are: • Port number error. • Network unavailable, IP not running. • Out of memory to complete operation. • Port Already registered. • Maximum number of ports already registered.		To correct this problem: a) Check IP addresses. b) Check cable. c) Free up node resources and restart.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
THE NUMBER OF SWITCHED SERVICE ENTRIES	242006	High	Critical	This message is generated when a new Switched Services entry is added or an existing one is deleted and a Tables Boot is performed.		Boot the node to correct this problem.
THE PEER'S NAME EXCEEDS16 CHARACTERS	270014	Medium	Critical	This alarm indicates that the name of the remote node received during authentication is longer than the maximum supported length.		Reconfigure the remote equipment to send a name no longer than 16 characters.
TN3270: *Device* CANNOT BOOT; ENTRY NOT DEFINED	419007	High		An attempt was made to boot a device that does not exist in configuration memory.		Check the spelling of the device that had been entered when invoking the Boot Command.
TN3270: *device* Device Active for *n.n.n.n*	419001	High		The remote TN3270 Server Subsystem Device *device* has established a TN3270 session with a TN3270 emulator running on a remote computer with an IP address of *n.n.n.n.*		None.
TN3270: *device* Device Inactive for *n.n.n.n*	419004	High		The TN3270 session between the Remote TN3270 Server Subsystem Device *device* and the TN3270 emulator running on the remote computer with an IP address of *n.n.n.n.* has terminated.		This is typically a normal condition. Determine if the user at the remote computer has terminated the TN3270 Emulator Program on the remote computer. If not, check if the session was terminated by the Host System Operator or if there was a network outage.
TN3270: *device* - LU BOOT COMPLETE	419008	High		The Remote TN3270 Server Device *device* boot completed.		None.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TN3270: *device* Session Active for *n.n.n.n.*	419002	High		The remote TN3270 Server Subsystem Device *device* has established an LU to LU session with the Host Computer. The IP address of the remote computer associated with this LU to LU session is *n.n.n.n.*		None.
TN3270: *device* Session Inactive for *n.n.n.n*	419005	High		The LU to LU session between the Remote TN3270 Server Subsystem Device *device* and the Host Computer has terminated. This LU to LU session had been associated with the remote computer, running a TN3270 Emulator Program, with an IP address of *n.n.n.n*		This is typically a normal condition.Determine if the user at the remote computer has terminated the TN3270 Emulator Program on the remote computer or if the session was terminated by the Host System Operator or if there was a network outage.
TN3270: *device* TCP Session Closed for *n.n.n.n*	419006	High		The TCP session between the Remote TN3270 Server Subsystem Device *device* and the TN3270 emulator, running on the remote computer, with an IP address of *n.n.n.n* has terminated.		This is typically a normal condition. Determine if the user at the remote computer has terminated the TN3270 Emulator Program on the remote computer. If not, check if the session was terminated by the Host System Operator or if there was a network outage.
TN3270: Server Parameters BOOT COMPLETE	419009	High		The Remote TN3270 Server Parameters Table boot completed.		None.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TN3270: TCP Session Opened for *n.n.n.n.*	419003	High		The remote TN3270 Server Subsystem has established a TCP session with a TN3270 emulator running on a remote computer with an IP address of *n.n.n.n.*		None.
TOPOLOGY STABLE	137004	Medium	Normal	The spanning tree has been determined by the spanning tree algorithm within the Vanguards in the network.		It is normal that the spanning tree algorithm will determine the spanning tree.
TOPOLOGY UNSTABLE	137003	Medium	Major	A link or connection in the spanning tree became disconnected. Within the Vanguards in the network a new spanning tree is being determined by the spanning tree algorithm.		The spanning tree algorithm running within the Vanguards in the network will re-determine the spanning tree.
ToW: NOT ACTIVE, ENTRY NOT FOUND IN CMEM	294001	Low	Critical	This alarm indicates that the ToW feature is not active; an entry was not found in CMEM.		This alarm is displayed only when the DEBUG function is turned on, and is used for advanced system diagnosis.
ToW: NOT ACTIVE, INITIALIZED TO DEFAULT	294002	Low	Major	This alarm indicates that the ToW feature is not active; and was initialized to its default entry.		This alarm is displayed only when the DEBUG function is turned on, and is used for advanced system diagnosis.
ToW: NOT ENOUGH MEMORY	294000	High	Critical	This alarm indicates that there is insufficient memory available in the node.		Contact your customer service representative.
ToW:ACTIVE	294003	Low	Minor	This alarm indicates that the ToW feature is active.		This alarm is displayed only when the DEBUG function is turned on, and is used for advanced system diagnosis.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TPA *(ident)* - CONNECTION UP	324001	High	Normal	This message indicates that X.25 connection between the TPA and the remote host is up. The *(ident)* value identifies the TPA involved.		This is an information message only. There are no corrective actions necessary.
TPA *(ident)* - CONNECTION DOWN *(cause)*	324002	High	Major	This message indicates that an X.25 connection towards a remote host is down. The *(ident)* value identifies the TPA involved, while the *(cause)* value indicates one of these causes of the problem: • Idle timeout • TPDU slot is disabled • TPDU Slot is booted • Clear request is received from the host	324001	This is an information message only. There are no corrective actions necessary.
TPA *(ident)* - CONNECTION IS IN PROGRESS	324003	Low	Normal	This message indicates that a connection towards a remote host is in progress. The *(ident)* value identifies the TPA involved.		This is an information message only. There are no corrective actions necessary.
TPA *(ident)* - MAXIMUM AUTOCALL ATTEMPTS FAILURE,	324006	Medium	Major	This alarm indicates that the Autocall establishment towards a remote host has failed. The *(ident)* value identifies the TPA involved.		Perform these checks to determine the cause of this failure and then correct as necessary: a) Check the Autocall mnemonic configuration for this TPA. b) Check for X.25 link c) Check for the routing table configuration

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TPA *(n)* - CONNECTION DOWN *(cause)*	330000	High	Major	This message indicates that the UDP connection is down. The value *(n)* identifies which TPA is affected while *(cause)* will indicate one of the following reasons for the failure: • TPDU slot boot • TPDU slot disable		This is an information message only. There are no corrective actions necessary.
TPA(FRA)-*(s)* - CLEARING CALL, BAD RESPONSE	344007	High	Warning	This alarm indicates that an existing call has been cleared due to a bad response from the remote host. The value *(s)* identifies the slot number affected.		This is an information message only. There are no corrective actions necessary.
TPA(FRA)-*(s)* - CONNECTION DOWN *(cause)*	344001	High	Major	This message indicates the FRA connection towards the remote host is down. The value *(s)* identifies the slot number affected while *(cause)* gives the causes of the problem, as indicated below: • Slot boot • Slot disable • CLR Request • Idle timer	344000	This is an information message only. There are no corrective actions necessary.
TPA(FRA)-*(s)* - CONNECTION IS IN PROGRESS *(cause)*	344002	Low	Normal	This message indicates that a connection towards a remote host is in progress. The value *(s)* identifies the slot number affected.		This is an information message only. There are no corrective actions necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TPA(FRA)-*(s)* - CONNECTION UP	344000	High	Normal	This indicated the FRA connection between the TPA and the remote host is UP. The value *(s)* identifies the slot number affected.		This is an information message only. There are no corrective actions necessary.
TPA-FRA, IDCM NOT UP	344006	High	Major	This alarm indicates that the initialization of a TPA FRA has failed. Possible reasons for this failure are: • Module IDCM/TGO not present in the image. • Memory is not available to initialize IDCM module.		To correct this problem, check the image contents for these modules. Rebuild the image including the IDCM and TGO modules. If this does not correct the problem, increase the memory in the node.
TPA-FRA, IDCM OR TGO DOES NOT EXIST	344005	High	Critical	This alarm indicates that the initialization of a TPA FRA has failed because the TGO or IDCM modules have not been configured in the image.		To correct this problem, check the image contents for the modules indicated and, if they are missing, rebuild the image including these modules.
TPA-FRA, NOT ENOUGH MEMORY	344004	High	Critical	This alarm indicates that there is not enough memory to support the TPA_FRA application.		To correct this problem either add more DRAM to the node or reduce the configuration in the node to create more available memory.
TPA-UDP, DOES NOT EXIST	330002	High	Critical	This alarm indicates that the TPA FRA has failed to initialize because the UDP module does not exist in the software image loaded into the node.		To correct this problem, check the image contents for the UDP module, and then rebuild the image including the UDP module if it was missing.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TPA-UDP, REGISTRATION WITH SIP FAILED	330004	High	Critical	This alarm indicates that registration with the SIP (Slim IP) module has failed.		Verify that the SIP module exists in the image you are using. If it does not, use the Vanguide applications to build and install the correct software image for your application.
TPA-UDP, REGISTRATION WITH UDP FAILED	330003	High	Critical	This alarm indicates that registration with the UDP has failed.		Two possible solutions to this problem are: a) Verify that your software image includes IP. b) The Maximum Number of UDP Clients have already registered. Wait until one of the clients is free and then reregister.
TPA2780 CONNECTED	343000	High	Normal	This message indicates that a TPA2780 port either received/ accepted a call or sent a call request and it was accepted.		This is an information message only. There are no corrective actions necessary.
TPA2780 DISCONNECTED	343001	High	Normal	This message indicates that a TPA2780 port either disconnected a call, or the call was disconnected.		This is an information message only. There are no corrective actions necessary.
TPA3270 CONNECTED	316000	High	Normal	This message indicates that the TPA3270 has received a call and accepted it, or sent a call request and it was accepted.		This is an information message only. There are no corrective actions necessary.
TPA3270 DISCONNECTED	316001	High	Normal	This message indicates that the TPA3270 has disconnected the call, or the call was disconnected.		This is an information message only. There are no corrective actions necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TPR SLOT *(s)* BOOT COMPLETE	317001	High	Normal	This message indicates that the TPDU Router Slot boot process is completed successfully. The value *(s)* identifies the slot number affected.		This is an information message only. There are no corrective actions necessary.
TPR SLOT *(s)* DISABLED	317008	High	Warning	This alarm indicates that the enabled TPDU Router slot has been disabled via the CTP port. The value *(s)* indicates the TPR slot that has been disabled.	317007	This is an information message only. There are no corrective actions necessary.
TPR SLOT *(s)* ENABLED	317007	High	Normal	This alarm indicates that the disabled TPDU Router slot has been enabled via the CTP port. The value *(s)* indicates the TPR slot that has been enabled.		This is an information message only. There are no corrective actions necessary.
TPR-BOOT FAILURE - NUMBER OF SLOTS CHANGED	317002	High	Critical	This message indicates that the parameter “Number of Slots” value is changed and that a node boot is required.		To correct this problem you can do one of two things: a) Boot the node or, b) Reconfigure the parameters back to their old values.
TPR-FWD Packet for DEAD slot *(s)* arrived	317009	Low	Critical	This message indicates that the TPDU Router has received a packet for a slot that does not exists. The value *(s)* indicates the slot affected.		To correct this problem you can do one of two things: a) Check the TPDU Router configuration b) Check the TPA configuration for correct addresses.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
TPR-INIT *(s)* TPA module *(d)* does not exist	317005	High	Critical	This alarm indicates that a module is not present in the image downloaded to the node and, therefore, the TPDU Router slot cannot be initialized. The value *(s)* indicates the slot affected and *(d)* indicates the module affected.		Download the image with the required TPA module
TPR-SLOT *(s)* BOOT FAILURE - SLOT TYPE CHANGED	317003	High	Critical	This message indicates that the TPDU Router slot boot has failed because the parameter "Slot Type" is changed. Changes to this parameter require a Node boot to take affect. The value *(s)* identifies the slot number affected.		To correct this problem you can do one of two things: a) Boot the node or, b) Reconfigure the parameters back to their old values.
TRANSMITTER INACTIVITY TIMEOUT	130003	Medium	Minor	The transmitting end of a connection is not able to transmit frames within a 15 second timeout period. The terminal could be blocking the transmission of these frames.		Rebooting the port may correct this problem.
TX MESSAGE QUEUE OVERFLOW	130002	Medium	Major	This message indicates that the speed at which the transmitting device is operating at does not match that which the destination device is receiving. The result of this mismatch in device speeds is that the queue on the originating, or transmitting, end overflows.		Reconfigure congestion parameters as required.
UDP Registration Failure	347000	High	Major			Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
UNABLE TO COMPRESS CMEM - CMEM NOT WRITTEN	4002	High	Critical	This alarm indicates that there is insufficient memory available to compress the last configuration into CMEM.		Delete redundant or unnecessary entries from your configuration. **■Note** Contact your customer service representative if you are unsure of what can be deleted.
UNASSIGNED LCN	46007	Medium	Minor	This alarm indicates that a packet has been received on a LCN which has not been configured.	46000	Check the PVC and SVC configurations in the port record (at both ends) and ensure that they are compatible.
UNESCAPED CHAR FOUND	308024	Low	Minor	This alarm indicates that a Control character has been sent without an escape character and that a frame has been discarded.	308000	Correct the software in the remote node OR packet was corrupted on the network.
UNEXPECTED FRAME	308025	Low	Minor	This alarm indicates that a frame is beginning with other than LINK/ACK character, and a frame has been discarded.	308000	Correct the software in the remote node OR packet was corrupted on the network.
UNEXPECTED INTERRUPT, SR/ VECTNUM $%6.6x	19016	High	Critical			Contact your customer service representative if this alarm is displayed.
Unreachable network *(net)* - in entry *(p)*	202001	High	Major	This alarm indicates that the next hop configured in the Static Table is not a directly attached network (*(net)* value) at the mentioned position *(p)* value.		Reconfigure the Static Table entry to have the next hop on a directly attached net or add an interface corresponding to the next hop address
UPDATING SOFTWARE	105004	High	Warning	This message indicates that a RAM-to-RAM transfer is taking place.	105002, 105005, 105014	This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
USER MESSAGE LOST	206000	Medium	Warning	This message indicates that the message queue is full and another message has been discarded. The cause of this alarm may be that too many inputs have been entered with waiting for system responses.		Wait until all previous inputs have been processed before keying in new inputs.
V.25 BIS CALL FAILURE - *(cause)*	6004	High	Minor	This alarm indicates that a call could not be established. The value *(cause)* indicates the type of error that has occurred.		Refer to the V.25 bis documentation to determine reason for call failure. The BSC2780/3780 protocol documentation contains information on Vanguard implementation of the V.25 *bis* protocol. **Note** Refer to the Vanguard *SNA Feature Protocols Manual* (Part Number T0101) for additional information.
V.25 BIS ERROR - *(cause)*	6005	High	Minor	This message indicates that the attached device has reported a V.25 *bis* protocol failure. The value *(cause)* identifies the cause of this error.		Verify that the device connected to the physical port is properly configured for V.25 *bis*.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
V.25 BIS PROTOCOL MISMATCH	6003	High	Minor	This message indicates that a device attempted to communicate with a port that is not configured for the V.25 *bis* protocol.	6002	To correct this problem: a) Verify that the device connected to the physical port is configured for V.25 *bis* protocol. b) Reconfigure this device if necessary, to support V.25 *bis*.
VIRTUAL MAPPING ERROR, CAUSE: %s	280013	Low	Critical	This alarm indicates that the Virtual Mapping Table has been configured for SO Special but the SO card is not installed in the correct slot.	280005	Check the configuration of the Virtual Mapping Table and the location of the SO Card to ensure that they are both correct.
VIRTUAL MAPPING ERROR, CAUSE: %s	280012	Low	Critical	This alarm indicates that no entry, for this virtual voice port, has been found in the Virtual Port Mapping Table.	280005	Check the voice port number and the Virtual Port Mapping Table configuration to ensure that the port has been configured.
VOICE RECORD CONVERSION	280016	High				Contact your customer service representative if this alarm is displayed.
VOICE RECORD CONVERSION COMPLETED	280014	High		This message indicates that a pre-5.2 version of CMEM has been updated to latest CMEM version.		This is an information message only. No corrective action is required.
VOICE RECORD CONVERSION FAILED	280015	High				Contact your customer service representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
VOICE SWITCHING RECORD CONVERSION COMPLETED	304001	High	Normal	This message indicates that the Voice Switching Table CMEM record (pre-5.0 release) has successfully been converted to a Release 5.x format.		This is an information message only. There are no corrective actions necessary.
VOICE SWITCHING RECORD FAILED CONVERSION	304000	High	Major	This alarm indicates that a problem was detected while converting, a pre-Release 5.0 Voice Switching Table CMEM record, to a post Release 5.0 format.	304001	Check the Voice Switching Table record and re-add the necessary files.
VOICE-SIGNALING TRACE/DEBUG:	281006	Medium	Normal	This report is enabled via the voice port configuration and is used to aid in debugging a voice signaling protocol issue.		This is an information message only. No corrective action is required.
%s DSP #%d LAST VSM RESPONSE: %02X %02X %02X %02X %02X	281018		Critical	This report is generated when the handshake to the DSPM-xx card times out. The information is displayed in hex format and is designed to be interpreted by engineering.		When this alarm is generated, it should be captured and sent to engineering for analysis.
VOICE-%d %s	281019		Major	Although this report is in the report table, it is not utilized anywhere in the code. It is never displayed.		This is an informative message only. No corrective action is required.
VOICE-%d SIGNALING TRACE: %s	281007	Medium	Minor	This report is enabled via the voice port configuration and is used to aid in debugging a voice signaling protocol issue.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
VOICE-*(x)* VSM COMMAND: EID *(x)*, OPCODE *(x)*, PAYLOAD *(x)*	281014	Medium	Normal	This report is enabled via the voice port configuration and is used to aid in debugging a voice signaling protocol issue.		This is an information message only. No corrective action is required.
XLB MODULE INITIALIZED	321001	High	Normal	This message indicates that Translational Bridging must be initialized and is only displayed if DEBUG is turned on.		This is an information message only. There are no corrective actions necessary.
qllc_packet %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	385031		Informa-tional	Received info from the WAN network.		This is an informative message only. No corrective action is required.
handle_pacing %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	385032		Informa-tional	Received info from AS/400.		This is an informative message only. No corrective action is required.
send_outbound %x	385033		Informa-tional	Sent a packet to WAN network.		This is an informative message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
purge_queue %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	385034		Informa-tional	Emptied remote work station packet queue.		This is an informative message only. No corrective action is required.
send_queued %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	385035		Informa-tional	Sent data from downstream packet queue.		This is an informative message only. No corrective action is required.
send_upstream %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	385036		Informa-tional	Sent data from upstream packet queue.		This is an informative message only. No corrective action is required.
%s - BAD CCBPTR IN %s, ch0ccbptr=%x, ccbptr=%x, ccb_index=%d, numchan=%d	46016		Informa-tional	Debug alarm indicating abnormal x25 channel information occurred and corrected		No corrective action.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
%s - PORT ERROR COUNT THRESHOLD	411000		Major	The combined number of CRC, parity, and overrun errors has exceeded a threshold value. The threshold value is configured as part of the node record. *PORT (n)* is the port number.		To correct this problem check the link status.
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	411001		Major	The port speed (%d) configured in the port record is not supported by the physical interface.		To correct this problem change the port speed in the port configuration.
%s - UNSUPPORTED RECEIVE BYTE COUNT: OPERATING WITH %d RX BYTE COUNT	411002		Major	This alarm indicates the number of bytes received is not supported.		Check the application to confirm that maximum frame size is less than the largest frame size in the node record.
%s - ERRONEOUS BOOLEAN PARAMETER: %s	411003		Major	This alarm indicates that the parameter is out of range.		Check the port configuration for out of range configured values.
%s - CLOCK SOURCE OVERRIDE	411004		Minor	This alarm indicates that the clock source configuration is not supported.		Check the port configuration for valid clock source settings.
%s - TX SANITY TIMEOUT	411005		Informa-tional	This alarm indicates that the transmitter did not receive a frame-transmitted indication.		Check the port cabling and configuration.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
%s - PORT ERROR COUNT >THRESHOLD	412000		Major	This alarm indicates that the combined number of CRC, parity and overrun errors exceeded a threshold value for port number %s.		Check the link status to correct this problem. Threshold value is configured as part of the node record.
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	412001		Major	The port speed (%d) configured in the port record for port %s is not supported by the physical interface.		Change the port speed in the port configuration.
%s - UNSUPPORTED RECEIVE BYTE COUNT: OPERATING WITH %d RX BYTE COUNT	412002		Major	This alarm indicates the number of bytes received is not supported.		Check the application to confirm that maximum frame size is less than the largest frame size in the node record.
%s - ERRONEOUS BOOLEAN PARAMETER: %s	412003		Major	This alarm indicates that the parameter is out of the permitted value range.		Check the port configuration for out of range configured files.
%s - CLOCK SOURCE OVERRIDE	412004		Minor	This alarm indicates the clock source configuration is not supported.		Check the port configuration for valid clock source settings.
%s - TX SANITY TIMEOUT	412005		Informa-tional	This alarm indicates that the transmitter did not receive frame-transmitted indication.		Check the port cabling and configuration.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
POSSIBLE RACE CONDITION IN SWITCH SERVICES - LINK ACTIVATE TIMER EXPIRED FOR %s	242020		Critical	This alarm indicates that there is not enough dynamic port creation heap to complete the boot.		Increase the dynamic port creation heap or delete some stations.
SOTCP Maximum Sessions Reduced to %d - Insufficient memory	331024		Critical	Insufficient memory for SOTCP to allocate all configured sessions. The number of sessions is reduced to %d.		Contact Customer Service.
SOTCP-%dC%d - Routing loop or maximum hop count exceeded.	331025		Informa-tional	SOTCP detects a routing loop in your configuration, or the number of hops in the node record is exceeded.		Correct entries in the route selection table to avoid a routing loop. If the maximum of 15 hops is exceeded, reduce the number by changing the routing configuration or increasing the hops count.
SOTCP-%sC%s - Routing loop or maximum hop count exceeded.	331026		Informa-tional	SOTCP detects a routing loop, or the maximum number of 15 hops is exceeded.		Correct entries in the route selection table to avoid a routing loop. If the maximum of 15 hops is exceeded, reduce the number by changing the routing configuration of increasing the hops count.
SOTCP Boot Failed: %s	331027		Critical	SOTCP cannot boot. This alarm is generated if SOTCP is booted and dynamic boot is not supported.		Warm boot the node.
SOTCP Boot failed - Insufficient memory	331028		Critical	SOTCP could not get enough memory while booting.		Retry. If the alarm persists, contact Customer Support.
SOTCP Dynamic Boot Started	331029		Critical	SOTCP module boot (Dynamic boot is supported by the node).		No corrective action required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action *(continued)*
SOTCP Dynamic Boot Completed	331030		Critical	SOTCP Dynamic boot has been completed.		No corrective action required.
%s CALL ROUTING ERROR: %s	16021		Critical	A call to the destination has been cleared with Cause Code 00, diagnostic code 81 (decimal). The call is rerouted to other active ports going to the same destination based on the load balancing procedure. This report will be generated only when the Concord EPS rerouting feature is enabled.		No corrective action required.
rout_main: Packet Semaphore Locked %s: Event: %s, Pck Addr: 0x%x	16022		Informa-tional	The packet semaphore is locked.		This is a debug report. Contact your representative if this report occurs repeatedly.
Packet pointer is NULL. Can not process the call request	16023		Minor	The call request packet is NULL.		Try the call once again. Contact your representative if the problem persists.
%s - INSUFFICIENT MEMORY FOR CONFIGURED STATIONS	112023		Critical	This alarm indicates that there is insufficient memory for configured stations.		Delete ports or stations that are not needed in the node and try again.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
PACKET_REPT_SEC_RELEASE_HIGH_ALL [REPORT_HIGH, "HIGH PRESERVING DBUFFER INTEGRITY ADDR: 0x%08X 0x%08X 0x%08X 0x%08X 0x%08X]	1300					Report this alarm to customer service.
BUFF_REPT_CORRUPTED_BUFFER	3001			REPORT_HIGH, "CORRUPTED BUFFER DROPPED 0x%08X 0x%08X 0x%08X 0x%08X 0x%08X]		Report this alarm to customer service.
BUFF_POOL_CORRUPTED	3002					Report this alarm to customer service.
TFTP Server Operation successful: *operation name* with *client IP address*	470000		High	This alarm message indicates the the Server operation i s successful.		This is an information message only. No corrective actions are necessary.
TFTP Server Enabled on port: *port number*	470005		Medium	This alarm message indicates the server is enabled on the port *(n)*.		This is an information message only. No corrective actions are necessary.
TFTP Server Disabled on port: *port number*	470006		Medium	This alarm message indicates the server is disabled on the port *(n)*.		This is an information message only. No corrective actions are necessary.
TFTP Server Image Downloading Start with *(file name)* to *(client IP address)*	470008		Medium	This alarm message indicates that TFTP Server Image downloading is started.		This is an information message only. No corrective actions are necessary.

Alarm Text	***Trap No.***	***Priority***	***Severity***	***Description***	***Cleared By:***	***Corrective Action*** *(continued)*
TFTP Server CMEM Downloading Start with *(file name)* to *(client IP address)*	470009		Medium	This alarm message indicates that TFTP Server CMEM downloading is started.		This is an information message only. No corrective actions are necessary.
TFTP Server Access Violation with *(file name)* from *(client IP address)*	470011		Medium	This alarm message indicates that there is a TFTP Server Access Violation.		This is an information message only. No corrective actions are necessary.
Digital Cert Gen Error			Medium	This message indicates a Digital Certificate general error message.		This is an information message only. No corrective actions are necessary.
Cannot Connect to CA			High	This alarm message indicates that you cannot setup a TCP connection with the CA.		Contact Customer Service.
Not enough memory for CRL			High	This alarm message indicates that there is not enough memory for a CRL file.		Contact Customer Service.
Certificate expires within one month			Medium	This alarm indicates that the operator the certificate is going to will expire within one month.		This is an information message only. No corrective actions are necessary.

Chapter 11
Vanguard 7300 Alarms and Reports

Overview

Introduction

This chapter describes Vanguard 7300 alarm messages and informational notices and reports. The alarms and reports are organized in numerical order by error code.

7300 Alarms

This Alarms and Reports section describes all Vanguard 7300-specific alarm and report messages generated by the Vanguard Applications Ware. A corrective action for each alarm and message suggests what to do when an unexpected error occurs when using any of the Applications Ware licenses on Vanguard 7300 products.

Alarms

An alarm message identifies a change of state in either the node itself or in the Applications Ware running on that node. An alarm message consists of a numeric trap number error identifier, a severity code, and a brief text descriptor.

Report

A report is an informational notice displayed by Applications Ware when specific network events take place. In most cases, a report requires no corrective action.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
NODE BOOT DELAYED DUE TO LAST GASP PROCESSING	2010		Critical	Node boot is delayed more than 10 seconds waiting CMEM and Images save to complete.		No corrective action - Informational due to the extended wait interval.
NODE BOOT CONTINUING - LAST CMEM CHANGE MAY BE LOST	2011		Critical	Node boot is delayed for 60 seconds; the node proceeds with booting.		When the node reboots, confirm the last configuration changes are saved.
%s rescued msg #%d\r\n%x/ %x/%x %x/%x	9002		Critical	Diagnostic indicating the system has recovered from an error condition.		Forward these alarms to Customer Service for evaluation.
%s rescued msg #%d\r\n%x:%x %x:%x %x:%x %x:%x %x:%x	9003		Critical	Diagnostic indicating the system has recovered from an error condition.		Forward these alarms to Customer Service for evaluation.
Packet pointer is NULL. Can not process the call request	16021		Informa-tional	Debug alarm indicating missing information in call-request packet.		No Action.
IBEX INIT FAILURE	19021	High	High	Critical failure of T1/E card to initialize, or communicate with host through the PCI bus.		Move the T1/E1 card to a different slot. Replace the T1/E1 card if there is no improvement.
%s - BAD CCBPTR IN %s, ch0ccbptr=%x, ccbptr=%x, ccb_index=%d, numchan=%d	46016		Informa-tional	Debug alarm indicating abnormal X.25 channel information corrected.		No Action.
%s WRONG POINTER PASSED IN	151007		Critical	A wrong pointer is passed to the SNMP module causing a node crash.		No corrective action. Informational only. Expect the node to crash.
%s - DYNAMIC ALL STATIONS BOOT STARTED	226009		Critical	All the stations are being de-allocated.		None.
%s - DYNAMIC ALL STATIONS BEING CREATED	226010		Major	All the stations are being allocated.		None.
%s - DYNAMIC ALL STATIONS BOOT COMPLETED	226011		Critical	Creation of all stations complete.		None.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
%s - DYNAMIC STATION BOOT STARTED	226012		Critical	Station %s is being de-allocated.		None.
%s - DYNAMIC STATION BEING CREATED	226013		Major	Station %s is being re-allocated.		None.
%s - DYNAMIC STATION BOOT COMPLETED	226014		Critical	%s station creation completed.		None.
INSUFFICIENT DYNAMIC MEMORY TO SUPPORT %s CONFIGURATION	226015		Critical	Not enough dynamic port creation heap to complete the boot.		Increase dynamic port creation heap and/or delete some stations.
%s - NO STATION CREATED	226016		Critical	No station configured for creation.		None.
*** %s WILL REQUIRE FRI BOOT OF PORT %d or\r\n	226018		Critical	Station %s requires port %d FRI station booted to connect.		Boot the associated FRI station.
%s ERR: SLAC DYNAMIC BOOT IN PROGRESS, TRY AGAIN WHEN COMPLETED	226019		Critical	Cannot boot; dynamic all stations boot is still in progress.		Wait for current boot to complete, then re-issue the boot.
POSSIBLE RACE CONDITION IN SWITCH SERVICES - LINK ACTIVATE TIMER EXPIRED for %s	242020		Critical	Link activation timer is a wrong state.		Retry. If the alarm persists, contact Customer Service.
OUTGOING CALL TO %s ON DSL %d	278021		Medium	This message indicates that there is an outgoing call. Trap 278021 is also used for these alarms in the Vanguard 6400 and 7300 Series. • INCOMING CALL FROM %s ON DSL %d, TrapNo=278021 • CALL IS DISCONNECTED FROM %s ON DSL %d: CAUSE %d, TrapNo=278021 • CALL IS DISCONNECTED FROM %s ON DSL %d: CAUSE %d, TrapNo=278021		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
ISDN VOICE: UNSUPPORTED MSG RCV'ed FROM CC, MSG_ID = 0x%x	278023		High	Unrecognized ISDN voice call signaling message received.		May not be fatal to call completion. Contact Customer Service.
%d: %s/%s->%s	278024		High	Status of ISDN voice call signaling progression.		This is an information message only. No corrective action is required.
ISDN VOICE ERROR: me_ccs_voice.c Line # %d	278025		High	ISDN Voice module has encountered a protocol/processing error.		Contact your representative if this alarm is displayed.
INVALID VOICE SIGNALING : PORT = %d : SIG. STATE = %d, STIMULUS = %d	278026		High	Current ISDN voice call signaling message is not handled in current call state.		Contact your representative if this alarm is displayed.
ISDN VOICE: %d CALL TO %s FROM %s FAILED ON PORT %d, %s	278027		High	The ISDN voice call attempt has failed. Destination may not be available, or a configuration error is preventing successful call completion.		Contact your representative if this alarm is displayed.
SOTCP Maximum Sessions Reduced to %d - Insufficient memory	331024		Critical	Insufficient memory for SOTCP to allocate all configured sessions. The number of sessions is reduced to %d.		Contact Customer Service.
SOTCP-%dC%d - Routing loop or maximum hop count exceeded.	331025		Informa-tional	SOTCP detects a routing loop in your configuration, or the number of hops in the node record is exceeded.		Correct entries in your network route selection table to avoid a routing loop. If the maximum of 15 hops is exceeded, reduce the number by changing the routing configuration or increasing the hops count.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
SOTCP-%sC%s - Routing loop or maximum hop count exceeded.	331026		Informa-tional	SOTCP detects a routing loop, or maximum number of 15 hops is exceeded.		Correct the entries in the route selection table to avoid routing loop. If the maximum of 15 hops is exceeded, reduce the number by changing the routing configuration or increasing the hops count.
SOTCP Boot Failed: %s	331027		Critical	SOTCP cannot boot. This alarm is generated if SOTCP is booted and dynamic boot is not supported.		Warm boot the node.
SOTCP Boot failed - Insufficient memory	331028		Critical	SOTCP could not get enough memory while booting.		Retry. If the alarm persists, contact Customer Service.
SOTCP Dynamic Boot Started	331029		Critical	SOTCP module boots. (Dynamic boot is supported by the node.)		No corrective action required.
SOTCP Dynamic Boot Completed	331030		Critical	SOTCP boot completes.		No corrective action required.
DOWNLOAD FAILED: VIRTUAL PORT - %d	339002		High	Virtual voice port failure related to DSP PMC modules.		Possible fault PMC and replacement is needed.
qllc_packet %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	385031		Informa-tional	Information received from the wide area network (WAN).		None. Informational only.
handle_pacing %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	385032		Informa-tional	Received information from AS/400.		None. Informational only.
send_outbound %x	385033		Informa-tional	Sent a packet to the wide-area network (WAN).		None. Informational only.
purge_queue %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	385034		Informa-tional	Emptied remote work station packet queue.		None. Informational only.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
send_queued %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	385035		Informa-tional	Sent data from downstream packet queue.		None. Informational only.
send_upstream %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	385036		Informa-tional	Sent data from upstream packet queue.		None. Informational only.
PORT (n) - ERROR COUNT > THRESHOLD	411000		Major	The combined number of CRC, parity, and overrun errors has exceeded a threshold value. The threshold value is configured as part of the node record. *PORT (n)* is the port number.		Check the link status to correct this problem.
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	411001		Major	The port speed (%d) configured in the port record is not supported by the physical interface.		Change the port speed in the port configuration.
%s - UNSUPPORTED RECEIVE BYTE COUNT: OPERATING WITH %d RX BYTE COUNT	411002		Major	The number of bytes received is not supported.		Check the application to confirm that maximum frame size is less than the largest frame size in the node record.
%s - ERRONEOUS BOOLEAN PARAMETER: %s	411003		Major	The parameter is out of range.		Check the port configuration for out-of-range configured values.
%s - CLOCK SOURCE OVERRIDE	411004		Minor	Clock source configuration is not supported.		Check the port configuration for valid clock source settings.
%s - TX SANITY TIMEOUT	411005		Informa-tional	The transmitter did not receive a frame-transmitted indication.		Check port cabling and configuration.
PORT (n) - ERROR COUNT > THRESHOLD	412000		Major	The combined number of CRC, parity, and overrun errors exceeded a threshold value for port number %s.		Check the link status to correct this problem. Threshold value is configured as part of the node record.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	412001		Major	The port speed (%d) configured in the port record for port %s is not supported by the physical interface.		Change the port speed in the port configuration.
%s - UNSUPPORTED RECEIVE BYTE COUNT: OPERATING WITH %d RX BYTE COUNT	412002		Major	The number of bytes received is not supported.		Check the application to confirm that maximum frame size is less than the largest frame size in the node record.
%s - ERRONEOUS BOOLEAN PARAMETER: %s	412003		Major	The parameter is out the permitted value range.		Check the port configuration for out-of-range configured values.
%s - CLOCK SOURCE OVERRIDE	412004		Major	Clock source configuration is not supported.		Check the port configuration for valid clock source settings.
%s - TX SANITY TIMEOUT	412005		Informa-tional	The transmitter did not receive frame-transmitted indication.		Check port cabling and configuration.
%s-%d RX Sanity Timer Expired	416000		High	The serial port receive has not received any frames.		This alarm is usually generated when the cable is disconnected. The user should check the cables.
PORT (n) - ERROR COUNT > THRESHOLD	423000		Major	The total error count (overrun errors plus underrun errors) for port %s exceeds the configured maximum Node Error Threshold parameter.		Generally this is a node hardware problem. Have the hardware serviced when convenient. No software-related corrective actions are indicated.
%s - UNSUPPORTED DATABITS: OPERATING WITH 8 DATABITS, NO PARITY	423001		Major	The configured number of data bits for port %s is less than 7, an unsupported configuration, and is defaulted to 8 Data Bits, No Parity.		Check the port configuration and modify the configuration as required.
%s - UNSUPPORTED BAUDRATE: OPERATING AT 9600 BPS	423002		Major	AutoSpeed is not supported on SMC ports (i.e. port 4 of LCIF) 9600 baud. The value % identifies the port.		Check the PAD port record configuration and modify it as required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
%s - UNSUPPORTED PARITY: OPERATING WITH 8 DATABITS, NO PARITY	423003		Major	The node %s does not support a port configuration of 8 Data Bits, No Parity.		Recheck the port configuration and change as required.
SG_NO_THROTTLE_TIMER	429000		Major	The Ethernet Driver bus timer could not be started.		To correct this problem, replace that Ethernet port PMC. See the *Vanguard 7300 Installation Guide* (Part Number T0185) for details.
SG_NO_INITIALIZATIO	429001		Major	See Trap 174001		
SG_CONFIGURATION_FAIL E	429002		Major	The Ethernet Driver encountered a failure when programming the Ethernet port.		To correct this problem, replace that Ethernet port PMC. See the *Vanguard 7300 Installation Guide* (Part Number T0185) for details.
SG_IA_FAILE	429003		Major	The Ethernet Driver encountered a failure when programming the Ethernet port's MAC Address.		To correct this problem, replace that Ethernet port PMC. See the *Vanguard 7300 Installation Guide* (Part Number T0185) for details.
SG_CONFIGURATION_TIME DOU	429004		Major	The Ethernet Driver encountered a time-out when programming the Ethernet port.		To correct this problem, replace that Ethernet port PMC. See the *Vanguard 7300 Installation Guide* (Part Number T0185) for details.
SG_NO_SUSPENSIO	429005		Major	The Ethernet Driver encountered a failure when programming the Ethernet port to suspend an operation.		To correct this problem, replace that Ethernet port PMC. See the *Vanguard 7300 Installation Guide* (Part Number T0185) for details.
SG_TX_LIST_PUT_FAILE	429006		Major	The Ethernet Driver could not place a transmit frame on the Ethernet transmit queue, because the transmit queue is filled.		Use Ethernet Port Statistics to confirm that the port is transmitting and the port has not lost carrier. Also, check the Ethernet connection for a bad clock or bad connection.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
SG_EXCESSIVE_TX_ERROR	429007		Major	The Ethernet Driver is experiencing a high rate of transmit errors.		Use Ethernet Port Statistics to confirm that the port is transmitting and the port has not lost carrier. Also, check the Ethernet connection for a bad clock or bad connection.
SG_LOSS_OF_CARRIE	429008		Major	The Ethernet Driver cannot detect a valid transmit clock.		Check the Ethernet connection and Ethernet for a bad connection.
SG_EXCESSIVE_RX_ERROR	429009		Major	The Ethernet Driver is experiencing a high rate of Receive Errors.		Use Ethernet Port Statistics to confirm that the port is transmitting and the port has not lost carrier. Also, check the Ethernet connection for a bad connection or excessive traffic rate.
SG_EXCESSIVE_TX_CLEA	429010		Major	The Ethernet Driver is no longer experiencing a high rate of Transmit Errors.		This is an information message only. No corrective action is required.
SG_LOSS_OF_CARRIER_CLEA	429011		Major	The Ethernet Driver is able to detect a valid transmit clock.		This is an information message only. No corrective action is required.
SG_EXCESSIVE_RX_CLEA	429012		Major	The Ethernet Driver is no longer having a high Receive Error rate.		This is an information message only. No corrective action is required.
SG_INVALID_STATE_ENABLE	429013		Major	Internal use only.		Contact your representative if this trap is displayed.
SG_INVALID_STATE_DISABLE	429014		Major	Internal use only.		Contact your representative if this trap is displayed.
SG_LOOPBACK_FAILE	429015		Major	Internal use only.		Contact your representative if this trap is displayed.
SG_TDR_FAILE	429016		Major	Internal use only.		Contact your representative if this trap is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
SG_NO_THROTTLE_TIMER	430000		Major	The Ethernet Driver bus timer could not be started.		To correct this problem, replace the Ethernet port's PMC or Chassis Card. Refer to the *Vanguard 7300 Installation Guide* (Part Number T0185) for details.
SG_NO_INITIALIZATIO	430001		Major	Internal use only.		Contact your representative if this trap is displayed.
SG_CONFIGURATION_FAIL E	430002		Major	The Ethernet Driver had a failure programming the Ethernet PMC		To correct this problem, replace the Ethernet port's PMC or Chassis Card. Refer to the *Vanguard 7300 Installation Guide* (Part Number T0185) for details.
SG_IA_559_FAILE	430003		Major	The Ethernet Driver encountered a failure when programming the Ethernet PMC MAC Address		To correct this problem, replace the Ethernet port's PMC or Chassis Card. Refer to the *Vanguard 7300 Installation Guide* (Part Number T0185) for details.
SG_CONFIGURATION_TIME DOU	430004		Major	The Ethernet Driver timed out when programming the Ethernet port.		To correct this problem, replace the Ethernet port's PMC or Chassis Card. Refer to the *Vanguard 7300 Installation Guide* (Part Number T0185) for details.
SG_NO_SUSPENSIO	430005		Major	The Ethernet Driver had a failure when programming the Ethernet port to suspend an operation.		To correct this problem, replace the Ethernet port's PMC or Chassis Card. Refer to the *Vanguard 7300 Installation Guide* (Part Number T0185) for details.
SG_TX_LIST_PUT_FAILE	430006		Major	The Ethernet Driver could not place a transmit frame on the Ethernet transmit queue; the Ethernet transmit queue is full.		Use Ethernet Port Statistics to confirm that the port is transmitting and the port has not lost carrier. Also, check the Ethernet connection for a bad clock or bad connection.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
SG_EXCESSIVE_TX_ERROR	430007		Major	The Ethernet Driver is experiencing a high rate of transmit errors.		Use Ethernet Port Statistics to confirm that the port is transmitting and the port has not lost carrier. Also, check the Ethernet connection for a bad clock or bad connection.
SG_LOSS_OF_CARRIE	430008		Major	The Ethernet Driver cannot detect a valid transmit clock.		Check for a bad Ethernet connection.
SG_EXCESSIVE_RX_ERROR	430009		Major	The Ethernet Driver is experiencing a high rate of Receive Errors.		Use the Ethernet Port Statistics for errors the port is receiving and check the Ethernet for a bad connection or excessive traffic.
SG_EXCESSIVE_TX_CLEA	430010		Major	The Ethernet Driver is no longer experiencing a high rate of Transmit Errors.		This is an information message only. No corrective action is required.
SG_LOSS_OF_CARRIER_CLEA	430011		Major	The Ethernet Driver detects a valid transmit clock.		This is an information message only. No corrective action is required.
SG_EXCESSIVE_RX_CLEA	430012		Major	The Ethernet Driver is no longer experiencing a high rate of Receive Errors.		This is an information message only. No corrective action is required.
SG_INVALID_STATE_ENABLE	430013		Major	Internal use only.		Contact your representative if this trap is displayed.
SG_INVALID_STATE_DISABLE	430014		Major	Internal use only.		Contact your representative if this trap is displayed.
SG_LOOPBACK_FAILE	430015		Major	Internal use only.		Contact your representative if this trap is displayed.
SG_TDR_FAILE	430016		Major	Internal use only.		Contact your representative if this trap is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
SG_CA_FAILE	430017		Major	The Ethernet Driver encountered a failure when programming the Ethernet PMC. The value *(cause)* identifies the cause of this alarm.		To correct this problem, replace the Ethernet port's PMC or Chassis Card. Refer to the *Vanguard 7300 Installation Guide* (Part Number T0185) for details.
SG_RX_LIST_ERRO	430018		Major	The Ethernet Driver encountered an error when receiving an Ethernet Packet. The Ethernet Driver recovers automatically from this error.		This is an information message only. No corrective action is required.
SG_TX_LIST_ERRO	430019		Major	The Ethernet Driver encountered a software error when transmitting an Ethernet Packet.		Contact your customer service representative if this alarm is displayed.
SG_LOCKUP_ERRO	430020		Major	The Ethernet Driver encountered an error condition in the Hardware Accelerator module. The Ethernet Driver recovers automatically from this error. The value *(cause)* identifies the reason for this alarm.		This is an information message only. No corrective action is required.
%s-%d Initialization Failed Cause Code: %x.	431000		Informa-tional	Serial Driver for slot %d failed to initialize the serial card. The value, %x is the reason code.		Run diagnostics on the card in this slot.
%s-%d Abort Frame Function Not Supported.	431001		Informa-tional	Serial Driver for port %d does not support this abort function.		None. Informational only.
%s-%d Data Scope Monitoring Function Not Supported.	431002		Critical	Serial Driver for port %d does not support this data scope function.		Disable the data scope for this port.
%s-%d Aborted Frames %d.	431003		Informa-tional	Serial Driver for port %d does not support this abort function with reason code %d		None. Informational only.
%s-%d TX Sanity Timer Expired %d.	431004		Informa-tional	Serial Driver for port %d keep alive timer expired with reason code %d.		None. Informational only.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
%s-%d Init Success a=%x b=%x.	431005		Informa-tional	Serial Driver Port Initialized successfully. a= Card Address b= port address		None. Informational only.
%s-%d RX Sanity Timer Expired.	431006		Informa-tional	The serial port receive has not received any frames.		This alarm is usually generated when the cable is disconnected. The user should check the cables.
PORT (n) - ERROR COUNT > THRESHOLD	432000		Major	The combined number of CRC, parity, and overrun errors exceeded the threshold value configured in the node record. *PORT (n)* is the port number.		Check the link status to correct this problem.
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	432001		Major	The port speed (%d) configured in the port record is not supported by the physical interface.		Change the port speed in the port configuration.
%s - UNSUPPORTED RECEIVE BYTE COUNT: OPERATING WITH %d RX BYTE COUNT	432002		Major	The number of bytes received is not supported.		Check the application to confirm that maximum frame size is less than the largest frame size in the node record.
%s - ERRONEOUS BOOLEAN PARAMETER: %s	432003		Major	The parameter is out the permitted value range.		Check the port configuration for out-of-range configured values.
%s - CLOCK SOURCE OVERRIDE	432004		Minor	Clock source configuration is not supported.		Check the port configuration for valid clock source settings.
%s - TX SANITY TIMEOUT	432005	Informa-tional	Informa-tional	The transmitter did not receive a frame-transmitted indication.		Check port cabling and configuration.
PORT (n) - ERROR COUNT > THRESHOLD	437000	Medium	Medium	This message indicates that the number of received errors, CRC for example, has exceeded the configured threshold. The value *PORT (n)* identifies the port effected.		Check your cables and cable lengths to ensure they are within specifications. If the cables are OK, check the transmission media for line quality.
VPMT entry for port %d missing or invalid	437006	High	High	Virtual port is configured but it has no record in the VPMT table.		Contact your representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
PORT (n) - PORT BOOT COMPLETE	439000	High	High	This message is displayed whenever a port boot is completed. The value *PORT (n)* identifies the port that has been booted.		This is an information message only. No corrective action is required.
PORT (n) - PORT BOOT FAILURE - *(cause)*	439001	High	High	This message indicates that a port boot has failed. The value *PORT (n)* indicates the port that failed to boot, and the *(cause)* provides you with a brief description of what problems occurred.		To correct this problem, reconfigure the port and then boot the port or node.
PORT (n) - PORT DISABLED	439002	High	High	This message indicates that a port has been successfully disabled. The value *PORT (n)* identifies the disabled port.		This is an information message only. No corrective action is required.
PORT (n) - PORT ENABLED	439003	High	High	This message indicates that a port has been successfully enabled. The value *PORT (n)* identifies the disabled port.		This is an information message only. No corrective action is required.
%s - Remote loopback in progress	439005	High	High	T1 port looped back from the Line side for maintenance.		This is an information message only. No corrective action is required.
%s - Remote loopback ended	439006	High	High	T1 port looped back ended.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
%s - %s, *PORT (n)* - Cannot use ISDN - ISDN module missing *PORT (n)* - Failed to register with ISDN Management Entity *PORT (n)* - PORT LOST COMMUNICATION WITH DRIVER *PORT (n)* - FRAMER HW NOT SUPPORTED *PORT (n)* - %s: CLEARED *PORT (n)* - %s	439007	High	High	T1/E1 port finds PRI ISDN module in the node. ISDN module did not respond. T1E1 port cannot communicate with driver. Framer Chip revision not supported. Line Alarms cleared. Line Alarms set %s is one of the following strings: T1: YELLOW ALARM or RED ALARM or BLUE ALARM E1: REMOTE ALARM INDICATION or LOSS OF FRAME or LOSS OF SIGNAL or REMOTE ALARM INDICATION		Load image that includes appropriate ISDN modules. Call customer service. Node BOOT is needed. Call customer service.
PORT (n) - THRESHOLD EXCEEDED %s is one of "LES" or "LCV" or "PCV" or "CSS" or "ES" or "BES" or "SES" or "SEFS" or "UAS"	439008	Medium	Medium			Contact your representative if this alarm is displayed.
PORT (n) - PORT INIT FAILURE - *(cause)*	439009	High	High	This alarm indicates a failure in the software initialization. The value *PORT (n)* identifies the port effected, while *(cause)* identifies possible causes of this failure.		Check the configuration, the version of installed software, and the hardware on which the software is installed.
TDMTG_CLK Module fail (OS Memory)	446000	High	High	This message indicates that there is insufficient memory available.		Check the configuration. Could be over configured.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
System Clock lost from port %d System Clock derives from port %d Card-%dc lost clock from port %d Card-%dc clock derives from port %d Card-%dc Group-%dg clock is lost from port %d Card-%dc Group-%dg clock derives from port %d %d is the port number %dc is card slot number %dg is group number	446001	Medium	Medium	Informs user that the port supplying system clock is down. Informs user that a new port was selected to supply system clock. Informs user that the port supplying card clock is down Informs user that a new port was selected to supply card clock. Informs user that the port supplying group clock is down. Informs user that a new port was selected to supply group clock.		This is an information message, and follows after T1/E1 alarms.
INVALID BCSR FOR SLOT %d	448000	High	High	This message indicates that the Board Command Status Register contains an invalid value.		Reboot the Vanguard 7300. If this problem persists, replace the T1/E1 hardware for this slot.
LUA SOCKET CONNECT FAILED	451000	High	High	This message indicates that memory allocation failed.		Delete resources such as LU entries, SLAC stations, ports, etc. that are not needed.
INTIALIZATION FAILED	452000	Medium	Medium			Contact your representative if this alarm is displayed.
SNABSC_CM CM SYSERR %x, p1=%x, p2=%x, p3=%x	452001	Medium	Medium			Contact your representative if this alarm is displayed.
INSUFFICIENT MEMORY TO SUPPORT SNABSC_CM CONFIGURATION	452002	High	High			Contact your representative if this alarm is displayed.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
%s- DEBUG - %s	454001	Debug	Debug	This message indicates various diagnostics alarms.		This is an informational message. No corrective action is required.
%s - SBS FW Upgrade %d.%d - %s	454002	High	High	This message indicates that the T3E3 card firmware has been upgraded.		This is an informational message. No corrective action is required.
%s -DEBUG - %s	455000	Debug	Debug	Used for various diagnostic alarms.		No corrective action is required.
PORT (n) - PORT INIT FAILURE - *(cause)*	455001	High	High	This message indicates a failure during the initialization of the T3E3 port. The following failure cause strings may appear: 1. Error saving cmem during init 2. Some of the required modules are missing. 3. Insufficient memory 4. Error create DRV_WANIC		Check the configuration, the version of installed software, and the hardware on which the software is installed. 1. Reduce node configuration 2. Relink image and reload node 3. Reduce node configuration 4. Check hardware and reboot node to reload the firmware
PORT (n) - PORT BOOT COMPLETE	455002	High	High	This message indicates that the T3E3 port has completed a port boot successfully.		This is an informational message. No corrective action is required.
PORT (n) - PORT BOOT FAILURE - *(cause)*	455003	High	High	Indicates that a failure during a port boot of the T3E3 port. The following failure cause strings can appear: 1. NO CONFIGURATION 2. PORT TYPE CHANGED 3. PORT DISABLED		To correct this problem, reconfigure the port and then boot the port or node. 1. Reconfigure 2. Reboot node for new configuration 3. Enable the port and reboot the port
PORT (n) - PORT DISABLED	455004	High	High	This message indicates that the T3E3 port is disabled.		This is an informational message. No corrective action is required.
PORT (n) - PORT ENABLED	455005	High	High	This message indicates that the T3E3 port is enabled.		This is an informational message. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
%s - TRANSMITTED ALARM SET: %s	455006	High	High	This message indicates that the alarms go from an OFF to ON state. The following alarms can appear, separated by a “+” character: “AIS”, “IDLE”, “RAI” and “AOS”.		This is an informational message. No corrective action is required.
%s - TRANSMITTED ALARM CLEARED: %s	455007	High	High	This message indicates that the alarms go from an ON to OFF state. The following alarms can appear separated by a “+” character: “AIS”, “IDLE”, “RAI” and “AOS”.		This is an informational message. No corrective action is required.
%s - RECEIVED ALARM SET: %s	455008	High	High	This message indicates that the alarms go from an OFF to ON state. The following alarms can appear, separated by a “+” character: “LOL”, “LOS”, “LOF”, “RAI”, “IDLE”, and “AIS”.		This is an informational message. No corrective action is required.
%s - RECEIVED ALARM CLEARED: %s	455009	High	High	This message indicates that the alarms go from an ON to OFF state. The following alarms can appear separated by a “+” character: “LOL”, “LOS”, “LOF”, “RAI”, “IDLE”, and “AIS”.		This is an informational message. No corrective action is required.

Chapter 12
VPN TUNNEL Alarms and Reports

Overview

Introduction

This chapter describes Vanguard VPN alarm messages and informational notices and reports. The alarms and reports are organized in numerical order by error code.

VPN Trap Number Duplication

VPN Tunnel alarms could have more than one Alarm Text, Description and Corrective Action associated to the same Trap Number.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TUNNEL - Not enough memory - Not Enough Memory to Initialize Module TUNNEL	426000	High	Critical	There is not enough memory to initialize and bring up the Module Tunnel.		To correct this situation: Add more system memory Delete any unused configurations, ports, or stations
TUNNEL - Not enough memory – Memory allocation for Tunnel Context Block failed	426000	High	Critical	Mem Allocation for Tunnel Context Block failed, Feature Tunnel/VPN is not available.		To correct this situation: Add more system memory. Delete any unused configurations, ports, or stations Delete Tunnel entry
TUNNEL - Not enough memory – Memory allocation for Tunnel Array failed	426000	High	Critical	Mem Allocation for Tunnel pointers array failed, Feature Tunnel is not available.		To correct this situation: Add more system memory. Delete any unused configurations, ports, or stations Delete Tunnel entry
TUNNEL - Not enough memory –Allocation of tunnel Table entry failed, TNL No. - (n) onwards not available	426000	High	Critical	Mem Allocation for individual tunnel data structure failed during node boot time, tunnel number ‘n’ onwards not available if configured.		To correct this situation: Add more system memory. Delete any unused configurations, ports, or stations Delete Tunnel entry
TUNNEL - Not enough memory – Allocation for Tunnel Table Entry Failed	426000	High	Minor	Mem Allocation for individual tunnel data structure failed during tunnel boot time, tunnel number ‘n’ not available.		To correct this situation: Add more system memory. Delete any unused configurations, ports, or stations Delete Tunnel entry

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TUNNEL - Not enough memory – cache is disabled	426000	High	Minor	Mem Allocation for Tunnel Cache data structure failed, tunnel cache is not available and tunnel slow path is used always.		To correct this situation: Add more system memory. Delete any unused configurations, ports, or stations Delete Tunnel entry
TUNNEL - Not enough memory - mem Alloc for tnl brdg link params failed	426000	High	Minor	Mem Allocation for tunnel bridge link parameters data structure failed, bridge traffic is not supported as tunnel payload.		To correct this situation: Add more system memory. Delete any unused configurations, ports, or stations Delete Tunnel entry
TUNNEL - Not enough memory - mem Alloc for tunnel encryption failed.	426000	High	Critical	Mem Allocation for tunnel encryption data structure failed, encrypted tunnel is not available.		To correct this situation: Add more system memory. Delete any unused configurations, ports, or stations Delete Tunnel entry
TUNNEL Table entry no. (n) duplicate of entry no. (m)	426001	Low	Normal	Duplicate tunnel record exists in the cmem. Here tunnel no ‘n’ is duplicate of tunnel no ‘m’.		Remove/change the duplicate tunnel entry.
TUNNEL – Configuration Error - In tunnel (n) interface is conflicting with lcon (m) interface	426002	Low	Minor	Tunnel n’s interface is used by LCON m.		Change the tunnel interface number, use the interface number which is free and not used by any LCON or any other tunnels.
TUNNEL – Configuration Error - In tunnel (n) bridge link no is conflicting with lcon (m) bridge link no	426002	Low	Minor	Tunnel n’s bridge link number is used by LCON m.		Change the tunnel bridge link number, use the bridge link number which is free and not used by any LCON or any other tunnels.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TUNNEL – Configuration Error - Invalid LAN nexthop in tunnel (n)	426002	Low	Minor	Next hop address configured in tunnel entry (n) is not a directly connected LAN.		Change the Next hop address to a valid directly connected LAN address.
TUNNEL – Configuration Error - LAN interface (i) used by tunnel (n) is not enabled	426002	Low	Minor	LAN interface 'i' used by tunnel 'n' for forwarding the tunneled packets is not enabled.		Enable the corresponding interface.
TUNNEL – Configuration Error - Tnl no. (n) 's Lcon no (m) not config	426002	Low	Minor	LCON 'm' used by tunnel 'n' for forwarding the tunneled packets is not configured.		Configure the corresponding LCON.
TUNNEL – Configuration Error - Tnl no (n) : source address not a NAT ext addr nor an ifc addr	426002	Low	Minor	Source address used by tunnel 'n' does not belong to the node.		Change the tunnel source address to a valid one, which belongs to the node. The source address can be 1. One of the logical interface address. 2. NAT external address.
TUNNEL – Configuration Error - IP tnl ifc (i) not conf for Tnl no (n)	426002	Low	Minor	IP interface 'i' used by tunnel 'n' is not configured.		Configure IP interface for tunnel/ virtual interface or remove IP from tunnel payload protocols.
TUNNEL – Configuration Error - IPX tnl ifc (i) not conf for Tnl no (n)	426002	Low	Minor	IPX interface 'i' used by tunnel 'n' is not configured.		Configure IPX interface for tunnel/virtual interface or remove IPX from tunnel payload protocols.
TUNNEL – Configuration Error - "IP and IPX tnl ifc (i) not conf for Tnl no (n)	426002	Low	Minor	IP & IPX interface 'i' used by tunnel 'n' is not configured.		Configure IP & IPX interface for tunnel/virtual interface or remove IP & IPX from tunnel payload protocols.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TUNNEL – Configuration Error - "tnl ifc (i) dis or unconfig for Tnl no (n)	426002	Low	Minor	Virtual Interface ‘i’ used by tunnel ‘n’ is in Disabled or Unconfigured state.		Change the Interface state to Enabled.
TUNNEL – Configuration Error - net pntr of vir/tnl ifc no – (i) for tunnel no – (n) is NULL	426002	Low	Minor	Net pointer of virtual interface ‘i’ used by tunnel ‘n’ is NULL.		This error might be because of MEM allocation failure for NET structure. Upgrade the device memory as required or contact your customer service representative.
TUNNEL – Configuration Error - Tnl-(n) tnl ifc clash phys ifc configured in lcon-(m)	426002	Low	Minor	Tunnel ‘n’ virtual interface clash with physical interface configured in LCON ‘m’.		Change the tunnel interface number, use the interface number which is free and not used by any LCON or any other tunnels.
TUNNEL – Configuration Error - Tnl-(n) bridge link clash lcon bridge link configured in lcon-(m)	426002	Low	Minor	Tunnel ‘n’ bridge link clash with LCON bridge link configured in LCON ‘m’.		Change the tunnel bridge link number, use the bridge link number which is free and not used by any LCON or any other tunnels.
TUNNEL - Configuration Error- Tnl# (n) ; tnl src addr is already used as vir addr by tnl - (m), ifc - (1)	426002	Low	Minor	Tunnel ‘n’ source address is overlapping with virtual address of interface ‘i’ used by tunnel ‘m’.		Change the configuration of tunnel and IP interface appropriately to resolve the conflict between tunnel source and virtual address.
TUNNEL - Configuration Error - Tnl# (n) ; tnl vir addr (ifc # (1) addr) is already used as src addr by tnl - (m)	426002	Low	Minor	Tunnel ‘n’ virtual address associated with interface ‘I’ is overlapping with source address of tunnel ‘m’ which is valid and up.		Change the configuration of tunnel and IP interface appropriately to resolve the conflict between tunnel source and virtual address.
TUNNEL – Configuration Error - Bridge Link no (m) not conf for Tnl no (n)	426002	Low	Minor	Bridge link ‘m’ used by tunnel ‘n’ is not configured.		Configure the corresponding bridge link record.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TUNNEL - Tnl pkt sent frm (x.x.x.x) to (y.y.y.y) on tnl no (n)	426003	Debug*	Informati onal	A packet is tunneled and sent on tunnel number 'n'		This is an information message only. No corrective actions are required.
TUNNEL - Tnl pkt rcvd frm (y.y.y.y) to (x.x.x.x) on tnl no (n)	426003	Debug*	Informati onal	A tunneled packet is received on tunnel number 'n' for detunneling.		This is an information message only. No corrective actions are required.
TNL_ENCR Channel opened for (x.x.x.x) -> (y.y.y.y)	426004	Medium	Informati onal	Encryption channel opened for tunnel x.x.x.x to y.y.y.y		This is an information message only. No corrective actions are required.
TNL_ENCR Channel closed for (x.x.x.x) -> (y.y.y.y)	426005	Medium	Informati onal	Encryption channel closed for tunnel x.x.x.x to y.y.y.y		This is an information message only. No corrective actions are required.
Packet is Encrypted on tunnel# (n) with src (x.x.x.x) dst (y.y.y.y)	426006	Low*	Informati onal	Packet is encrypted on tunnel 'n' with source address x.x.x.x and dest addr y.y.y.y		This is an information message only. No corrective actions are required.
Packet is Decrypted on tunnel# (n) with src (x.x.x.x) dst (y.y.y.y)	426007	Low*	Informati onal	Packet is decrypted on tunnel 'n' with source address x.x.x.x and dest addr y.y.y.y		This is an information message only. No corrective actions are required.
TNL_ENCR- Tunnel queue Full	426008	Low	Informati onal	Tunnel Encryption Queue is full; no more packets can be queued for encryption.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TNL_ENCR - Unknown packet (n)	426009	Low	Informati onal	Packets received for decryption when the encryption state is invalid or not up.		This is an information message only. No corrective actions are required.
TNL_ENCR - Tunnel queue Flush	426010	Low*	Informati onal	Tunnel encryption Queue flushed due to tunnel encrypt timer timeout.		This is an information message only. No corrective actions are required.
TUNNEL - Tunnel cache entry x.x.x.x -> y.y.y.y deleted	426011	Low	Informati onal	Tunnel with src addr x.x.x.x and dest addr y.y.y.y is deleted from tunnel cache.		This is an information message only. No corrective actions are required.
TUNNEL - Tunnel cache cleared	426012	Low	Informati onal	Entire tunnel cache is cleared due to tunnel boot.		This is an information message only. No corrective actions are required.
TUNNEL - Tunnel cache garbage collecting...	426013	Low	Informati onal	Tunnel Cache as started garbage collecting the least used entries.		This is an information message only. No corrective actions are required.
TUNNEL no (n) - Cache is not initialized and can't install cache	426014	Low*	Warning	If Cache is disabled because of memory allocation failure, installing cache entry is not possible.		This error might be because of MEM allocation failure for tnl cache structure Upgrade the device memory as required
TUNNEL no (n) - congestion, pkt dropped	426014	Low	Informati onal	Packets received for encryption when the encryption state is in handshaking and the tunnels encrypt queue is full.		Stop traffic over tunnel ‘n’, until the tunnel encryption channel is opened.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TUNNEL no (n) - Rcvd out of order pkt. Pkt dropped	426014	Low	Informati onal	Received tunneled packet with GRE sequence out of order and not the expecting sequence number.		This is an information message only. No corrective actions are required.
TUNNEL no (n) - Pkt drp due to err in GRE hdr cksum	426014	Low	Informati onal	Received tunneled packet with wrong GRE header checksum.		This is an information message only. No corrective actions are required.
TUNNEL no (n) - Pkt dropped due to unsupp payload prtcl	426014	Low	Informati onal	Received tunneled packet with unsupported tunnel payload protocol.		This is an information message only. No corrective actions are required.
TUNNEL no (n) - Outgoing IP pkt drp due to unsupp payload prtcl	426014	Low	Informati onal	IP is not configured has payload in tunnel number ‘n’, IP packets over this tunnel are dropped.		This is an information message only. No corrective actions are required.
TUNNEL no (n) - Outgoing IPX pkt drp due to unsupp payload prtcl	426014	Low	Informati onal	IPX is not configured has payload in tunnel number ‘n’, IPX packets over this tunnel are dropped.		This is an information message only. No corrective actions are required.
TUNNEL no (n) - Context State Pkt Sent	426014	Low	Informati onal	RUIHC context state packet sent over tunnel number ‘n’		This is an information message only. No corrective actions are required.
TUNNEL no (n) - Outgoing Bridge pkt drp due to unsupp payload prtcl	426014	Low	Informati onal	Bridge is not configured has payload in tunnel number ‘n’, Bridge traffic over this tunnel are dropped.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TUNNEL no (n) - Outgoing pkt drp due to unsupp payload prtcl	426014	Low	Informati onal	Unsupported tunnel payload protocol received for tunneling, packet is dropped.		This is an information message only. No corrective actions are required.
TUNNEL no (n) - Outgoing pkt drp due to unsupp encap prtcl	426014	Low	Informati onal	Unsupported encapsulation protocol requested for tunneling, packet is dropped.		This is an information message only. No corrective actions are required.
TUNNEL no (n) - Outgng pkt drp ,unavail of mem for fragm	426014	Low	Warning	Fragmentation of tunneled packets failed because of memory allocation failure, Packet is dropped.		To correct this problem, verify that the Vanguard device has sufficient memory. Upgrade the device memory as required.
TUNNEL no (n) - Incoming Pkt drp due to err in IP hdr	426014	Low	Informati onal	Error in IP header of the received tunneled packet.		This is an information message only. No corrective actions are required.
TUNNEL no (n) - Incoming Pkt drp as encr pkt rcvd on non-encr tnl	426014	Low	Informati onal	Incoming tunneled packet dropped because, encrypted packet received on non-encrypted tunnel.		This is an information message only. No corrective actions are required.
TUNNEL no (n) – Incoming Pkt drp as non-encr pkt rcvd on encr tnl	426014	Low	Informati onal	Incoming tunneled packet dropped because, non-encrypted packet received on encrypted tunnel.		This is an information message only. No corrective actions are required.
TUNNEL no (n) – Incoming Pkt drp due to unsupp encap prtcl	426014	Low	Informati onal	Incoming tunneled packet dropped because, unsupported tunnel encapsulation protocol received, GRE is the only tunneling protocol which is supported in Vanguard routers.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TUNNEL no (n) – Incoming IP Pkt drp as tnl ifc is down	426014	Low	Informati onal	Incoming tunneled packet with payload IP is dropped because, tunnel interface is down.		Check why the tunnel interface as gone down, tunnel interface may go down if the tunnel physical link goes down.
TUNNEL no (n) – Incoming IP Pkt drp as tnl netp is NULL	426014	Low	Informati onal	Incoming tunneled packet with payload IP is dropped because tunnel net pointer is NULL.		Contact your customer service representative if this alarms appears repeatedly.
TUNNEL no (n) – Incoming IP pkt drp due to unsupp payload prtcl	426014	Low	Informati onal	Incoming tunneled packet with payload IP is dropped because IP is not configured as tunnel payload protocol.		This is an information message only. No corrective actions are required.
TUNNEL no (n) - Incoming IPX Pkt drp as tnl ifc is down	426014	Low	Informati onal	Incoming tunneled packet with payload IPX is dropped because, tunnel interface is down.		Check why the tunnel interface has gone down, tunnel interface may go down if the tunnel physical link goes down.
TUNNEL no (n) - Incoming IPX Pkt drp as tnl netp is NULL	426014	Low	Informati onal	Incoming tunneled packet with payload IPX is dropped because, tunnel net pointer is NULL.		Contact your customer service representative if this alarms appears repeatedly.
TUNNEL no (n) - Incoming IPX pkt drp due to unsupp payload prtcl	426014	Low	Informati onal	Incoming tunneled packet with payload IPX is dropped because, IPX is not configured as tunnel payload protocol.		This is an information message only. No corrective actions are required.
TUNNEL no (n) - Incoming IP-RUIHC Pkt drp as tnl ifc is down	426014	Low	Informati onal	Incoming tunneled packet with payload IP-RUIHC is dropped because, tunnel interface is down.		Check why the tunnel interface has gone down, tunnel interface may go down if the tunnel physical link goes down.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TUNNEL no (n) - Incoming IP-RUIHC Pkt drp as tnl netp is NULL	426014	Low	Informati onal	Incoming tunneled packet with payload IP-RUIHC is dropped because, tunnel net pointer is NULL.		Contact your customer service representative if this alarms appears repeatedly.
TUNNEL no (n) - Incoming IP-RUIHC pkt drp due to Decompression failure	426014	Low	Informati onal	Incoming tunneled packet with payload IP-RUIHC is dropped because, Header Decompression failed. The reason for the decompression failure is shown by separate RUIHC alarms.		Check RUIHC profile configuration. Contact your customer service representative if this alarms appears repeatedly.
TUNNEL no (n) - Compression not supp. Incoming IP-RUIHC Pkt Drpd	426014	Low	Informati onal	Incoming tunneled packet with payload IP-RUIHC is dropped because, header compression is not supported on this tunnel.		This is an information message only. No corrective actions are required.
TUNNEL no (n) – Context State Pkt rcvd	426014	Low	Informati onal	RUIHC context state packet received on tunnel number ‘n’		This is an information message only. No corrective actions are required.
TUNNEL no (n) – Incoming Bridge Pkt drp as tnl bridge link is down	426014	Low	Informati onal	Incoming tunneled packet with payload Bridge is dropped because, tunnel bridge link is down.		Check why the tunnel bridge link is down, tunnel bridge link may go down if the tunnel physical link goes down.
TUNNEL no (n) – Incoming Bridge Pkt drp as tnl brdg ptr is NULL	426014	Low	Informati onal	Incoming tunneled packet with payload Bridge is dropped because, tunnel bridge pointer is NULL.		Contact your customer service representative if this alarms appears repeatedly.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TUNNEL no (n) – Incoming Bridge pkt drp due to unsupp payload prtcl	426014	Low	Informati onal	Incoming tunneled packet with payload Bridge is dropped because, Bridge is not configured as tunnel payload protocol.		This is an information message only. No corrective actions are required.
TUNNEL no (n) – Incoming Pkt drp due to unsupp payload prtcl	426014	Low	Informati onal	Incoming tunneled packet is dropped because, unsupported tunnel payload protocol is received. Vanguard only supports IP, IPX and Bridge as tunnel payload protocols.		This is an information message only. No corrective actions are required.
TUNNEL no (n) – Outgoing Bridge Pkt drp as tnl bridge link is down	426014	Low	Informati onal	Outgoing Bridge packet is dropped because, Tunnel bridge link is down.		Check why the tunnel bridge link is down, tunnel bridge link may go down if the tunnel physical link goes down.
TUNNEL no (n) – Outgoing Bridge pkt dropped by wan	426014	Low	Informati onal	Outgoing Bridge packet over tunnel ‘n’ is dropped by WAN or LAN or TUNNEL. The reason for the drop is shown by separate alarms.		This is an information message only. No corrective actions are required.
TUNNEL no (n) - SR Packet received when Bridge type is TB	426014	Low	Informati onal	Source Routing (SR) Packets received on tunnel ‘n’ when the bridge type is Transparent Bridging (TB)		This is an information message only. No corrective actions are required.
TUNNEL no (n) - STPE Bad Hello Threshold exceeded for tnl no (n)	426014	Low	Informati onal	STPE bad hello frames exceeded the threshold for tunnel number ‘n'		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TUNNEL No timer available for cache and cache disabled	426015	Low	Warning	No software local timer available for tunnel cache, so tunnel cache is disabled.		Remove unused and unwanted IP feature configurations to free some local timers.
TUNNEL Tnl no (n) Bridge Link no (b) - Conf as SR Bridge, Mod not present	426016	Low	Warning	For tunnel 'n' bridge link is configured as SR Bridge, but module SR does not exists in the vanguard software.		Use an image, which has module Source Route (SR) Bridge.
TUNNEL Tnl no (n) Bridge Link no (b) - Conf as TB Bridge, Mod not present	426016	Low	Warning	For tunnel 'n' bridge link is configured as TB Bridge, but module TB does not exists in the vanguard software.		Use an image, which has module TB (Transparent Bridging)
TUNNEL Tnl no (n) Bridge Link no (b) - Conf as TB SR Bridge, Mods not present	426016	Low	Warning	For tunnel 'n' bridge link is configured as TB SR Bridge, but modules TB & SR does not exists in the vanguard software.		Use an image, which has modules TB and SR Bridge.
TUNNEL Tnl no (n) Bridge Link no (b) - Conf Bridge type unsupported	426016	Low	Informati onal	In tunnel 'n' bridge link number 'b' Bridge types are not supported.		This is an information message only. No corrective actions are required.
TUNNEL Pkt sent out. Seq no->(s)	426017	Debug*	Informati onal	Tunneled packet sent out with GRE sequence number 's'		This is an information message only. No corrective actions are required.
TUNNEL Pkt rcvd.Accepted	426017	Debug*	Informati onal	Tunneled packet received and accepted with GRE sequence number.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TUNNEL no (n) – Module RUIHC does not Exists	426018	Low	Warning	RUIHC profile name is configured in tunnel ‘n’, but Module RUIHC does not exists in the vanguard software.		Use an image that has module RUIHC.
TUNNEL no (n) – RUIHC Profile not configured	426018	Low	Warning	RUIHC profile name is configured in tunnel ‘n’, but profile record is not configured.		Configure the RUIHC profile record or remove the RUIHC profile name from tunnel configuration.
TUNNEL no (n) - Not enough memory – RUIHC Module Failed to initialize ruihc ptr	426018	Low	Warning	Memory allocation failed for initializing RUIHC profile configured in tunnel ‘n’.		To correct this problem, verify that the Vanguard device has sufficient memory. Upgrade the device memory as required.
TUNNEL no (n) – RUIHC Module is unable to Init ruihc profile	426018	Low	Warning	RUIHC module is unable to initialize RUIHC profile configured in tunnel ‘n’. Separate alarms are generated by module RUIHC to give reasons for Init failure.		Take necessary steps, based on the RUIHC alarms.
TUNNEL no (n) – Module Encryption does not Exists	426019	High	Minor	Encryption profile name is configured in tunnel ‘n’, but Module Encryption does not exists in the vanguard software.		Use an image that has module Encryption.
TUNNEL no (n) – Encryption Disabled or Encryption H/W not running	426019	High	Minor	Encryption profile name is configured in tunnel ‘n’, but Encryption is disabled in the node or encryption hardware is not functional.		Enable Encryption is the node. Check for proper functioning of the encryption hardware.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
TUNNEL no (n) – Encryption SIMM not UP	426019	High	Minor	Encryption profile name is configured in tunnel 'n', but the Encryption SIMM or hardware is not UP.		Take necessary steps to bring UP the encryption hardware or change the encryption SIMM if necessary.
TUNNEL no (n) – Invalid encryption profile	426019	High	Minor	Encryption profile name is configured in tunnel 'n', but the corresponding encryption profile record does not exists or profile record is invalid.		Configure Encryption profile record or Change the profile record to make it valid.

Chapter 13
Border Gateway Protocol and Board Management Alarms and Reports

Overview

Introduction

This chapter describes Vanguard Border Gateway Protocol (BGP) and Board Management alarm messages and informational notices and reports. The alarms and reports are organized in numerical order by error code.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
Route to <net_prefix>/ <prefix_len> imported from BGP into OSPF Routing Table	207007	Low	Normal	This message is generated when a route to the specified NLRI is imported from BGP into the OSPF routing table.		This is an information message only. No corrective action is required.
Route to <net_prefix>/ <prefix_len> withdrawn by BGP from OSPF Routing Table	207008	Low	Normal	This message is generated when previously imported route to the specified NLRI is withdrawn by BGP from the OSPF routing table		This is an information message only. No corrective action is required.
BGP Route to <net_prefix>/ <prefix_len> Not Imported into OSPF due to Deny Policy No. <policy_id>	207009	Debug	Normal	This message is generated when BGP route to the specified NLRI is not imported into OSPF due to matching the specified Import deny policy <policy_id> indicates the entry number of the matching policy entry in the policy table. A value of 0 will be displayed for <policy_id> when the route does not match any policy entries configured in policy table i.e. when the Global Default Import Policy is applied to the route.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP Route to <net_prefix>/ <prefix_len> matched to BGP-OSPF Import Permit Policy No. <policy_id>	207010	Debug	Normal	This message is generated when BGP route to the specified NLRI is matched to the specified BGP-OSPF Import permit policy		This is an information message only. No corrective action is required.
BGP - Not Enough Permanent memory - %s	459000	High		Error detected within BGPRT Module. This report is generated when not enough permanent memory is available for BGP objects. <err_msg> specifies the consequence of memory allocation failure and can be one of the following: • BGP Module cannot come up • BGPRT Module cannot come up BGP-OSPF Interaction will not be operational		Increase the Permanent Memory Heap Size, and if needed add more DRAM in the node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Not Enough Dynamic Memory - %s	459001	High	Critical	Error detected within BGPRT Module This report is generated when not enough dynamic memory is available for BGP objects. <err_msg> specifies the consequence of memory allocation failure and can be one of the following: BGP Import/Export Policy functionality will not be operational. BGP Will not be Operational BGP Route to <net_prefix>/ <prefix_len> received from Peer No. <peer_id> not Added into Routing Table BGP AS Path received from Peer No. <peer_id> not Added into Routing Table IGP Route to <net_prefix>/ <prefix_len> not imported into BGP Routing Table BGP Route to <net_prefix>/ <prefix_len> will not be Advertised to BGP Peers BGP Peering will not be Established with Peer No. <peer_id> BGP Peering will not be Operational with Peer No. <peer_id> <Configuration Table>: Entry No. %d onwards will not be Applicable		a) Add more DRAM in the node. b) Disable some of the other features which are not currently being used.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Error in UPDATE Message Received from Peer No. %d - %s, %s	459002	High	Warning	where <err_msg> indicates the exact error and can be one of the following: • Missing Well-Known Attribute • Missing Local-Pref Attribute • Invalid Network field, Invalid Prefix Len in withdrawn Routes • Invalid Network Field, Invalid Prefix Len in Reachable Routes • Attribute Flags error Attribute Length error • Invalid ORIGIN Attribute • Malformed AS_PATH, bad AS Type in AS Path Segment • Local AS Already in AS Path • AS Routing Loop In AS Path • Invalid NEXT_HOP Attribute,Not a valid IP address • Invalid Nexthop attribute, Same as Local BGP Speaker IP Address		Contact your customer service representative.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Error in UPDATE Message Received from Peer No. %d - %s, %s (Continued)	459002	High	Warning	• Nexthop not present on the Shared Subnet between Peer and Local BGP Speaker and Indirect Peering is not allowed with the Peer • Local Pref rcvd from Ext Peer • Malformed Attribute List, Duplicate Attribute in Attribute List		
BGP - Invalid NLRI Received from Peer No. %d - %s	459003	High		This message is generated when a invalid NLRI is received from the specified Peer. <err_msg> specify the exact error and can be one of the following. • Subnet Prefix with Non continuous Mask • Destination Subnet Prefix & Nexthop shares the common subnet		Resolve the cause of erroneous data received from BGP Peer, as indicated by the alarm message.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Buffer not available for %s the %s message to Peer No. %d	459004	High	Critical	Error detected within BGPRT Module. This report is generated when buffer is not available for sending/ receiving a BGP message to/from a peer. <operation> can be either "Sending" or "Receiving" <msg_type> can be one of the following • Open • KeepAlive • Notify • Update <peer_id> - Unique Peer Number assigned to the Peer.		Increase the Buffer (IORB) Pool Size, and if needed add more DRAM in the node.
BGP - Route to %s\/%d Learnt from Peer No. %d (0 - IGP Route)	459005	Low	Normal	Route to <net_prefix>/ <prefix_len> Learnt from Peer No. <peer_id> This message is generated when a BGP route to the specified NLRI is learnt from the specified Peer.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Route to %s\/%d Withdrawn by Peer No. %d	459006	Low	Normal	Route to <net_prefix>/ <prefix_len> withdrawn by Peer No. <peer_id> This message is generated when a previously learnt BGP route to the specified NLRI is withdrawn by the specified Peer.		This is an information message only. No corrective action is required.
BGP - Non Existing Route to %s\/%d being tried to be Withdrawn by Peer No. %d	459007	Low	Normal	Non Existing Route to <net_prefix>/<prefix_len> being tried to be withdrawn by Peer No. <peer_id> This message is generated when a non existing BGP route is being tried to be is withdrawn by the specified Peer i.e Peer tries to withdraw the route which was never advertised by it to the local BGP Speaker.		This is an information message only. No corrective action is required.
BGP - Route to %s\/%d Unreachable via Peer No. %d	459008	Low	Normal	Route to <net_prefix>/ <prefix_len> unreachable via Peer No. <peer_id> This message is generated when a previously learnt BGP route to the specified NLRI becomes unreachable via the specified Peer due to the loss of BGP connection with it.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Best Route to %s\/%d Changed. Current Best Route via Peer No. %d	459009	Low	Normal	Best Route to <net_prefix>/<prefix_len> Changed - Current Best Route Via Peer No. <peer_id> This message is generated when a best route to the specified NLRI is changed.		This is an information message only. No corrective action is required.
BGP - Route to %s Not Available Anymore.	459010	Low	Normal	Route to <net_prefix>/ <prefix_len> not available anymore This message is generated when route for the specified NLRI is not available anymore i.e the last route to the specified NLRI is withdrawn.		This is an information message only. No corrective action is required.
BGP - Route to %s\/%d Relearnt from Peer No.	459011	Low	Normal	Route to <net_prefix>/ <prefix_len> Re-learnt from Peer No. <peer_id> This message is generated when route for the specified NLRI is re-learnt from the specified peer i.e. when the previously learnt route for the specified NLRI is replaced by a new route received from the same peer.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Route to %s\/%d Imported from IGP into BGP Routing Table	459012	Low	Normal	Route to <net_prefix>/ <prefix_len> imported from IGP into BGP Routing Table This message is generated when a route to the specified NLRI is imported from the IGP into the BGP routing table.		This is an information message only. No corrective action is required.
BGP - Route to %s\/%d Withdrawn by IGP from BGP Routing Table	459013	Low	Normal	Route to <net_prefix>/ <prefix_len> withdrawn by IGP from BGP Routing Table This message is generated when previously imported route to the specified NLRI is withdrawn by IGP from the BGP routing table.		This is an information message only. No corrective action is required.
BGP - NOTIFY Message %s to Peer No. %d \[ErrCode: %d,ErrSubCode: %d,ErrData: %s \]	459015	Debug				Contact your customer service representative.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - UPDATE Message %s from Peer No. %d \[Unfeasible Len: %d, Attr Len: %d, Reachable Len: %d \]	459016	Debug	Normal	This message is generated when BGP Update Message is sent or received to/from BGP Peer with the specified contents. <tot_unfeasible_rt_len> - Indicates the total length in octets of withdraw route information present in Update message. <tot_attr_len> - Indicates the total length in octets of Path Attributes information present in Update message <tot_reach_rt_len> - Indicates the total length in octets of Reachable route (NLRI) information present in Update message		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Route to %s\/%d received from Peer %d Filtered due to Deny Policy No %d	459017	Debug	Normal	This message is generated when BGP route to the specified NLRI received from the specified peer is filtered due to matching the specified Inbound deny policy <policy_id> indicates the entry number of the matching policy entry in the policy table. A value of 0 will be displayed for <policy_id> when the route does not match any policy entries configured in policy table i.e. when the Global Default Inbound Policy is applied to the route.		This is an information message only. No corrective action is required.
BGP - Route to %s\/%d received from Peer %d matched to Inbound Permit Policy No %d	459018	Debug	Normal	This message is generated when BGP route to the specified NLRI received from the specified peer is matched to the specified Inbound permit policy.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Route to %s\/%d not advertised to Peer %d due to Deny Policy	459019	Debug		This message is generated when BGP route to the specified NLRI is not advertised to the specified peer due to matching the specified Outbound deny policy A value of 0 will be displayed for <policy_id> when the route does not match any policy entries configured in policy table i.e. when the Global Default Outbound Policy is applied to the route.		This is an information message only. No corrective action is required.
BGP - Route to %s\/%d advertised to Peer %d due to Permit Policy	459020	Debug	Normal	This message is generated when BGP route to the specified NLRI is advertised to the specified peer due to matching the specified Outbound permit policy.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Not enough Permanent Memory %s	460000	High	Critical	Error Detected within the BGP Module. This report is generated when not enough permanent memory is available for BGP objects. <err_msg> specifies the consequence of memory allocation failure and can be one of the following: • BGP Module cannot come up • BGPRT Module cannot come up • BGP-OSPF Interaction will not be operational		Increase the Permanent Memory Heap Size, and if needed add more DRAM in the node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Not Enough Dynamic Memory %s	460001	High	Critical	Error detected within BGP module. This report is generated when not enough dynamic memory is available for BGP objects. <err_msg> specifies the consequence of memory allocation failure and can be one of the following: BGP Import/Export Policy functionality will not be operational. BGP Will not be Operational BGP Route to <net_prefix>/ <prefix_len> received from Peer No. <peer_id> not Added into Routing Table BGP AS Path received from Peer No. <peer_id> not Added into Routing Table IGP Route to <net_prefix>/ <prefix_len> not imported into BGP Routing Table BGP Route to <net_prefix>/ <prefix_len> will not be Advertised to BGP Peers BGP Peering will not be Established with Peer No. <peer_id> BGP Peering will not be Operational with Peer No. <peer_id> <Configuration Table>: Entry No. %d onwards will not be Applicable		a) Add more DRAM in the node. b) Disable some of the other features which are not currently being used.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP -> Missing Modules - %s	460002	High	Critical	This report is generated when not all the necessary modules are present in node for BGP to become operational. <err_msg> specifies the missing modules and the consequence of it. BGPRT/TCP: BGP will not be operational		Add the necessary modules in the software image.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Configuration Error - %s	460003	High	Warning	Configuration error <err_msg> Displayed at init time or after booting, if there is an invalid configuration. <err_msg> indicates the exact error message and can be one of the following. <Configuration Table>: Entry No. %d is Duplicate of Entry No. %d <Configuration Table>: Entry No. %d : Invalid Entry: <invld_err_msg> <Configuration Record>: Invalid Record: <invld_err_msg> In the above error messages, <Configuration Table> can be one of the following. BGP Peer Table BGP Import/Export Policy Table BGP->OSPF Import Policy Table <Configuration Record> can be one of the following. BGP Global Parameters <invld_err_msg> can be one of the following. Duplicate IP Address in Peer IP Address List Invalid BGP Identifier, Should be One of the Addresses Belonging to Node		Change or delete the entry with bad configuration.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - TCP Connection Error with Peer No. %d %s	460004	High	Warning	This report is generated when a TCP level connection error has happened while establishing the TCP connection with the specified peer. <err_msg> indicates the exact error and can be one of the following. Connection Request Failed due to Lack of Resource Connection Establishment Failed as no Route to Peer IP Address x.x.x.x Max Connection Retries Over TCP Listen Failed due to lack of resource, Can't Accept the Passive TCP Connections from BGP Peers for some time.		Resolve the cause of TCP connection error as indicated by the alarm message.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Buffer not Available for %s the %s Peer No. %d	460005	High	Critical	Error detected within BGP Module. This report is generated when buffer is not available for sending/ receiving a BGP message to/from a peer. <operation> can be either "Sending" or "Receiving" <msg_type> can be one of the following • Open • KeepAlive • Notify • Update <peer_id> - Unique Peer Number assigned to the Peer.		Increase the Buffer (IORB) Pool Size, and if needed add more DRAM in the node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP Connection Error with Peer No. %d - %s	460006	High	Warning	This report is generated when a BGP level connection error has happened while forming the BGP connection with the specified peer. <err_msg> indicates the exact error and can be one of the following. •Connection Request from BGP Peer Rejected as Peer IP Address x.x.x.x is not configured. •Connection Request from BGP Peer Rejected as Peer is Currently Disabled at Local BGP Speaker •Connection Request from BGP Peer Rejected as local BGP speaker is not in a FSM state to accept it •Connection Establishment Failed as Peer IP Address x.x.x.x is not on a directly connected network and the Indirect BGP Peering is not Allowed for the Peer •Connection Establishment Failed as Hold Timer Expired in OpenSent/OpenConfirm State.		Resolve the cause of BGP connection error as indicated by the alarm message.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Hold Timer Expired in Establish state on BGP connection with Peer No. %d	460007	High	Warning	This message is generated when Hold Timer is expired for the previously established BGP connection with a particular peer.		a) Inspect the TCP Connection and status of BGP Peer for possible problems. b) Otherwise Increase the Hold Down Timer for the BGP connection with the Peer

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Error in Open Message Received from Peer No. %d, %s %ld	460008	High	Warning	This report is generated when OPEN message with erroneous/unexpected/un-acceptable value in one of the OPEN message fields, is received from a peer. <err_msg> indicates the exact error and can be one of the following: • Unsupported Version Number • Bad Peer AS, not Matching to AS Number Configured for the Peer at Local BGP speaker • Bad BGP Identifier • Unsupported Optional Parameter • Authentication Failure, Bad Authentication Code • Authentication Failure, Bad Authentication Data • Unacceptable Hold Time • <err_val> indicates the value received in erroneous field.		Resolve the cause of erroneous/ unacceptable data received from BGP Peer, as indicated by the alarm message.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - FSM Error on BGP connection with Peer No. %d Curr state %d Curr Event %d	460009	High	Warning	This message is generated when a FSM error is detected on the BGP connection with a particular peer. A FSM error here means receipt of an unexpected event in a particular BGP connection state. <curr_state> indicates the current BGP connection state <curr_event> indicates unexpected event received, which has caused the FSM Error		Trace the BGP FSM state change and resolve the cause of FSM error.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Message Header Error in Message Received from Peer No. %d - %s %d	460010	High	Warning	Message Header Error in Message received from Peer No. <peer_id> - <err_msg>, <err_val> Includes <err_val> This report is generated when a BGP message with erroneous value in one of the BGP message header fields, is received from a peer. <err_msg> indicates the exact error and can be one of the following. • Bad Message Length • Bad Message Type • Connection Not Synchronized, Invalid Marker <err_val> indicates the value received in erroneous field.		Resolve the cause of erroneous data received from BGP Peer, as indicated by the alarm message.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Message Header Error in Message Received from Peer No. %d - %s	460011	High	Warning	Message Header Error in Message received from Peer No. <peer_id> - <err_msg>, Does not include <err_val> This report is generated when a BGP message with erroneous value in one of the BGP message header fields, is received from a peer. <err_msg> indicates the exact error and can be one of the following. • Bad Message Length • Bad Message Type • Connection Not Synchronized, Invalid Marker <err_val> indicates the value received in erroneous field		Resolve the cause of erroneous data received from BGP Peer, as indicated by the alarm message.
BGP - Connection Establish with Peer No. %d	460012	Low	Normal	This message is generated when the BGP connection with a Peer is successfully established i.e. whenever the BGP Connection with the peer is moved to "Established" state.		This is an information message only. No corrective action is required.
BGP - TCP Listen Failed Due to lack of resource, Can't Acept the Passive TCP Conn from BGP Peers for some time	460013	High	Warning	This message is geneated when a request to open a TCP Listen port has failed, and the LISTEN timeout interval has expired.		Resolve the cause of the TCP connction error as indicated by the alarm message. May accomapny Alarm msg #1 (Trap # 460004).

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - TCP Post Receive Failed for Peer No. %d	460014	Low	Warning			Contact your customer service representative.
BGP - Error in NOTIFY Message Received from Peer No. %d %s %d	460015	High		NOTIFY Error in Message received from Peer No. <peer_id> - <err_msg> This report is generated when an error is detected in the NOTIFY message received from a peer. <err_msg> indicates the exact error and can be one of the following. • Unrecognized Error Code • Unrecognized Error Subcode <err_val> indicates the erroneous value		Resolve the cause of erroneous data received from BGP Peer, as indicated by the alarm message.
BGP - Connection %s controlled by TCP with Peer No. %d	460016	Low	Normal	<conn_stat> = Flow This message is generated when BGP Connection with the specified peer is flow controlled by TCP i.e. when TCP is unable to transmit any more BGP data on the BGP connection with the specified peer.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Connection %s controlled by TCP with Peer No. %d	460016	Low	Normal	<conn_stat> = DeFlow This message is generated when BGP Connection with the specified peer is de-flow controlled by TCP i.e. when TCP is ready to transmit more BGP data on the BGP connection with the specified peer.		This is an information message only. No corrective action is required.
BGP - %s Connection Collision with Peer No. %d -%s	460017	Low	Normal	TCP Connection Collision with Peer No. <peer_id> - <action> <conn_type> = TCP This message is generated when the connection collision happens while establishing the TCP connection with the peer. <action> indicates the connection collision resolution and can be one of the following • Peer TCP Connection Request Rejected • Local TCP Connection process Aborted and Peer Connection Request Accepted.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - %s Connection Collision with Peer No. %d -%s	460017	Low	Normal	<conn_type> = BGP This message is generated when the connection collision happens while establishing the BGP connection with the peer. <action> indicates the connection collision resolution and can be one of the following • Peer BGP Connection Request Rejected • Local BGP Connection process Aborted and Peer BGP Connection Request Accepted		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Connection Lost with Peer No. %d -%s	460018	Low	Normal	BGP Connection Lost with Peer No. <peer_id> - <rsn> This message is generated when the previously established BGP connection with a Peer is lost i.e. whenever the BGP Connection with the peer is moved from "Established" state to a non-"Established" state. <rsn> indicates the cause of connection loss and can be one of the following. • Hold Down Timer Expired • Update Message Error • Explicit Close by the Administrator (i.e disabling the BGP peer at run time) • Connection Closure by BGP Peer (i.e. on reception of Notify message from peer) • TCP Connection Broken		This is an information message only. No corrective action is required.
BGP - Connection Retry Timer Expired for the BGP Connection with Peer No. %d	460019	Low	Normal	This message is generated when the Connection Retry Timer has expired while establishing the TCP connection with a particular peer.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - KEEPALIVE Message %s Peer No. %d	460020	Debug	Normal	KEEPALIVE Message <operation> to/from Peer No. <peer_id> This message is generated when BGP KeepAlive Message is sent or received to/from a BGP Peer <operation> can be either "Sent" or "Received"		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - OPEN Message %s Peer No. %d [Ver: %d AS: %d HldTm: %d BgpID: %s AuthInfo: %d %s]	460021	Debug	Normal	OPEN Message <operation> to/from Peer No. <peer_id> [Ver: <version> AS: <as_num> HldTm: <hold_time> BgpID: <bgp_id> AuthCode: <auth_code> AuthData: <auth_data> This message is generated when BGP Open Message is sent or received to/from BGP Peer with the specified contents. <version> - version number; can be 3 or 4 <as_num> - AS Number <hold_time> - Hold Time Proposed <bgp_id> - BGP Identifier <auth_code> - Authentication Code; 1 for "Simple Password" Scheme, 0 for "None" <auth_data> - 16 byte password string for "Simple Password" Scheme, NULL for "None"		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - NOTIFY Message %s Peer No. %d [ErrCode: %d ErrSubcode: %d ErrData: %s]	460022	Debug		NOTIFY Message <operation> to/from Peer No. <peer_id> [ErrCode: <err_code> ErrSubcode: <err_subcode> ErrData: <err_data> This message is generated when BGP Notify Message is sent or received to/from BGP Peer with the specified contents. <err_code> - Error Code indicating the type of error; can be any value between 1-6. <err_subcode>- Error Subcode providing the more specific information about the error; can be any value between 0-11 depending upon the error code. <err_data> - Error specific Data, depending upon the error code & subcode. 0 for error codes/subcodes for which Error Data is not needed or notified.		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - FSM State Changed on BGP connection with Peer No. %d [CurrState: %d Event: %d NewState: %d]	460023	Debug	Normal	This message is generated when FSM state is changed on the BGP connection with the peer. <curr_state> - indicates the current state of the BGP connection FSM; can be any value between 1-6 <curr_event> - indicates the event occurred which has caused the FSM state change; can be any value between 1-13 <new_state> - indicates the new state of the BGP connection FSM; can be any value between 1-6 depending on the current state and event occurred		This is an information message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Error in UPDATE Message Received from Peer No. %d - %s, %d	460024	High	Warning	This report is generated when UPDATE message with erroneous/ unexpected/unacceptable value in one of the UPDATE message fields, is received from a peer. <err_msg> indicates the exact error and can be one of the following. Malformed Attribute List, Unfeasible Route Length too Large; <err_val> indicates the erroneous unfeasible route length Malformed Attribute List, Total Attribute Length too Large; <err_val> indicates the erroneous total attribute length Malformed Attribute List, Total NLRI Length too Large; <err_val> indicates the erroneous total NLRI length Malformed Attribute List, Duplicate Attribute in Attribute List; <err_val> indicates the duplicate attribute type code, which appears more than once.		Resolve the cause of erroneous data received from BGP Peer, as indicated by the alarm message.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Error in UPDATE Message Received from Peer No. %d - %s, %d (Continued)	460024 (Cont.)	High	Warning	Missing Well-known Attribute; <err_val> will indicate the missing attribute type code Missing Local-Pref Attribute in IBGP Update Attribute Flags Error; <err_val> indicates the erroneous attribute in format <attr_type>,<attr_len>, <attr_value> Attribute Length Error; <err_val> indicates the erroneous attribute in format <attr_type>,<attr_len>, <attr_value> Invalid ORIGIN Attribute; <err_val> indicates the erroneous attribute in format <attr_type>,<attr_len>, <attr_value> Invalid Network Field, Invalid Prefix Len in Withdrawn Routes; <err_val> indicates the invalid prefix len. Invalid Network Field, Invalid Prefix Len in Reachable Routes; <err_val> indicates the invalid prefix len		Resolve the cause of erroneous data received from BGP Peer, as indicated by the alarm message. (Continued)

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Error in UPDATE Message Received from Peer No. %d - %s, %d (Continued)	460024 (Cont.)	High	Warning	Malformed AS_PATH, Bad AS Type in AS Path Segment; <err_val> indicates the erroneous attribute in format <attr_type>,<attr_len>, <attr_value>; where <attr_value> is sequence of AS path segment in format <[<seg_type>, <seg_len>,<seg_val>], [seg_type>, <seg_len>,<seg_val>] ...>; where <seg_val> is space separated list of AS numbers. AS Routing Loop in AS Path; <err_val> indicates the erroneous attribute in format <attr_type>,<attr_len>, <attr_value> Local AS Already in AS Path; <err_val> indicates the erroneous attribute in format <attr_type>,<attr_len>, <attr_value> Invalid NEXT_HOP Attribute, Not a Valid IP Address; <err_val> indicates the erroneous attribute in format <attr_type>,<attr_len>, <attr_value>		Resolve the cause of erroneous data received from BGP Peer, as indicated by the alarm message. (Continued)

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP - Error in UPDATE Message Received from Peer No. %d - %s, %d (Continued)	460024 (Cont.)	High	Warning	Invalid NEXT_HOP Attribute, Same as Local BGP Speaker IP Address; <err_val> indicates the erroneous attribute in format <attr_type>,<attr_len>, <attr_value> Invalid NEXT_HOP Attribute, Nexthop not Present on the Shared Subnet between Peer & Local BGP Speaker and Indirect Peering is Not Allowed with the Peer; <err_val> indicates the erroneous attribute in format <attr_type>,<attr_len>, <attr_value> Unrecognized Well-known Attribute, Local Pref Attribute received from Internal Peer; <err_val> indicates the erroneous attribute in format <attr_type>,<attr_len>, <attr_value>		Resolve the cause of erroneous data received from BGP Peer, as indicated by the alarm message. (Continued)
Bd src prt fr nt x.x.x.x		Medium		x.x.x.x = network IP		For other nodes that do not have this feature, change the node IP Address.
addr X.X.X.X.-> omt ## conflicts with addr in other IP dev on LAN		Medium				For other nodes that do not have this feature, change the node IP Address.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
Running software is %sSize-%d bytes	17003	High		Prints version and size of image.		None.
BMM - BOARD KEEPALIVE FAILURE - BOARD: %D	462000	Medium		Board can not be kept alive any longer.		Reset board statistics in the slot. Adjust the board management parameters.
BMM - BOARD FAULT - BOARD: %d CAUSE: %s	462001	High		Display the cause for a board fault.		None.
BMM - BOARD DEACTIVATED - BOARD: %D	462002	Medium		Board has been deactivated by user.		None
BMM - BOARD ACTIVATED - BOARD %d	462003	Medium		Board is activated by user.		None
BOARD STATUS MSG SLOT (%d) - \r\n%s	462004	Medium		Display board status.		None
BOARD STATUS MSG SLOT (%d) - \r\n%s	1012	Medium		Display board status.		None
BOARD HIGH MSG SLOT (%d) - \r\n%s	462005	High		Miscellaneous board management messages.		Take action according to the messages printed.
BOARD HIGH MSG SLOT (%d) - \r\n%s	1013	High		Miscellaneous board management messages.		Take action according to the messages printed.
BOARD HIGH MSG SLOT *(n)* - VC_LIB *(n)* Packet		High		This error indicates that a buffers was being returned, but the structure of the buffer was not consistent. The buffer was to contain a “general event” but the owner of the buffer (which is stored in the buffer header) indicated that it was not a general event.		Contact Customer Service.
BOARD DEBUG MSG SLOT (%d) - \r\n%s	462006	Mux		Miscellaneous board debugging messages.		None

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BOARD DEBUG MSG SLOT (%d) - \r\n%s	1014	Mux		Miscellaneous board debugging messages.		None
BMM BOOTED	462007	Medium		Board management parameters have been refreshed by newly set values. Node will use new values to maintain all the boards		None
Serial board disabled by user	462008	Medium		Serial board has been disabled by the user.		None
Serial board enabled by user	462009	Medium		Serial board has been enabled by the user.		None
BMM record defaulted	462010	Medium		All board management parameters have been changed back to the default value.		None
HTTPD AUTHENTICATION FAILURE	461000	Medium		Prints authentication failure information.		None
HTTPD-Internal Error: %s	461001	Medium		Prints internal error messages.		None
HTTPD-General Error: %s	461002	Medium		Prints general web access error messages.		None
HTTPD-General Debug: %s	461003	Debug		Generates debug information.		None
%HTTPD_LOG:%s	461004	Medium		Generates web access log messages.		None
Invalid config of wildcard community profile in policy #xxx		High		This message indicates that there is an invalid community profile.		Remove the invalid community profile.
LUA SOCKET CONNECT FAILED	451000			This alarm indicates that memory allocation failed.		Reduce SNABSC device entries and/or other node configurations.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
INITIALIZATION FAILED - MODULE SNABSC NOT INCLUDED	452000			Appropriate SNABSC modules did not get included in an image.		Load the image that includes the appropriate SNABSC modules
SNABSC_CM CM SYSERR	452001			Internal error during device boot, enable or disable.		Reconfigure and reboot the device. This alarm should be reported to a customer service representative.
INSUFFICIENT MEMORY TO SUPPORT SNABSC_CM CONFIGURATION	452002			This alarm indicates that memory allocation failed.		Reduce SNABSC device entries and/or other node configurations.
No mem for dav xx int ETH yyy		Debug	Low	Debug Alarm - xx = dav entry number, yyy = LAN Port number.		This is an information message only. No corrective actions are required.
Not Enough Memory for BGP Community Attributes		High	Critical	This alarm indicates a memory problem.		Increase the Permanent Memory Heap Size, and if needed add more DRAM in the node.
Not Enough Permanent Memory for BGP->RIPv2 Route Import		High	Critical	This report is generated when not enough permanent memory is available for BGP->RIPv2 Redistribution. The redistribution is not operational.		Increase the Permanent Memory Heap Size, and if needed add more DRAM in the node. Note: Current Maximum of Global Heap Size is reviewed for adequacy, w.r.t. addition of this feature.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
Not Enough Dynamic Memory - *<err_msg>*		Critical	High	This report is generated when not enough dynamic memory is available for objects. *<err_msg>* specifies the consequence of memory allocation failure and can be one of the following:-BGP->RIPv2 route importing can not work-BGP->RIPv2 policy #%d onwards is not applicable.		a) Add more DRAM in the node.b) Disable some of the other features that are not currently being used.
Missing BGP/BGPRT module		High	Critical	This report is generated when BGP/BGPRT is not available in the node.		Add the BGP/BGPRT modules.
RIPv2 is not running in this node		High	Critical	This report is generated when the router interface is not running RIPv2 in the node.		Modify the router interface's IGP protocol.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
Configuration error - <*err_msg*>		High	Warning	Displayed at init time or after booting, if there is an invalid configuration. <*err_msg*> indicates the exact error message and can be one of the following.<Configuration Table>: Entry No. %d is Duplicate of Entry No. %d<Configuration Table>: Entry %d: Invalid Entry.<Configuration Record>: Invalid Record. In the above error messages, <Configuration Table> can be one of the following.BGP->RIPv2, Import, Policy Table<Configuration Record> is BGP->RIPv2 Global Parameters.		Change or delete the entry with the bad configuration
Route to <*net_prefix*>/ <*prefix_len*> withdrawn by BGP from RIPv2		Debug	Normal	This message is generated when a previously imported route to a specified NLRI is withdrawn by BGP from RIPv2.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
BGP Route to <*net_prefix*>/ <*prefix_len*> not imported into RIPv2 due to Deny Policy No. <*policy_no*>		Debug	Normal	This message is generated when a BGP route to a specified NLRI is not imported into RIPv2 due to matching the specified import Deny policy. <*policy_no*> Indicates the entry number of the matching policy. A value of 0 means the default import policy		This is an information message only. No corrective actions are required.
BGP Route to <*net_prefix*>/ <*prefix_len*> matched to BGP->RIPv2 import Permit policy No. <*policy_no*>		Debug	Normal	This message is generated when a BGP route to the specified NLRI is matched to the specified import permit policy. <*policy_no*> Indicates the entry number of the matching policy. A value of 0 means the default import policy.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
Configuration error:<*err_msg*>		High	Warning	Displayed at init time, if there is an invalid configuration. <*err_msg*> indicates the exact configuration error and can be one of the following errors.BGP Aggregation: No Profiles configured. Aggregation and Proxy Aggregation disabled.Aggregation Profile: Entry %d is a Duplicate entry %d.Aggregation Profile: Specific Net and Suppressed Net are conflicted in entry %d.Aggregation Profile: Aggregate networks in entry %d is a suppressed network in entry %d.		Correct the bad configuration.
Aggregate route <*net_prefix*>/ <*prefix_len*> is created		Low	Normal	This message is displayed when an aggregate route is created		This is an information message only. No corrective actions are required.
Route <*net_prefix*>/ <*prefix_len*> is used to create aggregate route <*net_prefix*>/ <*prefix_len*>		Low	Normal	This message is displayed when a specific route is used to create an aggregate route.		This is an information message only. No corrective actions are required.
Route <*net_prefix*>/*prefix_len*> is not used to create aggregate route <*net_prefix*>/<*prefix_len*>		Low	Normal	This message is displayed when specific route that satisfies an aggregation profile entry cannot join an aggregate route due to various reason.		This is an information message only. No corrective actions are required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
Aggregate route <*net_prefix*>/<*prefix_len*> is deleted because only one specific route is left		Low	Normal	This message is displayed when an aggregate route is deleted due to not enough specific routes.		This is an information message only. No corrective actions are required.
Aggregate route <*net_prefix*>/<*prefix_len*> is created, matching Profile entry %d		Debug	Normal	This message is displayed when an aggregate route is created.		This is an information message only. No corrective actions are required.
Route <*net_prefix*>/<*prefix_len*> is used to create aggregate route <*net_prefix*>/<*prefix_len*>, matching Profile entry %d		Debug	Normal	This message is displayed when a specific route joins an aggregate route.		This is an information message only. No corrective actions are required.
Route <*net_prefix*>/*prefix_len*> is not used to create aggregate route <*net_prefix*>/<*prefix_len*> due to <*err_msg*> even matching Profile entry %d.		Debug	Normal	This message is displayed when specific route that satisfies an aggregation Profile entry cannot join an aggregate route due to some reason.The <*err_msg*> could be one of following:- MED difference- NEXT_HOP difference		This is an information message only. No corrective actions are required.
Route not advertised to peer #*xxx* due to community #*xxx*		Medium				Contact Vanguard Customer Service.
Specific route <*net_prefix*>/<*prefix_len*> is sent to peers due to the permission of <*msg*>		Debug	Normal	This message is displayed when a specific route is sent to peers. The <*msg*> is: <*Aggregation Profile*> Entry %d.		This is an information message only. No corrective actions are required.

Chapter 14
DHCP, RADIUS, VLAN, VRRP, PPP QoS and PPPo(X) Alarms and Reports

Overview

Introduction

This chapter describes Vanguard DHCP, RADIUS, VLAN, VRRP and PPPoE alarm messages and informational notices and reports. These alarms are generated with release 6.3 or greater software. If trap numbers are available, the alarms are listed in numerical order.

Release 6.4 and greater supports PPPo(X), where (X) refers to either PPP over ATM (PPPoA), PPP over Frame Relay (PPPoFR) or PPP over Ethernet over ATM over DSL (PPPoEoA) over DSL. G.SHDSL and MLP QoS are also supported with Release 6.4 and greater software.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
dhcp int *(intf)* lease *(ipadd)* for *(dur)* from *(serv)*		High		This message is generated when the DHCP client interface *(intf)* has obtained a lease of IP address *(ipaddr)* for *(dur)* seconds from the server IP address *(serv)*.		This is an information message only. No corrective action is required.
dhcp int *(intf)* no resp to discover		High		This message is generated when the DHCP client interface *(intf)* has not received a response to it's DHCPDISCOVER message.		Check the DHCP Server, make sure it is operating and that it is reachable by the node.
dhcp int *(intf)* no resp to request from *(serv)*		High		This message is generated when the DHCP client interface (intf) has not received a response to it's DHCPREQUEST message to server *(serv)*.		Check the DHCP Server, make sure it is operating and that it is reachable by the node.
dhcp int *(intf)* rcv nak from *(serv)* - *(msg)*		High		This message is generated when the DHCP client interface *(intf)* has received a DHCPNAK message fro the server *(serv)*. *(msg)* is the content of the "message" option, which may optionally be provided by the server in the DHCPNAK message.		Check that the Server and Client are configured properly.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
dhcp int *(intf)* retx *(msg)* *(n)* times in *(state)* to *(serv)*		Medium		This message is generated when the DHCP client interface *(intf)* is retransmitted *(msg)* for the *(n)th* time in state *(state)* to server *(serv)*. *(msg)* is one of: Discover or Request. *(state)* is one of: Selecting, Requesting, Renewing, Rebinding, Init-Reboot, Rebooting.		Check that the DHCP server is operating and is reachable by the node.
dhcp int *(intf)* renewing with *(serv)*		Low		This message is generated when the timer T1 has expired and the DHCP client interface *(intf)* has started the process of renewing it's lease with the server *(serv)*.		This is an informational message only. No corrective action is required.
dhcp int *(intf)* rebinding		High		This message is generated when the timer T2 has expired and the DHCP client interface *(intf)* has started the process of renewing it's lease with the server *(serv)*.		Check that the DHCP server is operating and is reachable by the node.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
dhcp int *(intf)* snd decline to *(serv)* - *(reason)*		High		This alarm message indicates that the client has declined an address offered by the server. The value *(intf)* identifies the IP interface. The value *(serv)* identifies the server sending the DHCPACK we are declining and the value *(reason)* is a string which identifies the reason we are declining the offer.		This is an informational message only. No corrective action is required. The server should mark the address as already in use and the client should be assigned another address the next time it requires one.
dhcp int *(intf)* lease expired		High		This alarm message indicates that the lease for IP interface *(intf)* has expired. The interface no longer has a valid IP address.		Confirm that the DHCP server is reachable by the client.
dhcp int *(intf)* unsp opts in *(msg)* from *(serv) : (opt), ...*		Debug		A DHCPOFFER or DHCPACK received from a server contains options not recognized by the DHCP client. The value *(intf)* identifies the IP interface. The value *(msg)* is one of: OFFER, ACK and the value *(serv)* is the address of the server that sends the message. The value *(opt)* is a list of the unknown option codes represented in hex.		Debug Alarm.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
dhcp int *(intf)* rcvd bad fmt *(msg)* from *(serv)- (reason)*		Medium		This alarm message indicates that the DHCP client has received an improperly formatted message from the server. The value *(intf)* identifies the IP interface. The value *(msg)* identifies the message type from the server and is on of: Offer, ACK, NAK. The value *(serv)* is the address of the server the message was from, and the *(reason)* is the reason the message was considered not formatted correctly.		Confirm that the DHCP server is reachable by the client.
dhcp int *(intf)* state change from *(fromstate)* to *(tostate)*		Debug		This alarm message is generated when the DHCP client moves from on state to another. The value *(intf)* identifies the IP interface. The value *(fromstate)* is the state the DHCP client was in and the *(tostate)* is the new state the DHCP client is entering. The values for the states are one of: INIT, Selecting, Requesting, Bound, Renewing, Rebinding, INIT-Reboot, ReBooting.		This is an informational message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
Radius Client Boot Complete		High		This alarm message is generated when the Boot RADIUS client has been completed.		This is an informational message only. No corrective action is required.
Radius Client Boot Failure		High		This alarm message is generated if the RADIUS boot fails. The fail reason can be RADIUS not enabled, no CMEM configuration for RADIUS client, etc....		Contact Vanguard Managed Solutions Customer Service.
Radius Failed		High		This alarm message is generated when the system runs out of resources and cannot generate any further report.		Contact Vanguard Managed Solutions Customer Service.
Bad Radius Response		Medium		This alarm message is generated when an invalid RADIUS response is received.		This is an informational message only. No corrective action is required.
Radius *(Authentication, Authorization, Accounting)* Timeout		Medium		This alarm message is generated when a timeout occurs.		This is an informational message only. No corrective action is required.
ETH.41 Priority mapping profile *(profnum)* not configured		Medium		This alarm message is printed when you configure a Ethernet mapping profile in the port configuration and have not configured the mapping profile itself. This is usually seen at a boot time. (VLAN)		Configure the appropriate profile or disable mapping on the port.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
ETH.42 disc vlan frame with cfi set on port *(n)* vlan *(m)*		Medium		This alarm message is generated when a frame has been received on the specified Ethernet port with the CFI bit set in the 802.1Q tag. The frame has been discarded.		Vanguard routers do not support the CFI bit. Reconfigure the attached equipment that is sending frames with the CFI bit set.
ARP.23 Rcv VID *(vid)* fm diff cfg *(vid)*				This alarm message is generated when the VLAN ID in the received frame is different for the configured VLAN ID, which should be the same since they are on the same subnet.		Correct the configuration.
MULTICLASS FAILURE		High		Cause: 1.) LOCAL PRIORITY DISABLED 2.) Rx NEGOTIATION FAILED 3.) LINK-BUNDLE MISMATCH Cause: 1.) PPP port negotiated Multiclass support but bundle Priority is disabled. 2.) Rx negotiation failed. Possible cause is mismatch in number of supported classes or peer does not support the long sequence number format. 3.) Options negotiated by this link differ from ones negotiated by already joined links.		1.) Port with negotiated Multiclass support is joining to bundle without Priority enabled. 2.) Link is configured to support Multiclass but multiclass is not negotiated 3.) Port is joining to the bundle without Multiclass support or with mismatching parameters.**Correct above by:** 1.a) Multiclass required: Set bundle Priority to ENABLE 1.b) Multiclass not required: Set port Multiclass to DISABLE 2.) Match number of supported classes between MLP peers. 3.) Configure the port to match the configuration of other links.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
PACKET REASSEMBLY FAILURE		Low		This alarm message is generated when one or more segments are lost and the packet reassembly cannot be completed. This occurs when segment loss is detected, imput queue is full or a timeout. When an MLP packet reassembly fails, an alarm message is released indicating that the reassembler is unsynchronized.		Check the links.
PACKET REASSEMBLY FAILURE THRESHOLD REACHED		High		This alarm message indicates the number of lost or discarded segments reached in the configured threshold. When one or more segments are lost, packet reassembly cannot be completed and segments already or subsequently received, that belong to uncompleted packet or packets, must be discarded. Caused by a timeout or full queue.		Check the links. **■ Note** Counting of un-received segments is based on certain assumptions and does not guaranty absolute accuracy. For instance, in case of continuous loss of segments without reception of valid segment the exact number of un-received segments cannot be determined. The loss will be detected by the timeout mechanism but the counter is incremented only for number of received and discarded segments.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
PACKET REASSEMBLY RESUMED		Low		This alarm indicates that the packet is successfully reassembled after one or more failures. Reassembled packets occur after a failure condition.		None.
Port/Station identifier - FAILED TO MAKE STACK CONNECTION		Medium		This alarm indicates that one minute has elapsed without a connection being established while configured for stacking support.		Verify the configuration of both PPP port and either FRI or AAM station is set to stacking support.
PPP - *port number*, PACKET RECEIVED FROM PEER WITH INVALID ENCAPSULATION		Medium		This alarm indicates that a packet was received from the peer with an encapsulation that does not match the configured encapsulation.		Verify encapsulation for PPPo*(X)* is set to the same setting in both peers.
PPP - *port number*, PPPoE SESSION *session id* TERMINATED *cause*		High		PPPoE session terminated. In addition to the alarm message an optional string with explanation about the reason may be shown. Event: PADT packet sent by the AC has been received. PPP terminated the session. The reason for termination may be: Connection loss detected, Idle link detected, (only when Auto Connect is disabled), some PPP problem, some PPPoE problem.		This is an informational message only. No corrective action is required.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
PPP - *port number*, PPPoE *session id*, DISCOVERY STAGE COMPLETED		Medium		This alarm message is generated when a PPPoE Discovery stage has been completed. Event: Valid PADS packet sent by AC has been received.		This is an informational message only. No corrective action is required.
PPP - *port number*, PPPoE DISCOVERY FAILED-CONFIGURED PARAMETER *Service-Name* or *AC-Name* CAN NOT BE MATCHED.		Medium		This alarm message is generated when PPPoE Discovery stage failed, no appropriate PADO packet has been received. When the total count of received PADO packets is zero, configured Service-Name cannot be matched or no AC is available. If the count is greater than zero, the configured AC-Name cannot be matched. Event: Tmax PADO waiting timeout has been reached.		Check the Service - Name and or AC-Name configuration parameters.
PPP - *port number*, PPPoE DISCOVERY FAILED - NO PADS FROM *AC_Name*		Medium		This alarm message is generated when the PPPoE Discovery stage failed, no response from the selected AC. Event: Tmax PADS waiting timeout has been reached.		Check the Service - Name configuration parameter.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
PPP - *port number*, PPPoE SERVICE NAME ERROR - *optional string*		High		The AC has sent this tag indicating that the requested Service-Name cannot be honored. If available in the TAG, an explanation of the problem is shown. Event: Service Name Error tag has been received.		Check the service - Name configuration parameter.
PPP - *port number*, PPPoE AC SYSTEM ERROR - *optional string*		High		The AC experienced some error in performing the client request. If available in the TAG, an explanation of the nature of the problem is shown. Event: AC System Error tag has been received.		Interpret the explanation of the problem.
PPP - *port number*, PPPoE GENERIC ERROR - *explanation string*		High		The AC has been sent to this tag to indicate that some unrecoverable error has occurred. If available in the TAG, an explanation of the nature of the problem is shown. Event: Generic Error tag has been received.		Interpret the explanation of the error.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
PPP - *port number*, PPPoE Configuration Error		High		PPPoE configuration cannot be completed. Some component is not available or not enough resources are. Example: specified port is not Ethernet type, or maximum number of PPPoE sessions has been already configured at a specified port. Event: Configuration completed		Check the Ethernet, PPP and PPPoE configurations.
PPP - *port number*, PPPoE Initialization Failure		High		PPPoE initialization cannot be completed. Some component is not available or not enough resources are available.		Check the Ethernet, PPP and PPPoE configurations.
SNMP Alarm/Trap for Node Configuration	5002			1. This will generate traps for all of configuration changes such as, Configurations, Default Node, Delete configuration records 2. To get the traps mentioned on the number 1, you need to enable a configuration parameter defaulted "Disabled", Menu.6.1-Configuration Change Alarm. 3. The trap number is 5002 for all the cases above.		Whenever user makes configuration changes in Vanguard Node (either via CTP/Telnet/CLI/Embedded Wed, or TFTP)... User can enable and disable this Alarm/ Trap based on his needs.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	Corrective Action
Station identifier - SOCKET SELECT ATTEMPT WHILE IN STACKING MODE		Medium		This message indicates that a Socket select request was received from router (due to PVC configuration) while the station is configured for stacking support.		No action is necessary for proper Stacking support operation. The PVC entry should be removed in order for the alarm to not appear anymore. If stacking support is not the desired method of operation, disable the stacking support in the station configuration.
vrrp : duplicate VRID *(vrid)* on int *(intf)*		High		The VRRP interface (*intf*) has duplicate instances of the same VRID (*vrid*)		VRRP has been misconfigured. Change the configuration for the proper operation.
vrrp : address<*addr*> cannot be configured on int (*intf*) vrid (*vrid*)		High		The VRRP interface (*intf*) and vrid (*vrid*) owns the configured secondary virtual address <*addr*> even though it does not own the primary address.		VRRP has been misconfigured. Change the configuration to ensure that the VRRP router can only own virtual ip(s) 2 to 16 if it also owns virtual ip 1.
vrrp : failed to allocate memory for a VRRP structure		High		The router could not allocate memory for a VRRP structure. The structure may be one of VRRP_CB, VRRP_GROUP or VRRP_GRP_ELEMENT.		The node is low on memory. Try rebooting the system. If the problem reoccurs contact customer service and report the alarm.
vrrp : virtual ip (*addr*) matches real address on int (*intf*)		High		The router received a packet with one of the advertised addresses corresponding to the real address on the routers interface (*intf*)		This indicates a VRRP misconfiguration. If multiple addresses are configured, the secondary address(es) should only be equal to the real address(es) on a VRRP router if that router also owns the primary address.

Alarm Text	Trap No.	Priority	Severity	Description	Cleared By:	
vrrp : int (*intf*) vrid (*vrid*) invalid authentication from (*ip_addr*)		Medium		The VRRP router defined by (*intf*) (*vrid*) received an improperly authenticated message from (*ip_addr*)		Config on the (*ip_ad*
vrrp : int (*intf*) vrid (*vrid*) ip address mismatch		Medium		The VRRP router defined by (*intf*) (*vrid*) has received a VRRP packet with a different set of IP Address(es) than the ones it already has.		A VRR miscon Every in the s identic combin
vrrp : int (*intf*) vrid (*vrid*) advertisement interval mismatch		Medium		The VRRP router defined by (*intf*) (*vrid*) received an advertisement with an advertisement interval that differs from its own configured interval.		Change interva consist in the g the lea enable
vrrp : int (*intf*) vrid (*vrid*) pkt discarded due to (*reason*)		Low		The VRRP router defined by (*intf*) (*vrid*) discarded a packet due to (*reason*). The reason would provide details as to why the packet was discarded (i.e invalid TTL, checksum error, incorrect version, packet length etc.).		Depen occurre be a pr frequen service details.
vrrp : int (*intf*) vrid (*vrid*) state change from (*old_state*) to (*new_state*)		Low		The VRRP router defined by (*intf*) (*vrid*) has changed state from (*old_state*) to (*new_state*).		This is only. N require
vrrp : int (*intf*) vrid (*vrid*) advertisement sent		Debug		The VRRP router defined by (*intf*) (*vrid*) sent an advertisement.		This is only. N require
vrrp : int (*intf*) vrid (*vrid*) advertisement recvd from (*ip_addr*)		Debug		The VRRP router defined by (*intf*) (*vrid*) received an advertisement from (*ip_addr*).		This is only. N require
vrrp : int (*intf*) vrid (*vrid*) gen debug (*detail*)		Debug		The VRRP router defined by (*intf*) (*vrid*) has reported a general informational message for debugging purposes. The nature of the message is specified by (*detail*).		This is only. N require

Trap Number	Page
386	10-25
1000	7-18
1001	7-18
1002	7-11
1003	10-67
1004	10-67
1005	6-2
1006	6-4
1007	6-4
1008	6-5
1009	6-5
1011	6-5
1012	13-38
1013	13-38
1014	13-39
1300	10-144
2000	2-38
2001	2-40
2004	2-15
2005	2-25
2006	2-98
2007	2-97
2008	2-97
2010	11-3
2011	11-3
3000	2-2
3001	10-144
3002	10-144
4000	7-5
4001	7-6
4002	10-134
4003	10-83
5000	10-40
5001	10-40
5002	14-12
6001	10-55
6002	10-55
6003	10-136
6004	10-135
6005	10-135
6006	2-111

Trap Number	Page
6007	2-92
6008	2-92
6009	2-91
6010	2-92
6011	2-91
6012	2-92
6013	10-111
6014	10-111
6015	10-111
6016	10-111
6017	2-92
6018	2-92
6019	10-43
6020	10-43
6021	7-16
6022	10-87
6024	10-71
6032	10-71
9000	10-106
9001	6-5
9001	10-64
9002	10-65
9002	11-3
9003	10-65
9003	11-3
15001	10-82
16000	10-39
16001	10-44
16002	4-11
16003	4-12
16003	4-12
16004	10-84
16005	10-84
16019	6-5
16019	10-102
16021	10-143
16021	11-3
16022	10-143
16023	10-143
17000	2-71
17001	2-62
17002	10-40

Trap Index

Trap Number	Page
17003	13-38
19000	7-17
19001	10-85
19002	10-83
19003	10-85
19004	10-85
19005	10-84
19006	10-86
19007	7-9
19008	7-8
19009	2-4
19010	2-9
19011	2-4
19012	7-13
19013	2-41
19014	7-15
19015	7-5
19016	10-134
19017	2-26
19018	10-86
19021	11-3
20006	2-21
20007	2-20
20008	2-20
20009	2-21
20009	2-21
20020	2-91
20021	2-91
20022	2-91
21000	10-84
25000	10-106
25000	10-106
32000	10-31
33000	10-44
33001	10-46
33002	10-46
33003	10-47
33004	10-47
33005	10-45
33006	10-48
33007	10-49
33008	10-49

Trap Number	Page
33009	10-49
33010	10-48
33011	10-46
33012	10-45
33013	10-46
33014	10-44
33015	10-48
33016	10-45
33017	10-49
33018	10-47
33019	10-49
33020	10-49
33021	10-45
33022	10-46
33023	10-45
39000	2-34
39001	2-48
39002	2-52
39003	2-58
40000	10-7
40001	10-8
41000	10-7
41001	10-8
42000	10-80
42001	10-43
42002	10-26
42003	10-22
42004	10-25
42005	2-23
42006	2-22
42007	2-28
42008	2-28
42009	2-14
42010	2-2
42011	2-13
42012	2-11
42013	2-12
42014	2-32
43000	10-81
43001	10-44
43002	10-26
43003	10-22

Trap Number	Page
43004	10-26
43005	2-23
43006	2-22
43007	2-29
43008	2-28
43009	2-14
43010	10-24
43011	2-13
43012	2-12
43013	2-12
43014	2-32
44000	2-25
44002	2-24
44003	2-15
44004	2-31
44005	2-77
44006	2-32
44007	2-76
44008	2-90
44009	2-90
44010	2-89
44011	2-89
46000	2-33
46001	4-4
46002	4-4
46003	4-2
46004	10-28
46005	10-2
46007	10-134
46008	10-28
46009	10-28
46010	4-3
46011	10-72
46012	10-89
46013	10-22
46014	7-12
46016	10-139
46016	11-3
49000	2-34
49001	2-40
49002	2-52
49003	2-58

Trap Number	Page
49004	2-71
49005	2-62
49006	2-68
51000	2-34
51001	2-41
51002	2-98
51003	2-98
51004	2-99
51005	2-99
51006	4-5
56000	2-34
56001	2-42
56002	2-52
56003	2-58
56004	2-56
56005	2-30
56006	2-20
56007	2-71
56008	2-67
57000	2-34
57001	2-43
57002	2-52
57003	2-58
57004	2-56
57005	5-2
57006	5-2
57007	7-14
57008	7-14
57009	7-8
57010	7-8
57011	2-68
57012	7-8
57013	7-7
57014	7-8
57015	7-8
57016	7-7
57016	10-43
57017	7-7
57017	10-43
59000	10-88
61000	2-62
65000	10-3

Trap Index

Trap Number	Page
65001	10-38
68000	10-86
68001	3-43
68002	3-43
68003	10-27
68004	10-69
68005	10-22
68006	10-82
68007	7-15
68008	10-27
68009	10-26
68010	3-25
68011	7-15
69000	2-35
69001	2-84
69002	2-85
69004	3-36
69005	3-37
69006	2-71
69007	2-62
69008	3-42
69009	3-21
69010	3-37
69011	3-36
69012	3-32
69013	2-38
69014	2-55
69015	2-50
69016	2-49
69017	3-23
69018	2-49
69019	2-68
74000	2-35
74001	2-41
74002	2-52
74003	2-50
74004	2-58
74005	2-57
74006	3-20
74007	3-19
74008	3-27
74009	3-24

Trap Number	Page
74010	3-25
74011	3-38
74012	2-71
74013	2-63
74014	2-49
74015	2-49
74016	3-42
74017	3-23
74018	2-68
74019	3-12
74020	3-29
74021	3-6
74022	3-4
74023	3-5
75001	3-13
75002	3-13
75003	3-13
75004	3-12
75005	3-14
75006	3-27
75007	3-25
75008	3-27
75009	3-14
75010	3-16
75011	3-16
75012	3-16
75013	3-16
75014	3-28
75015	3-28
75016	3-18
76000	10-90
76001	10-90
76002	10-90
76003	10-90
76004	3-41
76005	3-41
76006	3-31
76007	3-31
86000	2-35
86001	2-39
86002	2-53
86003	2-59

Trap Number	Page
86004	2-55
86005	2-30
86006	2-31
86007	2-27
86008	2-28
86009	2-18
86010	2-18
86011	2-19
86012	2-29
86013	2-29
87000	2-79
87001	3-30
87002	3-6
87005	3-29
87006	3-29
87008	3-12
87011	3-2
87012	3-3
87014	2-79
87015	2-81
87016	2-80
87017	2-89
87018	3-3
87019	3-3
87020	2-21
88000	2-81
88001	2-84
88002	2-84
88003	2-85
88004	2-88
88005	3-37
88006	3-38
88007	3-33
88008	3-35
88009	2-87
88010	2-87
88011	3-40
88014	3-41
90000	10-21
91000	10-83
91001	10-38
91002	10-100

Trap Number	Page
91003	10-99
91004	10-99
91005	10-101
91006	10-100
91007	10-100
92000	10-101
92001	10-100
97000	2-35
97001	2-39
97002	2-53
97003	2-59
97004	2-56
97005	2-51
104000	7-4
105000	10-39
105001	10-37
105002	10-39
105003	10-66
105004	10-134
105005	10-106
105006	10-67
105007	10-67
105008	7-4
105009	7-5
105010	10-67
105011	7-4
105012	7-5
105013	10-39
105014	10-81
105015	10-81
106000	10-38
106001	10-106
106002	7-29
106003	7-16
107000	2-86
107001	2-93
107002	2-93
107003	2-93
108000	2-63
108001	10-8
108002	10-8
108003	10-4

Trap Index

Trap Number	Page
108004	10-3
109000	2-63
110000	2-35
110001	2-43
110002	2-53
110003	2-59
110004	2-56
110005	2-31
110006	2-31
110007	2-27
110008	7-14
110009	3-19
110010	3-26
110011	3-32
110012	10-111
110013	3-15
110014	3-15
110015	3-17
110016	2-25
111001	3-44
111002	3-44
111003	3-44
111004	3-43
111005	3-45
111006	3-27
111007	3-45
111008	3-45
111009	3-47
111010	3-46
111011	3-46
111012	3-47
111013	3-46
112000	2-35
112001	2-44
112002	2-53
112003	2-51
112004	2-59
112005	2-57
112006	3-20
112007	3-22
112007	3-23
112008	3-24

Trap Number	Page
112009	3-24
112010	3-25
112011	3-20
112012	2-72
112014	3-20
112015	2-67
112016	3-27
112017	2-33
112018	2-76
112019	3-6
112020	3-6
112021	3-5
112022	3-5
112023	10-143
115000	7-2
115001	10-2
115002	10-2
115003	10-2
115004	4-2
115005	4-2
115006	4-2
115007	10-9
116000	10-4
116001	10-43
116002	10-9
116003	4-2
116004	4-2
116005	4-9
116006	10-9
125000	2-36
125001	2-45
125002	2-53
125003	2-59
125004	2-56
125005	10-10
125006	10-11
125007	7-14
125008	7-14
125009	3-20
125010	3-26
125011	3-42
125012	10-88

Trap Number	Page
126000	2-36
126001	2-45
126002	2-53
126004	2-59
126006	2-72
126008	2-49
126010	2-69
129000	2-98
129001	2-77
129002	2-85
129004	10-88
130001	10-103
130002	10-133
130003	10-133
130004	2-99
134000	10-36
134001	10-37
134002	10-37
134003	10-37
134004	10-37
134005	10-37
134006	10-37
134007	10-65
136000	10-34
136001	10-32
136002	10-33
136003	10-33
136004	10-33
136005	10-33
137000	10-80
137001	10-36
137002	10-36
137003	10-127
137004	10-127
137005	2-2
137006	2-2
138000	2-107
138001	2-107
138002	2-107
138003	2-108
138004	2-108
138005	2-110

Trap Number	Page
138006	2-106
138007	2-106
138008	2-105
138010	2-110
138011	2-110
138012	2-104
138013	2-105
138014	2-106
138015	2-105
138016	2-108
138017	2-104
138018	2-106
138019	2-106
138020	2-108
138021	2-108
138022	2-107
138023	2-109
138024	2-109
138025	2-109
138026	2-105
139000	2-81
139002	2-86
139003	2-84
139004	2-87
139005	2-75
141000	2-78
141001	2-80
150000	2-36
150001	2-39
150002	2-54
150003	2-59
150004	2-56
150005	2-17
150006	2-30
151000	10-105
151001	10-105
151002	10-104
151003	10-105
151006	10-104
151007	11-3
152000	10-7
152001	10-9

Trap Index

Trap Number	Page
152002	10-8
152003	10-9
152004	10-9
152005	10-9
153000	10-106
153001	10-106
153002	10-105
153003	10-105
154000	10-102
154001	10-102
154002	10-102
155000	10-81
155001	5-2
155002	5-2
155003	5-3
156000	10-3
156001	10-6
156002	10-6
156003	10-6
156004	10-6
156005	10-5
156006	10-5
156007	10-5
156008	10-3
156009	10-3
156010	10-4
156011	10-89
156012	10-88
157000	10-8
157001	10-6
157002	10-9
157003	10-3
159000	10-8
159001	10-7
162000	10-87
162001	10-87
162002	10-87
173000	10-85
174000	10-60
174002	10-59
174003	10-59
174004	10-59

Trap Number	Page
174005	10-59
174006	10-57
174007	10-58
174008	10-58
174009	10-57
174010	10-58
174011	10-58
174012	10-58
174013	10-60
174014	10-59
174015	10-60
174016	10-60
174017	10-57
174018	10-58
174019	10-59
174020	10-60
176000	10-11
176001	10-12
176002	10-14
176003	10-13
176004	10-14
176005	10-14
176006	10-102
177000	2-80
177001	2-80
177002	10-14
177003	10-15
177004	10-16
177005	10-16
177006	10-17
177007	10-16
177008	10-17
177009	10-17
177010	10-88
177011	10-15
177012	10-16
177013	10-15
178000	10-13
178001	10-15
178002	10-82
186000	2-36
186001	2-46

Trap Number	Page
186002	2-54
186003	2-60
186004	2-72
186005	3-19
186006	3-26
186007	3-21
186008	3-23
186009	2-70
186011	7-17
187000	2-22
187001	3-16
187002	10-68
187006	2-80
187008	2-81
187009	2-81
187011	3-33
187012	3-37
188000	10-3
188001	10-7
188002	10-80
188003	10-80
188004	10-80
189000	10-6
191000	10-7
192000	3-4
193000	2-81
193002	2-86
193003	2-84
193004	2-87
195000	7-15
195001	10-44
195002	10-26
195003	10-22
195004	10-26
195005	2-23
195006	2-23
195007	2-29
195008	2-28
195009	2-14
195010	7-3
195011	2-14
195012	2-12

Trap Number	Page
195013	2-12
195014	2-33
196000	2-82
196001	2-82
196002	2-85
196003	2-86
196004	2-88
196005	2-87
196006	2-93
198000	10-123
198001	10-123
198002	10-123
198003	10-124
198004	10-124
198005	10-124
198006	10-124
198007	10-123
198008	10-123
198009	10-123
198010	10-122
198011	10-124
198012	10-123
202000	10-52
202001	10-134
202002	10-73
202003	7-16
202006	7-16
202007	7-17
202008	7-16
202008	7-16
206000	10-135
207003	9-19
207004	9-19
207005	9-19
207006	9-20
207007	9-20
207007	13-2
207008	9-20
207008	13-2
207009	9-20
207009	13-2
207010	9-20

Trap Index

Trap Number	Page
207010	13-3
210000	7-13
210000	7-13
210000	7-27
210003	10-66
210004	10-101
211000	7-3
211001	10-10
211002	7-10
211003	7-15
211004	7-10
215000	2-22
215001	2-17
215002	2-20
215003	2-26
215004	2-19
215005	2-28
215006	2-32
215007	2-25
215008	2-16
215009	2-16
215010	2-27
215011	2-27
215012	2-19
215013	2-24
215014	2-18
215015	2-75
215016	2-75
215017	2-77
215018	2-76
215019	2-24
215020	2-26
215021	2-67
215022	2-17
215023	2-18
216000	2-36
216001	2-48
216002	2-54
216003	2-52
216004	2-60
216005	2-57
216007	2-72

Trap Number	Page
218000	2-79
218001	2-78
219000	2-82
219001	2-83
219002	2-85
219003	2-86
219004	2-72
219005	2-69
219006	2-64
222000	3-40
222001	3-32
222002	3-40
222003	3-33
222004	10-101
222005	3-31
225001	3-4
226000	3-33
226001	3-34
226002	3-36
226003	3-36
226004	3-32
226005	3-38
226007	3-31
226009	3-2
226009	11-3
226010	3-2
226010	11-3
226011	3-2
226011	11-3
226012	3-2
226012	11-4
226013	3-2
226013	11-4
226014	3-2
226014	11-4
226015	3-3
226015	11-4
226016	3-3
226016	11-4
226017	3-3
226018	3-3
226018	11-4

Trap Number	Page
226019	3-3
226019	11-4
227000	2-96
227001	2-96
227002	2-96
227003	2-95
227004	2-19
227005	2-13
227006	2-74
227007	2-16
227008	2-17
227009	2-30
227010	2-74
227011	2-74
227012	2-16
227013	2-75
227014	2-77
228000	2-36
228001	2-46
228002	2-54
228003	2-51
228004	2-60
228005	2-57
228006	2-50
228007	2-73
228008	2-69
229000	10-86
229000	10-86
229001	7-17
229002	10-86
229003	4-10
229004	4-10
229005	10-6
230000	7-30
230001	7-30
230002	7-14
230003	7-14
230004	7-27
230005	7-3
230006	7-3
230007	7-13
230008	7-29

Trap Number	Page
230009	2-100
230010	2-99
231000	2-36
231001	2-39
231002	2-60
231003	2-73
231005	2-70
231006	2-64
232000	10-4
233000	10-4
233001	10-5
234000	10-7
236000	10-29
236000	10-30
236001	7-17
236002	10-23
236003	10-23
236004	10-83
236006	2-8
236006	2-11
236010	10-39
241001	10-34
241002	10-36
241003	10-35
241004	10-34
241005	10-34
241006	10-35
241007	10-35
241008	10-35
241009	2-2
241010	2-2
241011	10-34
241012	4-2
241013	10-36
241014	10-34
241015	10-36
241016	10-55
241017	10-56
241018	10-56
241019	10-55
241020	10-56
241021	10-56

Trap Index

Trap Number	Page
241022	10-56
241023	10-56
241024	10-55
241025	10-56
241026	10-32
241027	10-2
241028	10-56
241029	10-103
241030	10-103
241031	10-103
241032	10-103
241033	10-103
241034	10-32
241035	10-57
241036	10-109
241037	10-56
241038	10-109
241039	10-57
241040	10-104
241041	10-104
241042	10-103
241043	10-38
241044	10-99
241045	10-38
241046	10-55
241047	10-55
241048	10-110
241049	10-110
241050	10-111
241051	10-111
241052	10-110
241053	10-110
241054	10-110
241055	10-109
241056	10-110
241057	10-110
241058	10-109
241059	10-109
241060	10-43
241061	10-38
242002	7-19
242003	2-9

Trap Number	Page
242004	10-109
242005	10-109
242006	10-125
242007	10-43
242008	10-82
242009	10-24
242013	6-10
242013	10-104
242014	6-10
242014	10-104
242015	6-5
242015	10-89
242020	10-142
242020	11-4
243000	2-37
243001	2-40
243002	2-54
243003	2-60
243004	2-70
245000	4-3
245001	4-3
245002	2-37
245003	2-46
245004	4-3
245005	2-54
245006	2-69
245007	2-73
245008	4-4
245009	4-3
245010	2-60
245011	4-4
245012	4-10
246000	10-87
248000	7-7
248001	7-6
248002	7-7
248003	7-7
248004	4-7
248005	4-7
248006	4-9
248007	4-5
248008	4-8

Trap Number	Page
248009	4-6
248010	4-7
248011	4-6
248012	4-6
248013	4-5
248014	4-8
248015	4-5
248016	4-7
248017	4-8
248018	4-8
248020	6-3
248021	6-4
248022	6-4
248025	6-2
248031	6-2
248032	6-3
248033	6-2
248034	6-2
248035	6-3
248037	6-3
248038	6-4
248039	6-3
250000	2-37
250001	2-48
250002	2-54
250003	2-51
250004	2-60
250005	2-57
250006	2-50
250007	2-73
250008	2-70
250009	2-3
250010	2-110
250011	2-104
251000	2-10
251001	2-10
251002	2-9
251003	2-10
252000	2-7
252001	2-4
252002	2-7
252003	2-6

Trap Number	Page
252004	2-5
252005	2-6
253000	10-51
253001	10-50
253002	10-50
253003	10-50
253004	10-50
253005	10-50
255002	4-2
256000	6-18
256001	6-21
256002	6-15
256003	6-20
256004	6-20
256005	6-21
256006	6-16
256007	6-20
256008	6-18
256009	6-25
256010	6-22
256011	6-15
256012	6-15
256013	6-16
256014	6-22
256015	6-26
256016	6-19
256017	6-21
256018	6-21
256019	6-22
256020	6-22
256021	6-23
256022	6-16
256023	6-19
256024	6-18
256025	6-15
256026	6-17
256027	6-25
256028	6-25
256029	6-23
256030	6-15
256031	6-16
256032	6-24

Trap Index

Trap Number	Page
256033	6-24
256034	6-27
256035	6-18
256036	6-27
256037	6-23
256038	6-19
256039	6-26
256040	6-26
256041	6-17
256042	6-17
256043	6-17
256044	6-24
256045	6-24
256046	6-25
256047	6-19
256048	6-20
256049	6-19
256050	6-18
256051	6-24
256052	6-17
256053	6-26
256054	6-23
256055	6-26
256056	6-14
256057	6-27
256058	6-14
257000	10-116
257000	10-117
257000	10-118
257001	10-113
257001	10-114
257001	10-115
259000	2-86
259001	2-92
259002	2-94
259003	2-93
261000	2-64
268000	2-37
268001	2-46
268002	2-55
268003	2-61
268004	2-73

Trap Number	Page
268005	2-70
268006	2-65
268007	2-13
268008	2-25
268009	2-19
270000	10-100
270001	6-28
270002	10-72
270003	10-82
270004	10-39
270005	10-41
270006	10-17
270007	10-42
270008	10-44
270009	10-100
270010	10-102
270011	10-2
270012	10-71
270013	10-83
270014	10-125
270015	10-21
270016	10-81
270017	10-66
270018	10-87
271000	10-5
271001	10-5
275000	4-5
278000	10-78
278001	10-78
278002	10-79
278003	10-71
278004	10-118
278005	10-78
278007	2-8
278008	10-36
278009	10-79
278010	10-79
278011	10-118
278012	4-10
278013	4-10
278014	10-79
278015	10-52

Trap Number	Page
278016	10-79
278021	11-4
278023	11-5
278024	11-5
278025	11-5
278026	11-5
278027	11-5
280000	7-11
280001	2-98
280002	2-66
280003	2-67
280004	2-47
280005	2-37
280006	2-55
280007	2-48
280008	2-33
280009	2-61
280010	2-33
280012	10-136
280013	10-136
280014	10-136
280015	10-136
280016	10-136
281000	7-18
281001	7-19
281002	2-99
281003	2-99
281004	10-52
281005	10-52
281006	10-137
281007	10-137
281008	4-9
281009	10-51
281010	10-51
281011	2-7
281011	10-51
281012	2-111
281012	2-112
281014	10-138
281015	2-112
281018	10-137
281019	10-137

Trap Number	Page
282000	2-34
282001	2-38
282002	2-55
282003	2-61
282004	2-66
282005	2-94
283001	10-112
283002	10-112
283003	7-3
283004	10-9
283005	10-112
283006	10-54
283007	7-2
283008	7-2
283009	10-10
283010	10-112
283011	10-89
283012	2-100
283013	2-100
283014	2-100
283015	2-100
283016	2-100
283017	2-101
283018	4-10
283019	4-10
283020	4-11
283021	4-11
283022	4-9
283023	4-9
283024	4-10
283025	10-89
283026	10-69
283027	10-112
283028	4-11
283029	2-8
283030	2-104
283032	2-104
283032	2-104
283033	10-89
285001	10-108
285002	10-108
285003	10-108

Trap Index

Trap Number	Page
285004	10-108
285005	10-107
285006	10-107
285007	10-108
285008	10-108
285009	10-107
286001	10-108
286002	10-108
289000	10-4
289001	10-5
289002	10-3
290000	10-4
290001	10-5
290002	3-12
291003	2-61
291004	2-74
291005	2-67
292000	10-4
292001	10-4
292002	10-6
293000	10-74
293001	10-75
293002	10-77
293003	10-78
293004	10-78
293005	10-78
293006	10-78
293007	10-78
293008	10-78
293009	10-74
293010	10-74
293011	10-74
293012	10-74
293013	10-74
293014	10-75
293015	10-75
293016	10-75
293017	10-75
293018	10-75
293019	10-75
293020	10-76
293021	10-76

Trap Number	Page
293022	10-76
293023	10-76
293024	10-76
293025	10-76
293026	10-76
293027	10-77
293028	10-77
293029	10-77
293030	10-77
293031	10-77
293032	10-77
293033	10-77
294000	10-127
294001	10-127
294002	10-127
294003	10-127
295000	3-28
295001	3-28
295002	3-28
295003	3-28
295004	3-12
298000	7-27
298001	10-120
298002	10-118
298003	10-119
298004	10-120
298005	10-119
298006	10-120
298007	10-120
299000	10-122
299001	10-121
299002	10-122
299003	10-120
299004	10-121
299005	10-121
299006	10-122
300000	2-82
300001	2-85
300002	2-61
300003	2-11
300004	2-68
300005	2-88

Trap Number	Page
303000	10-38
304000	10-137
304001	10-137
306000	2-82
306001	2-83
306002	2-85
306003	2-84
306004	2-61
306005	2-58
306006	2-68
306007	3-31
306008	3-35
306009	3-37
306010	3-36
306011	3-38
306012	3-38
306013	3-33
306014	3-26
306015	3-39
306016	3-32
306017	3-39
306018	3-29
306019	3-18
306020	3-17
306021	3-30
306022	3-30
306023	3-31
306024	3-40
306025	3-19
308000	2-37
308001	2-47
308002	2-55
308003	2-50
308004	2-61
308005	2-58
308006	3-41
308007	3-23
308008	3-41
308009	3-42
308010	3-42
308011	3-42
308012	2-74

Trap Number	Page
308014	2-49
308016	3-41
308018	2-69
308020	7-15
308021	10-73
308022	10-38
308023	10-68
308024	10-134
308025	10-134
308031	10-68
308032	10-43
308033	10-82
308034	7-7
308035	7-15
308036	3-7
308037	10-107
308039	3-43
308040	10-81
308041	10-24
308042	3-26
308043	3-15
308044	10-71
308045	7-12
308046	7-12
308047	2-31
308048	2-32
315000	10-19
315001	10-19
315002	10-19
315003	7-28
315004	7-28
315005	7-27
315006	7-2
315007	10-20
315008	7-3
315009	5-3
315010	5-3
315011	5-3
315012	5-4
315013	10-19
315014	10-20
315015	10-20

Trap Index

Trap Number	Page
315016	10-21
316000	10-131
316001	10-131
317000	2-104
317001	10-132
317002	10-132
317003	10-133
317004	7-29
317005	10-133
317006	7-29
317007	10-132
317008	10-132
317009	10-132
317010	5-4
317011	5-4
317012	5-4
317013	5-4
317014	5-5
317015	5-5
317016	5-5
317017	5-5
317018	5-6
317019	5-6
317020	5-6
317021	5-6
317022	5-6
317023	5-7
317024	5-7
317025	5-7
317026	5-7
317027	5-8
317028	7-17
317029	5-8
317030	5-8
317031	5-8
318000	2-37
318001	2-47
318002	2-55
318003	2-51
318004	2-62
318005	2-57
318006	3-24

Trap Number	Page
318007	3-24
318008	3-26
318009	3-25
318010	2-74
318011	2-70
318012	2-15
318013	2-15
318014	3-27
321001	10-138
324000	7-29
324001	10-128
324002	10-128
324003	10-128
324004	7-28
324005	7-28
324006	10-128
327001	10-69
327002	7-12
327003	10-70
327004	10-70
327005	10-70
327006	10-70
327008	10-71
327009	10-71
327010	10-69
327011	10-69
327012	10-70
327013	10-70
327014	10-70
327015	7-11
327016	7-11
327017	7-11
327018	7-11
327019	7-12
327020	7-12
328001	10-52
328002	7-10
328003	10-53
328004	10-53
328005	10-54
328006	10-54
328007	10-54

Trap Number	Page
328008	10-54
328009	10-54
328010	10-52
328011	10-52
328012	10-53
328013	10-53
329003	6-27
329004	6-28
329005	7-29
329006	7-29
329007	6-28
329008	6-27
329010	10-18
329011	6-2
329012	6-27
330000	10-129
330001	7-28
330002	10-130
330003	10-131
330004	10-131
331000	6-11
331001	10-107
331002	6-12
331003	6-14
331004	6-14
331005	6-10
331006	6-13
331007	6-14
331008	6-11
331009	6-12
331010	6-14
331011	6-14
331012	6-13
331013	6-11
331014	6-12
331016	6-11
331017	6-12
331018	6-13
331019	6-10
331021	6-13
331022	6-11
331024	10-142

Trap Number	Page
331024	11-5
331025	10-142
331025	11-5
331026	10-142
331026	11-6
331027	10-142
331027	11-6
331028	10-142
331028	11-6
331029	10-142
331029	11-6
331030	10-143
331030	11-6
339000	7-9
339001	7-9
339002	11-6
341000	2-24
341001	7-2
341002	7-2
343000	10-131
343001	10-131
344000	10-130
344001	10-129
344002	10-129
344003	3-15
344004	10-130
344005	10-130
344006	10-130
344007	10-129
347000	10-133
347001	10-89
347002	10-89
347003	10-90
371001	7-21
371002	7-21
371003	7-19
371003	7-19
371003	7-19
371003	7-19
371003	7-20
371003	7-20
371003	7-20

Trap Index

Trap Number	Page
371003	7-21
371003	7-21
371003	7-21
371003	7-21
371003	7-22
371003	7-22
371003	7-22
371003	7-22
371003	7-22
371003	7-22
371003	7-22
371003	7-23
371003	7-23
371003	7-23
371004	7-23
371004	7-23
371004	7-23
371004	7-24
371004	7-24
371004	7-24
371004	7-24
371004	7-24
371004	7-24
373001	7-6
373002	10-41
373003	2-3
373004	10-41
373005	10-40
373006	10-40
373007	10-40
373008	10-41
379000	7-10
379001	7-13
379002	5-8
379003	5-9
379004	10-66
379005	10-66
379006	10-85
379007	10-68
379008	10-21
379010	10-85
379011	10-30

Trap Number	Page
379012	10-68
379013	10-102
379015	10-55
379017	10-32
379018	10-31
379019	10-42
379020	7-6
379021	10-80
383000	10-23
383001	10-72
384000	10-104
385001	3-11
385009	3-8
385010	3-7
385016	3-8
385017	3-10
385028	3-9
385029	3-7
385030	3-9
385031	10-138
385031	11-6
385032	10-138
385032	11-6
385033	10-138
385033	11-6
385034	10-139
385034	11-6
385035	10-139
385035	11-7
385036	10-139
385036	11-7
387000	10-92
387000	10-93
387001	10-91
389000	10-93
389001	10-93
392000	10-69
392001	10-69
392002	10-83
400000	7-18
400000	10-98
400001	10-94

Trap Number	Page
401000	10-95
401000	10-96
401001	10-99
401002	10-99
401003	10-98
402000	10-97
402000	10-98
402001	10-73
403000	10-86
403001	10-39
403002	2-7
403003	2-7
403003	10-68
403004	2-7
403005	2-8
403006	2-8
403007	2-8
403008	2-11
403009	2-11
404000	6-10
404001	6-7
404002	6-9
404003	6-6
404004	6-8
404005	6-7
404006	6-8
404007	6-8
404008	6-9
404009	6-9
404010	6-6
404011	6-6
404043	7-25
404044	7-25
404045	7-25
404046	7-25
404047	7-25
404048	7-25
404049	7-25
404050	7-26
404051	7-26
404052	7-26
404053	7-26

Trap Number	Page
406002	9-75
406003	9-75
411000	10-140
411000	11-7
411001	10-140
411001	11-7
411002	10-140
411002	11-7
411003	10-140
411003	11-7
411004	10-140
411004	11-7
411005	10-140
411005	11-7
412000	10-141
412000	11-7
412001	10-141
412001	11-8
412002	10-141
412002	11-8
412003	10-141
412003	11-8
412004	10-141
412004	11-8
412005	10-141
412005	11-8
413006	10-63
413007	10-63
413008	10-63
413009	10-64
413010	10-64
413011	10-64
413012	10-64
413021	10-64
416000	11-8
419000	10-72
419001	10-125
419002	10-126
419003	10-127
419004	10-125
419005	10-126
419006	10-126

Trap Index

Trap Number	Page
419007	10-125
419008	10-125
419009	10-126
423000	11-8
423001	11-8
423002	11-8
423003	11-9
425000	10-72
425001	10-73
425002	10-88
425003	10-27
425004	10-27
425005	10-27
425006	10-27
425007	10-61
425007	10-62
4250028	10-63
425008	10-101
425009	10-62
425010	10-79
425011	10-73
425012	10-65
425013	10-65
425014	10-101
425015	10-21
425016	10-79
425017	10-80
425020	10-72
425021	10-17
425022	10-18
425024	10-18
425025	10-18
425026	10-18
425027	10-18
426000	12-2
426000	12-2
426000	12-2
426000	12-2
426000	12-2
426000	12-3
426000	12-3
426000	12-3

Trap Number	Page
426001	12-3
426002	12-3
426002	12-3
426002	12-4
426002	12-4
426002	12-4
426002	12-4
426002	12-4
426002	12-4
426002	12-4
426002	12-5
426002	12-5
426002	12-5
426002	12-5
426002	12-5
426002	12-5
426002	12-5
426003	12-6
426003	12-6
426004	12-6
426005	12-6
426006	12-6
426007	12-6
426008	12-6
426009	12-7
426010	12-7
426011	12-7
426012	12-7
426013	12-7
426014	12-7
426014	12-7
426014	12-8
426014	12-8
426014	12-8
426014	12-8
426014	12-8
426014	12-8
426014	12-8
426014	12-9
426014	12-9
426014	12-9
426014	12-9

Trap Number	Page
426014	12-9
426014	12-9
426014	12-9
426014	12-10
426014	12-10
426014	12-10
426014	12-10
426014	12-10
426014	12-10
426014	12-10
426014	12-11
426014	12-11
426014	12-11
426014	12-11
426014	12-11
426014	12-11
426014	12-12
426014	12-12
426014	12-12
426014	12-12
426014	12-12
426014	12-12
426015	12-13
426016	12-13
426016	12-13
426016	12-13
426016	12-13
426017	12-13
426017	12-13
426018	12-14
426018	12-14
426018	12-14
426018	12-14
426019	12-14
426019	12-14
426019	12-15
426019	12-15
429000	11-9
429001	11-9
429002	11-9
429003	11-9
429004	11-9

Trap Number	Page
429005	11-9
429006	11-9
429007	11-10
429008	11-10
429009	11-10
429010	11-10
429011	11-10
429012	11-10
429013	11-10
429014	11-10
429015	11-10
429016	11-10
430000	11-11
430001	11-11
430002	11-11
430003	11-11
430004	11-11
430005	11-11
430006	11-11
430007	11-12
430008	11-12
430009	11-12
430010	11-12
430011	11-12
430012	11-12
430013	11-12
430014	11-12
430015	11-12
430016	11-12
430017	11-13
430018	11-13
430019	11-13
430020	11-13
431000	11-13
431001	11-13
431002	11-13
431003	11-13
431004	11-13
431005	11-14
431006	11-14
432000	11-14
432001	11-14

Trap Index

Trap Number	Page
432002	11-14
432003	11-14
432004	11-14
432005	11-14
433000	9-120
433001	9-121
437000	11-14
437006	11-14
439000	11-15
439001	11-15
439002	11-15
439003	11-15
439005	11-15
439006	11-15
439007	11-16
439008	11-16
439009	11-16
446000	11-16
446001	11-17
448000	11-17
451000	9-126
451000	11-17
451000	13-39
452000	9-126
452000	11-17
452000	13-40
452001	9-126
452001	11-17
452001	13-40
452002	9-126
452002	11-17
452002	13-40
454001	11-18
454002	11-18
455000	11-18
455001	11-18
455002	11-18
455003	11-18
455004	11-18
455005	11-18
455006	11-19
455007	11-19

Trap Number	Page
455008	11-19
455009	11-19
459000	13-3
459001	13-4
459002	13-5
459002	13-6
459003	13-6
459004	13-7
459005	13-7
459006	13-8
459007	13-8
459008	13-8
459009	13-9
459010	13-9
459011	13-9
459012	13-10
459013	13-10
459015	13-10
459016	13-11
459017	13-12
459018	13-12
459019	13-13
459020	13-13
460000	13-14
460001	13-15
460002	13-16
460003	13-17
460004	13-18
460005	13-19
460006	13-20
460007	13-21
460008	13-22
460009	13-23
460010	13-24
460011	13-25
460012	13-25
460013	13-25
460014	13-26
460015	13-26
460016	13-26
460016	13-27
460017	13-27

Trap Number	Page
460017	13-28
460018	13-29
460019	13-29
460020	13-30
460021	13-31
460022	13-32
460023	13-33
460024	13-34
460024	13-35
460024	13-36
460024	13-37
461000	13-39
461001	13-39
461002	13-39
461003	13-39
461004	13-39
462000	13-38
462001	13-38
462002	13-38
462003	13-38
462004	13-38
462005	13-38
462006	13-38
462007	13-39
462008	13-39
462009	13-39
462010	13-39
470000	10-144
470005	10-144
470006	10-144
470008	10-144
470009	10-145
470011	10-145
478002	9-127
478003	9-128
478004	9-128
478005	9-129
478006	9-129
478007	9-130
478008	9-130
478009	9-131
478010	9-131

Trap Number	Page
478011	9-132
478012	9-132
478013	9-132
478014	9-133
478015	9-133
478016	9-134
478017	9-134
478018	9-134
478019	9-135
478020	9-135
478021	9-135
478022	9-136
478023	9-136
478024	9-137
478025	9-137
478026	9-137
478027	9-138
478028	9-138
478029	9-138
478030	9-138
478031	9-138
478032	9-139
478033	9-139
478034	9-139
478035	9-139
479001	9-2
479002	9-2
479003	9-2
479004	9-2
479005	9-3
480001	9-116
480002	9-117
480003	9-117
480004	9-117
480005	9-118
480006	9-118
480007	9-118
480008	9-118
480009	9-118
480010	9-119
480011	9-119
480012	9-119

Trap Index

Trap Number	Page
480013	9-120
480014	9-120
480015	9-120
481001	9-23
481002	9-23
481003	9-23
481004	9-24
481005	9-24
481006	9-25
481007	9-25
481008	9-26
481009	9-26
481010	9-26
481011	9-26
481012	9-26
481013	9-27
481015	9-27
481016	9-27
481017	9-27
481018	9-27
481019	9-28
481020	9-28
481021	9-28
481024	9-28
481025	9-28
481028	9-29
481031	9-29
481032	9-29
481033	9-30
481034	9-30
481035	9-30
481036	9-30
481037	9-31
481038	9-31
481039	9-31
481040	9-31
481041	9-32
481042	9-32
481043	9-32
481044	9-33
481045	9-33
481046	9-33

Trap Number	Page
481047	9-33
481048	9-34
481049	9-34
481050	9-34
481051	9-34
481052	9-35
481053	9-35
481054	9-35
481055	9-35
481056	9-36
481058	9-36
481059	9-36
481060	9-36
481061	9-36
481062	9-36
481063	9-37
481064	9-37
481065	9-37
481066	9-37
481067	9-37
481068	9-38
481069	9-38
481070	9-38
481071	9-38
481072	9-39
481073	9-39
481074	9-39
481075	9-40
481076	9-40
481077	9-41
481078	9-41
481079	9-42
481080	9-42
481081	9-42
481082	9-43
481083	9-43
481084	9-43
481085	9-43
482001	9-140
482002	9-140
482003	9-140
482004	9-140

Trap Number	Page
483001	9-121
483002	9-121
483003	9-121
483004	9-121
483005	9-122
483006	9-122
483007	9-122
483008	9-122
483009	9-123
483010	9-123
483011	9-123
483012	9-124
483013	9-124
483014	9-124
483015	9-124
483016	9-125
483017	9-125
483018	9-125
483019	9-125
483020	9-125
485001	9-77
485002	9-78
485003	9-78
485004	9-78
485005	9-79
485006	9-79
485007	9-79
485008	9-80
485009	9-80
485010	9-80
485011	9-81
485012	9-81
485013	9-81
485014	9-81
485015	9-82
485016	9-82
485017	9-82
485018	9-83
485019	9-83
485020	9-83
485021	9-84
485022	9-84

Trap Number	Page
486001	9-97
486002	9-97
486003	9-98
486004	9-99
486005	9-100
486006	9-100
486007	9-100
486008	9-101
486009	9-101
486010	9-102
486014	9-103
486017	9-103
486018	9-104
486019	9-104
486020	9-104
486022	9-104
486023	9-104
486025	9-105
486026	9-105
486027	9-105
486028	9-105
486029	9-106
486030	9-106
486031	9-106
486032	9-107
486033	9-108
486034	9-109
486035	9-110
486036	9-111
486037	9-112
486038	9-112
486039	9-112
486040	9-113
486041	9-113
486042	9-113
486043	9-113
486044	9-113
486045	9-114
486046	9-114
486047	9-114
487001	9-3
487002	9-3

Trap Index

Trap Number	Page
487003	9-3
487004	9-4
487005	9-4
487006	9-4
487007	9-5
487008	9-5
487009	9-5
487010	9-5
487011	9-5
487012	9-6
487013	9-6
487014	9-7
487015	9-8
487016	9-8
487017	9-9
487018	9-9
487019	9-9
487020	9-10
487021	9-11
487022	9-12
487023	9-12
487024	9-12
487025	9-12
487026	9-12
487027	9-13
487028	9-13
487029	9-13
487030	9-13
487031	9-14
487032	9-14
487033	9-14
487034	9-14
487035	9-15
487036	9-15
487037	9-15
487038	9-15
487039	9-15
487040	9-16
487041	9-16
487042	9-16
487043	9-16
487044	9-17

Trap Number	Page
487045	9-17
487046	9-17
487047	9-17
487048	9-17
487050	9-18
487051	9-18
487052	9-18
487053	9-18
487054	9-19
487055	9-19
487056	9-19
488001	9-44
488002	9-45
488003	9-45
488004	9-45
488005	9-46
488006	9-46
488007	9-46
488008	9-47
488009	9-47
488010	9-47
488011	9-48
488012	9-48
488013	9-48
488014	9-49
488015	9-49
488016	9-49
488017	9-49
488018	9-50
488019	9-50
488020	9-51
488021	9-51
488022	9-52
488023	9-52
488024	9-52
488025	9-53
488026	9-53
488027	9-54
488028	9-54
488029	9-54
488030	9-54
488031	9-55

Trap Number	Page
488032	9-55
488033	9-55
488034	9-55
488035	9-56
488036	9-56
488037	9-56
488038	9-56
488039	9-57
488040	9-57
488041	9-58
488042	9-58
488043	9-59
488044	9-59
488045	9-60
488046	9-60
488047	9-61
488048	9-62
488049	9-62
488050	9-63
488051	9-64
488052	9-64
488053	9-65
488054	9-66
488055	9-66
488056	9-67
488057	9-67
488058	9-67
488059	9-68
488060	9-68
488061	9-68
488062	9-69
488063	9-69
488064	9-70
489001	9-141
489002	9-141
489003	9-141
489004	9-142
489005	9-142
489006	9-142
489007	9-143
489008	9-143
489009	9-143

Trap Number	Page
489010	9-144
489011	9-144
489012	9-144
489013	9-145
489014	9-145
489015	9-145
489016	9-146
489017	9-146
489018	9-147
491001	9-84
491002	9-85
491003	9-85
491004	9-86
491005	9-86
491006	9-86
491007	9-87
491008	9-87
491009	9-87
491010	9-88
491011	9-88
491012	9-88
491013	9-88
491014	9-89
491015	9-89
491016	9-89
491017	9-89
491018	9-90
491019	9-90
491020	9-90
491021	9-91
491022	9-91
491023	9-91
491024	9-92
491025	9-92
491031	9-92
491032	9-93
491033	9-93
491034	9-93
491035	9-93
491036	9-94
491037	9-94
491038	9-95

Trap Index

Trap Number	Page
491039	9-95
491040	9-95
491041	9-96
491042	9-96
494000	2-101
494001	2-101
494002	2-102
494003	2-101
494004	2-102
494005	2-102
494006	2-103
494007	2-103
494008	2-103
494009	2-103
494010	2-103

Alarm	Page
##@@**Event to LCON %d, %s	10-3
%s - ALL STATIONS BOOT COMPLETE	3-3
%s - ERR: SLAC DYNAMIC BOOT IN PROGRESS, TRY AGAIN WHEN COMPLETED	3-3
%s - NO STATION CREATED	3-3
%s - WILL REQUIRE FRI BOOT OF %d or/r/n	3-3
%s CONNECTED TO MAIN CHANNEL	4-2
%s FAILED MAIN CHANNEL CONNECT	4-2
%s HAS DETECTED A STREAMING DEVICE	10-2
%s NCCP CRC ERROR	10-2
%s STREAMING DEVICE CONDITION CLEARED	10-2
%s WRONG POINTER PASSED IN	11-3
%d BYTES LOADED FROM NSO DISK	10-3
%d is the port number	11-17
%d: %s/%s->%s	11-5
%dc is card slot number	11-17
%dg is group number	11-17
%HTTPD_LOG:%s	13-39
%ld - RECEIVED INVALID PROTOCOL ID FROM THE ROUTER %d	10-3
%s - %s, PORT (n) - Cannot use ISDN - ISDN module missing	11-16
%s - BAD CCBPTR IN %s, ch0ccbptr=%x, ccbptr=%x, ccb_index=%d, numchan=%d	10-139
%s - BAD CCBPTR IN %s, ch0ccbptr=%x, ccbptr=%x, ccb_index=%d, numchan=%d	11-3
%s - CANNOT BE ACTIVATED. <SRC, DST, ENCAPSULATION> CONFLICTS WITH STN %d	10-3
%s - CLOCK SOURCE OVERRIDE	10-3
%s - CLOCK SOURCE OVERRIDE	10-140
%s - CLOCK SOURCE OVERRIDE	10-141
%s - CLOCK SOURCE OVERRIDE	11-7
%s - CLOCK SOURCE OVERRIDE	11-8
%s - CLOCK SOURCE OVERRIDE	11-14
%s - CONFIG ERROR - %s	10-3
%s - CONFIG ERROR - %s %d	10-3
%s - CONFIG ERROR - %s %s	10-3
%s - DATA LOST FROM DATA QUEUE	10-4
%s - DATA LOST FROM DATA QUEUE	10-4
%s - DATA LOST FROM DATA QUEUE	10-4
%s - DATA LOST FROM DATA QUEUE	10-4
%s - DATA LOST FROM Rx DATA QUEUE	10-4
%s - DATA LOST FROM Tx DATA QUEUE	10-4
%s - DPAD '%s' IS NON RESPONDING	10-4
%s - DYNAMIC ALL STATION BOOT BEING CREATED	3-2
%s - DYNAMIC ALL STATION BOOT COMPLETED	3-2

Alarm Index

Alarm	Page
%s - DYNAMIC ALL STATION BOOT STARTED	3-2
%s - DYNAMIC ALL STATIONS BEING CREATED	3-2
%s - DYNAMIC ALL STATIONS BEING CREATED	11-3
%s - DYNAMIC ALL STATIONS BOOT COMPLETED	11-3
%s - DYNAMIC ALL STATIONS BOOT CREATED	3-2
%s - DYNAMIC ALL STATIONS BOOT STARTED	3-2
%s - DYNAMIC ALL STATIONS BOOT STARTED	11-3
%s - DYNAMIC STATION BEING CREATED	11-4
%s - DYNAMIC STATION BOOT COMPLETED	11-4
%s - DYNAMIC STATION BOOT STARTED	11-4
%s - END-TO-END SEGMENTATION LINK DOWN (or)	3-2
%s - END-TO-END SEGMENTATION LINK UP	3-3
%s - ERRONEOUS BOOLEAN PARAMETER: %s	10-4
%s - ERRONEOUS BOOLEAN PARAMETER: %s	10-140
%s - ERRONEOUS BOOLEAN PARAMETER: %s	10-141
%s - ERRONEOUS BOOLEAN PARAMETER: %s	11-7
%s - ERRONEOUS BOOLEAN PARAMETER: %s	11-8
%s - ERRONEOUS BOOLEAN PARAMETER: %s	11-14
%s - EXCEEDING MAXIMUM RANGE ALLowED	10-4
%s - FRAME SEGMENTER LINK DOWN	3-2
%s - I.430 DIM IN SYNC	7-2
%s - I.430 DIM OUT OF SYNC	7-2
%s - INSUFFICIENT MEMORY FOR CONFIGURED STATIONS	10-143
%s - INVALID ENCAPSULATION	10-5
%s - INVALID ENCAPSULATION	10-5
%s - INVALID ENCAPSULATION	10-5
%s - INVALID ENCAPSULATION	10-5
%s - INVALID ENCAPSULATION	10-5
%s - LAN CONNECTION BOOTED	10-5
%s - LAN CONNECTION BOOT FAILURE - %s	10-5
%s - LAN CONNECTION CREATION FAILURE - %s	10-5
%s - LAN CONNECTION CREATION FAILURE - %s	10-6
%s - LAN CONNECTION CREATION FAILURE - %s	10-6
%s - LAN CONNECTION DISABLE FAILURE - %s	10-6
%s - LAN CONNECTION DISABLED	10-6
%s - LAN CONNECTION ENABLE FAILURE - %s	10-6
%s - LAN CONNECTION ENABLED	10-6
%s - NCI CHANNEL UTILIZATION >100%%	4-2
%s - NO HEARTBEAT	10-6
%s - NO STATION CREATED	11-4
%s - NS INVALID CONFIGURATION	10-6
%s - PACKET RECEIVED WITH INVALID RFC1294 ENCAPSULATION	10-7

Alarm	Page
%s - PACKET TYPE NOT SUPPORTED FOR ENCAPSULATION	10-7
%s - PORT ERROR COUNT > THRESHOLD	10-7
%s - PORT ERROR COUNT > THRESHOLD	10-7
%s - PORT ERROR COUNT >THRESHOLD	10-141
%s - PORT ERROR COUNT THRESHOLD	10-140
%s - RECEIVED ALARM CLEARED: %s	11-19
%s - RECEIVED ALARM SET: %s	11-19
%s - RECEIVED INVALID FORWARDER ID FROM THE WAN LINK %d	10-7
%s - RECEIVED INVALID FORWARDER ID FROM THE WAN LINK %d	10-7
%s - Remote loopback ended	11-15
%s - Remote loopback in progress	11-15
%s - SBS FW Upgrade %d.%d - %s	11-18
%s - SNMP Manager is Restarting	10-7
%s - STPE BAD HELLO THRESHOLD EXCEEDED	10-8
%s - TRANSMITTED ALARM CLEARED: %s	11-19
%s - TRANSMITTED ALARM SET: %s	11-19
%s - TX SANITY TIMEOUT	10-140
%s - TX SANITY TIMEOUT	10-141
%s - TX SANITY TIMEOUT	11-7
%s - TX SANITY TIMEOUT	11-8
%s - TX SANITY TIMEOUT	11-14
%s - UNSUP-PORTED SPEED: OPERATING AT %d BITS PER SECOND	10-8
%s - UNI SEGMENTATION LINK DOWN	3-3
%s - UNI SEGMENTATION LINK UP	3-3
%s - UNSUP-PORTED RECEIVE BYTE COUNT: OPERATING WITH %d RX BYTE COUNT	10-8
%s - UNSUPPORTED BAUDRATE: OPERATING AT 9600 BPS	11-8
%s - UNSUPPORTED DATABITS: OPERATING WITH 8 DATABITS, NO PARITY	11-8
%s - UNSUPPORTED PARITY: OPERATING WITH 8 DATABITS, NO PARITY	11-9
%s - UNSUPPORTED RECEIVE BYTE COUNT: OPERATING WITH %d RX BYTE COUNT	10-140
%s - UNSUPPORTED RECEIVE BYTE COUNT: OPERATING WITH %d RX BYTE COUNT	10-141
%s - UNSUPPORTED RECEIVE BYTE COUNT: OPERATING WITH %d RX BYTE COUNT	11-7
%s - UNSUPPORTED RECEIVE BYTE COUNT: OPERATING WITH %d RX BYTE COUNT	11-8
%s - UNSUPPORTED RECEIVE BYTE COUNT: OPERATING WITH %d RX BYTE COUNT	11-14
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	11-7
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	11-8
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	10-8
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	10-8
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	10-140
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	10-141
%s - UNSUPPORTED SPEED: OPERATING AT %d BITS PER SECOND	11-14
%s - WSL BOOT COMPLETE	10-8
%s -DEBUG - %s	11-18

Alarm Index

Alarm	Page
%s CALL ROUTING ERROR: %s	10-143
%s CONNECTED TO MAIN CHANNEL	4-2
%s CONNECTED TO MAIN CHANNEL	10-8
%s CONNECTED TO PMS CHANNEL	10-9
%s DETECTED DEVICE %d (%x hex) %s	7-2
%s DSP #%d LAST VSM RESPONSE: %02X %02X %02X %02X %02X	10-137
%s DUPLICATE NCCP DEVICE ent #%d	10-9
%s ERR: SLAC DYNAMIC BOOT IN PROGRESS, TRY AGAIN WHEN COMPLETED	11-4
%s FAILED MAIN CHANNEL CONNECT	4-2
%s FAILED MAIN CHANNEL CONNECT	10-9
%s IS NOT MONITORED BY BOD, NO PARALLEL LCON CREATED	10-9
%s LOST MAIN CHANNEL CONNECTION	4-2
%s LOST MAIN CHANNEL CONNECTION	10-9
%s LOST PMS CHANNEL CONNECTION	10-9
%s NCCP PROTOCOL ERROR	10-9
%s rescued msg #%d\r\n%x/%x/%x %x/%x	11-3
%s rescued msg #%d\r\n%x:%x %x:%x %x:%x %x:%x %x:%x	11-3
%s STATE SEARCH ABORTED %s	10-9
%s- DEBUG - %s	11-18
%s-%d Abort Frame Function Not Supported.	11-13
%s-%d Aborted Frames %d.	11-13
%s-%d Data Scope Monitoring Function Not Supported.	11-13
%s-%d Init Success a=%x b=%x.	11-14
%s-%d Initialization Failed Cause Code: %x.	11-13
%s-%d RX Sanity Timer Expired	11-8
%s-%d RX Sanity Timer Expired.	11-14
%s-%d TX Sanity Timer Expired %d.	11-13
%s-<%d> %s THRESHOLD EXCEEDED	10-9
%s-<%d> - BOARD BOOT: CAUSE WATCHDOG TIMER EXPIRED	7-2
%s-<%d> - HW BOARD FAILURE, CAUSE: BACKGROUND DIAGNOSTIC	7-2
%s-<%d> - Warning - Illegal T1/E1 clock mode - Both ports configured for 'REC' timing	10-10
(#) BYTES LOADED FROM EXTENDED FLASH MEMORY	10-10
(cause) - NON-RECOVERABLE INBOUND ERROR	10-10
(cause) - NON-RECOVERABLE OUTBOUND ERROR	10-11
(entity) - BOOT COMPLETE	10-11
(entity) - BOOT FAILURE (cause)	10-12
(entity) - BUFFER DISCARDED (cause)	10-13
(entity) - DISABLE FAILURE	10-13
(entity) - DISABLED	10-14
(entity) - ENABLE FAILURE	10-14
(entity) - ENABLED (cause)	10-14
(entity) - FLOW CONTROL IMPOSED	10-14

Alarm	Page
(entity) - FLOW CONTROL RELEASED	10-15
(entity) - HOST TIMEOUT	10-15
(entity) - MESSAGE DISCARDED, NO CONNECTION	10-15
(entity) - X.25 CALL FAILED	10-15
(entity) -HOST HAS STARTED POLLING	10-16
(IA) - IA ENTERING FAST POLL	10-16
(IA) - IA ENTERING SLOW POLL	10-16
(IA) - RESET DISCARDED	10-16
(IA) - STOPPED POLLING IA	10-17
(IA) - T1 TIMEOUT	10-17
(IA) - T2 TIMEOUT	10-17
(l) - DEDICATED LINK - NOT CONFIGURED	10-17
(n) BAD ISAKMP PRESHARED KEYS FOUND IN CMEM	10-18
(n) GOOD ISAKMP PRESHARED KEYS FOUND IN CMEM	10-17
(OS Memory)	11-16
(p) changed from LHHHHHHHHLH to HHHHHHHHHLH	10-71
(s) - CONNECTION UP	10-18
(s) - TIMEOUT FROM TCP	6-2
(s) CLEARING CALL, BAD OR NO RESPONSE FOR QSM	7-2
(s) CLEARING CALL, UNEXPECTED Q-BIT PACKET (q)	10-19
(s) CONNECTION DOWN	10-19
(s) CONNECTION UP	10-19
(s) INVALID CP PACKET (header)	10-19
(s) INVALID LU PACKET (header)	10-20
(s) LU SESSION ACTIVATED	5-4
(s) LU-LU SESSION CLEARED, CLEARING SVC	5-3
(s) OUT OF SEQUENCE PACKET, Event Code (n)	10-20
(s) PU SESSION ACTIVATED	5-3
(s) PU SESSION CLEARED, CLEARING SVC	5-3
(s) RECEIVED -VE RESPONSE,SENSE DATA- (d)	10-20
(s) RETRIES OVER FOR SENDING BIND	10-21
(s) RETRY EXCEEDED, FOR SNA MESSAGE	7-3
(x) BYTES LOADED FROM EXTENDED FLASH MEMORY	7-3
(xx) TABLES BOOTED	10-21
(xxxx) AUTHENTICATION WAS REJECTED BY PEER	10-21
*** %s WILL REQUIRE FRI BOOT OF PORT %d or\r\n	11-4
-> (dstprt)	9-40
-> (dstprt)	9-41
0 ERROR DETECTED AT 0x0 bit(s) 0x0 CORRECTED	6-2
0x80d50c 0x80d510	6-5
<%s>-<%d>: BOARD BOOT: CAUSE SOFTWARE DOWNLOAD FAILED	7-3
<app_id> does not exist	9-147

Alarm Index

Alarm	Page
<n> entries of Egress IP ClTcQosMap Prof #<num> ignored - no classifiers	9-152
<n> entries of Ingress IP ClTcQosMap Prof #<num> ignored - no classifiers	9-152
<n> entries of IPX ClTcQosMap Prof #<num> ignored - no classifiers	9-152
<n> entries of Service Prof #<num> ignored - Duplicate Records	9-153
<n> entries of TB ClTcQosMap Prof #<num> ignored - no classifiers	9-153
= %d	11-5
AAM - PORT (n) - ATM PORT DOWN	9-76
AAM - PORT (n) - ATM PORT UP	9-76
AAM - PORT (n) CANNOT CREATE VCC FOR VPI (vpi) VCI (vci)	9-76
AAM - PORT (n) STATION (s) - ATM STATION DOWN	9-75
AAM - PORT (n) STATION (s) - ATM STATION UP	9-75
AAM - PORT (n) STATION (s) - STATION BOOT FAILURE - (cause)	9-74
AAM - PORT (n) STATION (s) - STATION DISABLED	9-75
AAM - PORT (n) STATION (s) - STATION ENABLED	9-75
AAM- PORT (n) - OUT OF MEMORY - SOME STATIONS NOT CREATED	9-72
AAM- PORT (n) - PORT BOOT COMPLETE	9-73
AAM- PORT (n) - PORT BOOT FAILURE - (cause)	9-73
AAM- PORT (n) - PORT DISABLED	9-73
AAM- PORT (n) - PORT ENABLED	9-74
AAM- PORT (n) - PORT INITIALIZATION FAILED - (cause)	9-72
AAM- PORT (n) - PORT STATUS WARNING - PORT DISABLED	9-73
AAM- PORT (n) - PORT UTILIZATION > THRESHOLD	9-75
AAM- PORT (n) STATION (s) - STATION BOOT COMPLETE	9-74
ABNORMAL CALL TERMINATION - xxx PROTOCOL : xx STATES : xxxx EVENT : x	10-21
ABNORMAL NS COMMAND, CMD	10-21
addr X.X.X.X.-> omt ## conflicts with addr in other IP dev on LAN	13-37
ADDRESS ERROR (h)	10-22
ADDRESS ERROR (h)	10-22
ADDRESS ERROR (h)	10-22
ADDRESS ERROR (hh)	10-22
Aggregate route <net_prefix>/<prefix_len> is created	13-44
Aggregate route <net_prefix>/<prefix_len> is created, matching Profile entry %d	13-45
Aggregate route <net_prefix>/<prefix_len> is deleted because only one specific route is left	13-45
ALL PRIORITY QUEUES UNBLOCKED	10-22
ap2_ (cause)	10-23
ap2_net_change: Got netdown twice in a row	10-23
APPN_CM SYSERR (counter)	10-23
ARP.001 Q ovf nt (net)	9-77
ARP.002 Pkt in (op_type) (hwd_add) (type) nt (net_id)	9-78
ARP.003 Unkwn hdw (hwd_add) nt (net_id)	9-78
ARP.004 Bd hdw (hwd_add) (add_len) nt (net_id)	9-78
ARP.005 Unkwn prt (type) nt (net_id)	9-79

Alarm	Page
ARP.006 Bd prt (type) (add_len) nt (net_id)	9-79
ARP.007 Mk ent (hwd_add) (type) nt (net_id)	9-79
ARP.008 Bd opc (op_type) (hwd_add) (type) nt (net_id)	9-80
ARP.009 Rply (hwd_add) (type) nt (net_id)	9-80
ARP.010 Err on rply nt (net_id)	9-80
ARP.011 Del ent (hwd_add) (type) nt (net_id)	9-81
ARP.012 No iorb fr rqst nt (net_id)	9-81
ARP.013 No mem fr addr nt (net_id)	9-81
ARP.014 Rqst (hwd_add) (type) nt (net_id)	9-81
ARP.015 Err in rqst nt (net_id)	9-82
ARP.016 unkn dst prot ad nt (net_id)	9-82
ARP.017 No mem fr ent (hw_addr) (type) nt (net_id)	9-82
ARP.018 No mem fr nt (net_id)	9-83
ARP.019 No mem fr prt (proto_no) nt (net_id)	9-83
ARP.020 Bd src hdw fr nt (src_prot_addr)	9-83
ARP.021 No mem fr dav (net_id)	9-84
ARP.022 Bd src prt fr nt (src_prot_addr)	9-84
ARP.23 Rcv VID (vid) fm diff cfg (vid)	14-7
Assign a new IP address for the interface.	9-43
AT ClTcQosMap Prof #<num> does not exist	9-149
ATM-3000 - AAL5 CPCS FRAME TRANSMIT ERROR	10-23
AUTOCALL RETRIES EXHAUSTED	10-24
BACKUP LINK ACTIVATED	2-2
BACKUP LINK ACTIVATED	7-3
BACKUP LINK ACTIVATED	10-24
BACKUP NAME IN SWITCHED SERVICE ENTRY	10-24
bad adv/ovflo: (ls_type, dest_addr, adv_source)	10-25
BAD FRAME LENGTH (b)	10-25
BAD FRAME LENGTH (b)	10-26
BAD FRAME LENGTH (b)	10-26
BAD FRAME LENGTH (bbbb)	10-26
BAD FRAME TYPE (h)	10-26
BAD FRAME TYPE (h)	10-26
BAD FRAME TYPE (h)	10-26
BAD FRAME TYPE (hh)	10-27
BAD IPSEC PROFILE CMEM RECORD (xx)	10-27
BAD IPSEC TRANSFORM SET CMEM RECORD (n)	10-27
BAD ISAKMP POLICY CMEM RECORD (n)	10-27
BAD ISAKMP PRESHARED KEY RECORD (n)	10-27
BAD N(R) (hh/hh)	10-27
BAD P(K)	4-2
BAD P(R)	10-28

Alarm Index

Alarm	Page
BAD P(S)	10-2
BAD PACKET LENGTH (bbbb)	10-28
BAD PACKET TYPE (h)	10-28
Bad Param in (message)	10-29
Bad Param in (message) (ContÕd)	10-30
Bad Radius Response	14-6
BASE KEY CHANGED: (base_key_name)	10-30
Bd src prt fr nt x.x.x.x	13-37
BGP - %s Connection Collision with Peer No. %d -%s	13-27
BGP - %s Connection Collision with Peer No. %d -%s	13-28
BGP - Best Route to %s\/%d Changed. Current Best Route via Peer No. %d	13-9
BGP - Buffer not available for %s the %s message to Peer No. %d	13-7
BGP - Buffer not Available for %s the %s Peer No. %d	13-19
BGP - Configuration Error - %s	13-17
BGP - Connection %s controlled by TCP with Peer No. %d	13-26
BGP - Connection %s controlled by TCP with Peer No. %d	13-27
BGP - Connection Establish with Peer No. %d	13-25
BGP - Connection Lost with Peer No. %d -%s	13-29
BGP - Connection Retry Timer Expired for the BGP Connection with Peer No. %d	13-29
BGP - Error in NOTIFY Message Received from Peer No. %d %s %d	13-26
BGP - Error in Open Message Received from Peer No. %d, %s %ld	13-22
BGP - Error in UPDATE Message Received from Peer No. %d - %s, %d	13-34
BGP - Error in UPDATE Message Received from Peer No. %d - %s, %d	13-35
BGP - Error in UPDATE Message Received from Peer No. %d - %s, %d	13-36
BGP - Error in UPDATE Message Received from Peer No. %d - %s, %d	13-37
BGP - Error in UPDATE Message Received from Peer No. %d - %s, %s	13-5
BGP - Error in UPDATE Message Received from Peer No. %d - %s, %s (Continued)	13-6
BGP - FSM Error on BGP connection with Peer No. %d Curr state %d Curr Event %d	13-23
BGP - FSM State Changed on BGP connection with Peer No. %d [CurrState: %d Event: %d NewState: %d]	13-33
BGP - Hold Timer Expired in Establish state on BGP connection with Peer No. %d	13-21
BGP - Invalid NLRI Received from Peer No. %d - %s	13-6
BGP - KEEPALIVE Message %s Peer No. %d	13-30
BGP - Message Header Error in Message Received from Peer No. %d - %s	13-25
BGP - Message Header Error in Message Received from Peer No. %d - %s %d	13-24
BGP - Non Existing Route to %s\/%d being tried to be Withdrawn by Peer No. %d	13-8
BGP - Not Enough Dynamic Memory %s	13-15
BGP - Not Enough Dynamic Memory - %s	13-4
BGP - Not enough Permanent Memory %s	13-14
BGP - Not Enough Permanent memory - %s	13-3
BGP - NOTIFY Message %s Peer No. %d [ErrCode: %d ErrSubcode: %d ErrData: %s]	13-32
BGP - NOTIFY Message %s to Peer No. %d \[ErrCode: %d,ErrSubCode: %d,ErrData: %s \]	13-10
BGP - OPEN Message %s Peer No. %d [Ver: %d AS: %d HldTm: %d BgpID: %s AuthInfo: %d %s]	13-31

Alarm	Page
BGP - Route to %s Not Available Anymore.	13-9
BGP - Route to %s\/%d advertised to Peer %d due to Permit Policy	13-13
BGP - Route to %s\/%d Imported from IGP into BGP Routing Table	13-10
BGP - Route to %s\/%d Learnt from Peer No. %d (0 - IGP Route)	13-7
BGP - Route to %s\/%d not advertised to Peer %d due to Deny Policy	13-13
BGP - Route to %s\/%d received from Peer %d Filtered due to Deny Policy No %d	13-12
BGP - Route to %s\/%d received from Peer %d matched to Inbound Permit Policy No %d	13-12
BGP - Route to %s\/%d Relearnt from Peer No.	13-9
BGP - Route to %s\/%d Unreachable via Peer No. %d	13-8
BGP - Route to %s\/%d Withdrawn by IGP from BGP Routing Table	13-10
BGP - Route to %s\/%d Withdrawn by Peer No. %d	13-8
BGP - TCP Connection Error with Peer No. %d %s	13-18
BGP - TCP Listen Failed Due to lack of resource, Can't Acept the Passive TCP Conn from BGP Peers for some time	13-25
BGP - TCP Post Receive Failed for Peer No. %d	13-26
BGP - UPDATE Message %s from Peer No. %d \[Unfeasible Len: %d, Attr Len: %d, Reachable Len: %d \]	13-11
BGP -> Missing Modules - %s	13-16
BGP Connection Error with Peer No. %d - %s	13-20
BGP Route to <net_prefix>/<prefix_len> matched to BGP-OSPF Import Permit Policy No. <policy_id>	13-3
BGP Route to <net_prefix>/<prefix_len> matched to BGP->RIPv2 import Permit policy No. <policy_no>	13-43
BGP Route to <net_prefix>/<prefix_len> Not Imported into OSPF due to Deny Policy No. <policy_id>	13-2
BGP Route to <net_prefix>/<prefix_len> not imported into RIPv2 due to Deny Policy No. <policy_no>	13-43
BILLING RECORDS EXCEED LIMIT - BILLING RECORD LOST	10-31
BMM - BOARD ACTIVATED - BOARD %d	13-38
BMM - BOARD DEACTIVATED - BOARD: %D	13-38
BMM - BOARD FAULT - BOARD: %d CAUSE: %s	13-38
BMM - BOARD KEEPALIVE FAILURE - BOARD: %D	13-38
BMM BOOTED	13-39
BMM record defaulted	13-39
BOARD DEBUG MSG SLOT (%d) - \r\n%s	13-38
BOARD DEBUG MSG SLOT (%d) - \r\n%s	13-39
BOARD HIGH MSG SLOT (%d) - \r\n%s	13-38
BOARD HIGH MSG SLOT (%d) - \r\n%s	13-38
BOARD HIGH MSG SLOT (n) - VC_LIB (n) Packet	13-38
BOARD STATUS MSG SLOT (%d) - \r\n%s	13-38
BOARD STATUS MSG SLOT (%d) - \r\n%s	13-38
BOD FEATURE DISABLED BY TIME OF WEEK	7-3
BOD FEATURE ENABLED BY TIME OF WEEK	7-3
BOOTED ENCRYPTION PROFILE: (profile_name)	10-31
BOOTED ENCRYPTION KEY: (base_key_name)	10-32
bop_bri_sm_pck() ALLRIGHT+ CLOSED : RETURN	10-32
bop_bri_sm_pck() DEFAULT : RETURN	10-2
bop_bri_state_machine : CS=%d, STIM=%d, RES=%d, NS=%d	10-32

Alarm Index

Alarm	Page
BR-%d BRIDGE ID MISMATCH	10-32
BR-%d DUPLICATE RBR TRIPLET	10-33
BR-%d INCOMPATIBLE LINK MODE	10-33
BR-%d ONE TRANS LINK ALLowED PER NODE	10-33
BR-%d RING NUMBER MISMATCH LOCAL=%d REMOTE=%d	10-34
BRI - LINK DOWN, CAUSE =DIAG	10-34
BRI - PORT (n) - PORT BOOT COMPLETE	2-2
BRI - PORT (n) - PORT BOOT FAILED. REASON CODE = (cause)	2-2
BRI - PORT (p) - BRI TX BUFFERS CONGESTED	10-34
BRI - PORT (p) - CALL CONNECTED	10-34
BRI - PORT (p) - CALL DISCONNECT FAILED. REASON CODE = (n)	10-34
BRI - PORT (p) - CALL SETUP FROM %s FAILED. REASON CODE	10-34
BRI - PORT (p) - CALL SETUP FROM REJECTED. REASON CODE = (n)	10-35
BRI - PORT (p) - CALL SETUP TO DISCONNECTED BEFORE CON-NECTION COMPLETED. REASON CODE = (n)	10-35
BRI - PORT (p) - CALL SETUP TO FAILED. REASON CODE = (n)	10-35
BRI - PORT (p) - INITIALIZATION INCOMPLETE. REASON CODE = (n)	10-35
BRI - X.25 OVER D CHANNEL ERROR:	4-2
BRI CARD FAILURE	10-36
BRI INT. %d %s CONNECTED TO %s	10-36
BRI INTERNAL ERROR	10-36
BRI- PORT (p) - CALL DISCONNECTED REASON CODE = (n)	10-36
BRIDGE INITIALIZATION FAILURE (xx)	10-36
BRIDGE IS NOT THE ROOT	10-36
BRIDGE IS THE ROOT	10-36
BRIDGE LINK BOOT COMPLETE	10-37
BRIDGE LINK BOOT FAILURE (xx)	10-37
BRIDGE LINK DISABLE COMPLETE	10-37
BRIDGE LINK ENABLE COMPLETE	10-37
BRIDGE PARAMETERS BOOT FAILURE %s	10-37
BRIDGE PARAMETERS BOOT COMPLETE	10-37
Bridged or Routed packet received with invalid rfc1483 encapsulation on LCON (n)	9-72
BROADCAST OVERRUN	4-3
BTP.001, received request from (client_IP_address, net Network ID)	9-2
BTP.002, bad request from (client_IP_address, net Network ID): reason	9-2
BTP.003, Forwarding request to server_IP_address	9-2
BTP.004, Forwarding reply from server_IP_address to client_IP_address	9-2
BTP.005, Bad reply from server_IP_address to client_IP_address	9-3
BUFF_POOL_CORRUPTED	10-144
BUFF_REPT_CORRUPTED_BUFFER	10-144
BUFFER NOT AVAILABLE FOR STP CONFIG BPDUs	2-2
BUFFER NOT AVAILABLE FOR STP TCN BPDUs	2-2

Alarm	Page
BUFFER POOL UTILIZATION > THRESHOLD ON CARD (n)	2-2
BYTES COPIED TO FLASH MEMORY	10-37
CALL THRESHOLD EXCEEDED	2-3
Called bop_bri_sm_shutdown() from bop_bri_sm_pck() rnt_cod = 0x%x	10-38
Called state machine in the disabled state	10-38
CAN'T GET FACILITY FOR DCP	10-38
Cannot Connect to CA	10-145
CANNOT CREATE ENCRYPTION SESSION (cause)	5-9
CANNOT ERASE FLASH MEMORY	7-4
CANNOT ERASE FLASH MEMORY, SLOT (s)	7-4
CANNOT READ FROM FLASH MEMORY, SLOT (s)	7-4
CANNOT READ FROM NSO DISK, SLOT %d	10-38
CANNOT WRITE TO FLASH MEMORY	7-5
CANNOT WRITE TO FLASH MEMORY, SLOT (s)	7-5
Card-%dc clock derives from port %d	11-17
Card-%dc Group-%dg clock derives from port %d	11-17
Card-%dc Group-%dg clock is lost from port %d	11-17
Card-%dc lost clock from port %d	11-17
Certificate expires within one month	10-145
CERTIFICATE FOR IPSEC PROFILE xx DOES NOT EXIST	10-63
CFIAB	2-2
CFICB	2-3
CFIDT	2-3
CFINT	2-3
CFIRT	2-3
CHAIN portion of the TRANSPARENT BRIDGE FORWARDING TABLE is full	3-4
Channel %d state variable is at location 0x%x	10-38
CHANNEL (c) - CHANNEL BOOT COMPLETE	4-3
CHANNEL (c) - CHANNEL BOOT FAILURE - (cause)	4-3
CHANNEL (c) - CHANNEL DISABLED	4-3
CHANNEL (n) - CHANNEL ENABLED,	4-3
CHANNEL (n) - CHANNEL RESET RECEIVED	4-4
CHANNEL (n) - CHANNEL STATUS WARNING - (cause)	4-4
CHANNEL (n) - CHANNEL UTILIZATION > THRESHOLD	4-4
CHANNEL (n) - NO RESPONSE	4-4
CHANNEL (n) FRAME SEQUENCING OVERRIDE	4-5
CHECKSUM ERROR	10-38
CLI Error	10-38
CMEM BATTERY BAD	7-5
CMEM CORRUPTION DETECTED ON BOARD (n)	7-5
CMEM RECOVERED FROM BOARD (n)	7-6
CMEM SIMM REINITIALIZED	10-38

Alarm Index

Alarm	Page
COMMUNICATION ERROR - X25 CAUSE (cause)	2-6
completed	9-120
COMPRESSION NEGOTIATION FAILED	10-39
Configuration error - (err_msg)	10-39
Configuration error - <err_msg>	13-42
Configuration error:<err_msg>	13-44
CONFIGURED PKT SIZE > MAX ALLOWED ISDN D-CHANNEL	4-5
CONNECTED TO (destination)	10-39
Contact Customer Service.	9-43
COPY COMPLETE	10-39
COPYING SOFTWARE TO FLASH MEMORY	10-39
COPYING SOFTWARE FROM LOCAL FLASH TO FLASH	10-39
Could not bring up interface	10-39
CPU UTILIZATION > THRESHOLD ON CARD (c)	10-40
CTP - at wrong task, TCB =	10-40
CTP HELP MESSAGE ARRAY OVERFLOW	10-40
CVS - %s	10-40
CVS - Centralized Voice Switching disabled	10-40
CVS - Centralized Voice Switching enabled	10-40
CVS - Connection to PORT (n) terminated before match	2-3
CVS - CVS Table Copy Complete	10-41
CVS - Invalid Execution, Line No. %d	10-41
CVS - Module failed initialization	7-6
CVS - No digit value matching (value) found, calling address: (add)	10-41
DATA ENCRYPTION NOT ENABLED, H/W IS O.K	7-6
DATA IN IDLE STATE FROM SLOT (s)	5-7
DATA LOST FROM OUTBOUND (xxxx) QUEUE	10-41
DC - %s CONFIGURATION IS INCORRECT	4-5
DC - ABNORMAL CLEAR FLUSH FROM NS: Event=%d, State=%d, Chan_ID=%d	4-5
DC - ABNORMAL COMMAND ID FROM NS: Command_ID = (id)	4-5
DC - ABNORMAL FSM EVENT: Event=%d, State=%d, Chan_ID=%d	6-2
DC - BAD COMPRESSED PACKET	6-2
DC - CALL REQUEST ORIGINATOR IS NOT CONFIGURED FOR DATA COMPRESSION - CHANNEL (n)	4-6
DC - CHANNEL (n) CLEARED THE CALL DURING SRC NEGOTIATION, SAVED FACILITY WAS (b) CORRUPTED CONTROL BLOCK	4-6
DC - CHANNEL (n) IS CONNECTED TO ANOTHER AP, COMPRESSION IS NOT ALLOWED	4-6
DC - CHANNEL (n) RECEIVED NEGOTIATE FACILITY IN CALL REQUEST AND IS CONFIGURED AS FORCE ON	4-7
DC - CHANNEL UNAVAILABLE, CALL REJECTED FOR (cause)	4-7
DC - CHANNEL UNAVAILABLE, PVC CHANNEL (n) DID NOT GET CONNECTED WITH DATA COMPRESSION	4-7
DC - DATA COMPRESSION DISABLED, DC HARDWARE FAILURE	7-6
DC - DATA COMPRESSION DISABLED, DSP RAM NOT FOUND	7-7

Alarm	Page
DC - DATA COMPRESSION DISABLED, POWER-UP DIAGNOSTICS FAILURE	7-7
DC - DATA COMPRESSION HEADER ERROR, AP=%s, NP=%s	4-7
DC - DATA COMPRESSION DISABLED, DSP DOWNLOAD FAILURE, STATUS = %d	4-8
DC - DC HANDLER CHANNEL NUMBER FAILURE	6-2
DC - DC HANDLER CHANNEL STATISTICS FAILURE, STATUS = %d	6-2
DC - DC HANDLER CHANNEL STATS RESET FAILURE, STATUS = %d	6-3
DC - DC HANDLER FUNC TYPE FAILURE	6-3
DC - DC HANDLER GENERAL INIT FAILURE	4-8
DC - DC HANDLER VOCABULARY RESET FAILURE	6-3
DC - DC WAS CALLED TO PROCESS CALL ACCEPT WITHOUT A SAVED CALL REQUEST FOR %s	6-3
DC - dca_channel_flush(): PACKET COUNT ON THE QUEUE IS NON-ZERO	6-3
DC - dca_deallocate_resources() WAS CALLED WITH A NULL DCCB PTR	6-4
DC - dca_get_config_value() WAS CALLED WHEN CONFIG AS DISABLED FOR %s	6-4
DC - dch_api_dho_provide_new_buf() RETURNED DCH FAILURE	6-4
DC - INSUFFICIENT RAM FOR DATA COMPRESSION	7-7
DC - LOST/PENDING CALL CLEAR IN EP Q: Event=%d, State=%d, Chan_ID=%d	4-8
DC - NODE CONFIGURATION FOR DATA COMPRESSION CHANNELS DIFFERS CMEM. MAX DC CHANNELS=(n)	4-8
DC - PVC MISCONFIGURED, CHANNEL (n) IS AN AP CONNECTING TO ANOTHER AP	4-9
DC SIMM, MOTHERBOARD & T1E1 INCOMPATIBLE - DATA COMPRESSION DISABLED	10-41
DCCM-%d: Board Recovery Complete	10-42
DCCM-%d: Board Recovery Timeout (Ready Check)	10-42
DCCM-%d: Board Timeout (Reset Check)	10-42
DCCM-%d: DC Communication Lost	10-42
DEDICATED LINK (l) ALREADY ALLOCATED	10-42
DELETED ALL ENCRYPTION KEYS	10-42
DESTINATION NAME IN SWITCHED SERVICE ENTRY	10-43
DEVICE ACTIVE	7-7
DEVICE BOOT COMPLETE	7-7
DEVICE BOOT COMPLETE	10-43
DEVICE BOOT FAILURE	7-7
DEVICE BOOT FAILURE	10-43
DEVICE DISABLED	7-7
DEVICE DISABLE FAILURE	7-8
DEVICE DOWN	7-8
DEVICE ENABLE FAILURE	7-8
DEVICE ENABLED	7-8
DEVICE NOT RESPONDING	10-43
DEVICE OPERATIONAL	7-8
DEVICE_STATUS %d	10-43
dhcp int (intf) lease (ipadd) for (dur) from (serv)	14-2
dhcp int (intf) lease expired	14-4

Alarm Index

Alarm	Page
dhcp int (intf) no resp to discover	14-2
dhcp int (intf) no resp to request from (serv)	14-2
dhcp int (intf) rcv nak from (serv) - (msg)	14-2
dhcp int (intf) rcvd bad fmt (msg) from (serv)- (reason)	14-5
dhcp int (intf) rebinding	14-3
dhcp int (intf) renewing with (serv)	14-3
dhcp int (intf) retx (msg) (n) times in (state) to (serv)	14-3
dhcp int (intf) snd decline to (serv) - (reason)	14-4
dhcp int (intf) state change from (fromstate) to (tostate)	14-5
dhcp int (intf) unsp opts in (msg) from (serv) : (opt), ...	14-4
DIAGNOSTIC FAILURE ON BOARD ##	7-8
DIAGNOSTIC FAILURE ON BOARD (##), PORT (n)	2-4
DIAGNOSTIC FAILURE ON BOARD 0, (x) SECTION	7-9
DIAGNOSTIC FAILURE ON FLASH SIMM	2-4
DIAL IN NOT ALLOWED	10-43
DIAL OUT NOT ALLOWED	10-43
Digital Cert Gen Error	10-145
DISABLED state detected in bop_bri_rx_isr()	10-43
DISC RECEIVED	10-43
DISC RECEIVED	10-44
DISC RECEIVED	10-44
DISCARDED - SESSION MESSAGE FROM SLOT (s)	5-8
DISCARDING (n) FRAMES	10-44
DISCONNECTED FROM (destination)	10-44
DLCI CHANNEL DISCONNECTED BY FRI	3-4
DLSV Loader: ATTEMPTING TO DOWNLOAD	10-44
DLSV Loader: CANNOT WRITE FLASH	10-44
DLSV Loader: CANNOT ERASE FLASH	10-45
DLSV Loader: COPYING SW TO FLASH	10-45
DLSV Loader: DOWNLOAD COMPLETE	10-45
DLSV Loader: FAILED TO COPY SOFTWARE	10-45
DLSV Loader: FLASH HAS BEEN CORRUPTED	10-45
DLSV Loader: INCOMPATIBLE IMAGE LOAD ADDRESS	10-46
DLSV Loader: MNEMONIC NOT CONFIGURED	10-46
DLSV Loader: NO CONFIGURED SERVER	10-46
DLSV Loader: RECEIVED AN INVALID RECORD TYPE	10-46
DLSV Loader: RECEIVED NO RECORDS	10-46
DLSV Loader: RECEIVED RECORD WITH BAD CHECKSUM	10-47
DLSV Loader: RECEIVED RECORD WITH BAD LENGTH	10-47
DLSV Loader: SW DOWNLOAD ALREADY IN PROGRESS	10-47
DLSV Server: (cause)	10-48
DLSV Server: CANNOT READ FLASH	10-48

Alarm	Page
DLSV Server: CONNECTION IDLE TOO LONG	10-48
DLSV Server: DOWNLOAD COMPLETE TO	10-49
DLSV Server: F2F FLASH BANK UNAVAILABLE	10-49
DLSV Server: FAILED TO SEND SOFTWARE	10-49
DLSV Server: LOADING TO ADDRESS	10-49
DLSV Server: REQUEST WITH INVALID ADDRESS	10-49
DLSV Server: SW DOWNLOAD ALREADY IN PROGRESS	10-49
DORA - CONFIGURATION ERROR - (cause)	2-4
DORA - DIAL-OUT REQ (E.164) ABANDONED - (cause)	2-5
DORA - DORM (address)	2-6
DORA - STAT OVERFLow - (parameter)	2-6
DORA - TABLE OVERFLow	2-7
DORA - UNKNOWN CALLER - (address)	2-7
DORM - (address) DORA FAILURE - REMOVED FROM DORM TABLE	10-50
DORM - DIAL-OUT REQ (E.164) ABANDONED - DOR FAILURE	10-50
DORM - DORM COMMUNICATION ESTABLISHED	10-50
DORM - DORM LINK FAILURE	10-50
DORM - TABLE OVERFLOW	10-50
DORM CONFIGURATION - (add)	10-51
DOWNLOAD FAILED: INSUF. MEMORY FOR %s	7-9
DOWNLOAD FAILED: VIRTUAL	
DOWNLOAD FAILED: VSMIO OPERATION FAILED	7-9
DRAM CODE CHECKSUM ERROR - REPAIRED	6-4
DRAM CODE CHECKSUM ERROR - UNABLE TO REPAIR - WRONG or NO FLASH	6-4
DRAM IDATA ARRAY BITS[0 - 3]: 0x80d508 0x80d500	6-5
DRAM IDATA CHECKSUM ERROR - RELOADING IDATA	6-5
DRAM IDATA Was reloaded correctly, contact customer service with above information	6-5
DSPM CRASH REASON - %s PC=%x ADD=%x	10-51
DSPM FIRST RECOVERY SUCCESSFUL	10-51
DSPM PROTOCOL INITIALIZATION FAILED -PORT (n)	2-7
DSPM SECOND RECOVERY SUCCESSFUL	10-51
DSPM SOFTWARE DOWNLOAD COMPLETED	10-52
DSPM SOFTWARE DOWNLOAD FAILED	10-52
DUPLICATE FIX TEI %d DETECTED FOR PKT D ON BRI INTERFACE %d	10-52
Duplicate static path to (net) - in entry (p)	10-52
DVMRP.1 dvmrp_init called with NULL rfcm Context Block\r\n,	10-52
DVMRP.10 Too many routing types from remote end, lcon %d	10-52
DVMRP.11 Unknown Net %s indication on interface %d	10-52
DVMRP.12 Unknown LCON %s indication with number %d	10-53
DVMRP.13 %s	10-53
DVMRP.2 DVMRP Module Aborted; not enough RAM\r\n,	7-10
DVMRP.3 Memory allocation for failed	10-53

Alarm Index

Alarm	Page
DVMRP.4 DVMRP is not active in	10-53
DVMRP.5 %s called with a NULL DVMRPCB	10-54
DVMRP.6 DVMRP not up in lcon %d - dropping the packet	10-54
DVMRP.7 Bad format packet received, lcon %d	10-54
DVMRP.8 getbuf failed in %s	10-54
DVMRP.9 Unsupported packet type with code %d on circuit %d	10-54
DYNAMIC STATION BEING CREATED	3-4
DYNAMIC STATION BEING CREATED	3-5
DYNAMIC STATION BOOT COMPLETED	3-5
DYNAMIC STATION BOOT COMPLETED	3-5
DYNAMIC STATION BOOT STARTED	3-6
DYNAMIC STATION BOOT STARTED	3-6
E1-<%d> - <%s> - %s	10-54
Egress IP ClTcQosMap Prof #<num> does not exist	9-148
EIA HANDSHAKE COMPLETE	10-55
EIA HANDSHAKE INCOMPLETE	10-55
ENCRYPTION MIS-CONFIGURED, %s IS A NETWORK PROTOCOL	10-55
ENCRYPTION SIMM IS DEFECTIVE	7-10
END of bop_bri_boardParams	10-55
END of bop_bri_boardRestart	10-55
END of bop_bri_Call Connected() : RETURN	10-55
END of bop_bri_cd_ost_req uest() : RETURN	10-55
END of bop_bri_eia_reject() : RETURN	10-55
END of bop_bri_sig_response() : RETURN	10-56
END of bop_bri_sm_pck() : RETURN	10-56
END of bop_bri_sm_restart() : RETURN	10-56
END of bop_bri_sm_shutdown() : RETURN	10-56
END of bop_bri_trans_response () : RETURN	10-56
END of bop_bri_tx_callsetup() : RETURN	10-56
END of bop_bri_tx_dis conn_msg() : RETURN	10-56
END of bop_bri_tx_E_Eia Shutdown() : RETURN	10-56
END of bop_bri_validate_call() : RETURN	10-56
END of bop_bri_x25_response() : RETURN	10-57
END of sdrvc_traitetbenrep()	10-57
Enet %d - Excessive RX Error Condition Set	10-57
Enet - 82596 Hardware Failure (cause)	10-57
Enet - Adding to the Transmit queue failed	10-57
Enet - Excessive RX Error Condition CLR	10-58
Enet - Excessive TX Error Condition CLR	10-58
Enet - Excessive TX Error Condition Set	10-58
Enet - Loss of Carrier Condition CLR	10-58
Enet - Loss of Carrier Condition Set	10-58

Alarm	Page
Enet - RX List Error (f)	10-58
Enet - The 82596 failed to suspend operation	10-59
Enet - The Configuration command timed out	10-59
Enet - The Configuration command failed	10-59
Enet - The Individual address command failed	10-59
Enet - TX List Error (f)	10-59
Enet%d - Invalid driver state, should be disabled, function not performed.	10-59
Enet%d - Invalid driver state, should be enabled, function not performed.	10-60
Enet%d - The loopback Configuration command failed.	10-60
Enet%d - The Time Domain Reflectometry command failed.	10-60
Enet- Bus Throttle Timers wouldn't load.	10-60
Enet13 - Diag Check (cause)	10-60
EPx rescued msg 1 n1/n2/n3:n4n5	10-65
EPx rescued msg n0 n1/n2:n3/n4:n5/n6:n7/n8:n9/n10	10-65
EPx task rescued from possible deadlock	6-5
EPx task rescued from possible deadlock	10-64
Error in ATMARP Packet received on LCON (n) - (msg), (field)	8-4
Error in ATMARP Packet received on LCON (n) - (msg), (field)	8-5
Error in ATMARP Packet received on LCON (n) - (msg), (field)	9-71
ERROR ON CHANNEL (n) - (cause)	4-9
ESTABLISHED ENCRYPTION SESSION	5-8
ESTABLISHED IPSec CONNECTION with aa.bb.cc.dd	9-154
ESTABLISHED IPSEC CONNECTION WITH (aa.bb.cc.dd)	10-65
ESTABLISHED ISAKMP CONNECTION WITH aa.bb.cc.dd	9-154
ESTABLISHED ISAKMP CONNECTION WITH (aa.bb.cc.dd)	10-65
ETH.001 brd rev unkwn typ (type) (source) -> (dest) nt (net)	9-84
ETH.002 rev unkwn typ (type) (source) -> (dest) nt (net)	9-85
ETH.003 brd 802.3 bd in (actual) (claimed) (source) -> (dest) nt (net)	9-85
ETH.004 802.3 bd in (actual) (claimed) (source) -> (dest) nt (net)	9-86
ETH.005 DN bd Ln (actual) (claimed) (source) -> (dest) nt (net)	9-86
ETH.006 IPX bd ECONFIG 8137 nd (add) nt (net)	9-86
ETH.007 IPX bd ECONFIG 802.2 nd (add) nt (net)	9-87
ETH.008 IL (selftest) fld (error) nt (net)	9-87
ETH.009 PE selftest) fld (error) nt (net)	9-87
ETH.010 LLC unk SAP (DSAP) (source) -> (dest) nt (net)	9-88
ETH.011 LLC nt typ 1 (LLC_Cont) nt (net)	9-88
ETH.012 LLC RSP (LLC_SSAP) nt (net)	9-88
ETH.013 LLC XID (LLC_SSAP) nt (net)	9-88
ETH.014 LLC TEST (LLC_SSAP) nt (net)	9-89
ETH.015 unrec ctl (LLC_Cont) nt (net)	9-89
ETH.016 VL (selftest) fld (error) nt (net)	9-89
ETH.017 LOOP rev (source)->(dest), nt (net)	9-89

Alarm Index

Alarm	Page
ETH.018 LOOP odd skp count, (source)->(dest), nt (net)	9-90
ETH.019 LOOP func (function) forw, (source)->(dest), nt (net)	9-90
ETH.020 LOOP mc fwd dst (forw), (source)->(dest), nt (net)	9-90
ETH.021 LOOP fwd (source) -> (forw), nt (net)	9-91
ETH.022 LOOP fwd to (forw) dsc, rsn (code), nt (net)	9-91
ETH.023 LLC RSP to (dest) dsc, rsn (code), nt (net)	9-91
ETH.024 MOP bd in (actual), (claimed), (source) -> (dest) nt (net)	9-92
ETH.025 LOOP bd skp (count), (source) -> (dest), nt (net)	9-92
ETH.031 NP no buf fr slf-tst, nt (net)	9-92
ETH.032 NP slf-tst cmd, nt (net)	9-93
ETH.033 NP diag cmd, nt (net)	9-93
ETH.034 slf-tst cmd timeout, nt (net)	9-93
ETH.037 NP diags OK, ETH bad, stat (code), nt (net)	9-94
ETH.038 NP load timeout, nt (net)	9-95
ETH.039 NP (command) rst, nt (net)	9-95
ETH.040 NP slf-tst fld (code), nt (net)	9-95
ETH.041 NP loaded, slf-tst, nt (net)	9-96
ETH.042 Unable to get buf for ethernet packet.	9-96
ETH.35 NP diag cmd timeout, nt (net)	9-93
ETH.36 NP fld (mod) diag, stat (code), nt (net) disabled	9-94
ETH.41 Priority mapping profile (profnum) not configured	14-6
ETH.42 disc vlan frame with cfi set on port (n) vlan (m)	14-7
EXCEEDING MAXIMUM RANGE ALLowED	10-65
EXCEEDING THE MAXIMUM NUMBER OF INTERFACES ALLOWED	10-66
EXCEEDS MAXIMUM NUMBER OF LINKS FOR THIS BUNDLE	10-66
EXTENDED CHECKSUM ERROR: SLOT (s) DISABLED	7-10
EXTENDED SOFTWARE LOAD FAILS IN SLOT (s)	7-10
FAILED KEY EXCHANGE	10-66
FAILED KEY EXCHANGE, NO RESPONSE	10-66
FAILED TO COPY SOFTWARE	10-66
FAILED TO NEGOTIATE IPSec PARAMETERS WITH aa.bb.cc.dd (Reason)	9-154
FAILED TO NEGOTIATE ISAKMP PARAMETERS WITH aa.bb.cc.dd (Reason)	9-153
FAILED TO NEGOTIATE IPSEC PROPOSAL WITH (aa.bb.cc.dd) (yy**)	10-62
FAILED TO NEGOTIATE ISAKMP PROPOSAL WITH (aa.bb.cc.dd) (yy**)	10-61
FAILED TO NEGOTIATE ISAKMP PROPOSAL WITH (aa.bb.cc.dd) (yy**)	10-62
FAILED TO UPDATE SOFTWARE	10-67
FAN FAILED	7-11
FLASH CHECKSUM ERROR	10-67
FLASH CHECKSUM ERROR, SLOT (s)	10-67
FLASH CHECKSUM ERROR, (b) (e) (a)	10-67
FLASH CHECKSUM OK, (b) (e) (a)	10-67
Flow (src addr -dst addr), (protocol), (src port -dst port) dropped	2-7

Alarm	Page
Flow (src addr -dst addr), (protocol), (src port -dst port) dropped	10-68
Flow (src addr -dst addr), (protocol), (src port -dst port) has primary link available.	2-8
Flow (src addr -dst addr), (protocol), (src port -dst port) is active on nexthop nnnn	2-7
Flow (src addr -dst addr), (protocol), (src port -dst port) is expired	2-7
Flow (src addr -dst addr), (protocol), (src port -dst port) is no more active on nexthop nnnn	2-8
Flow (src addr -dst addr), (protocol), (src port -dst port) is out of allowed Time of Week	2-8
FOUND (n) BAD BASE KEYS IN CMEM	10-68
FOUND (n) GOOD BASE KEYS IN CMEM	10-68
FRAME DROPPED AFTER MAX RETRY	10-68
FRAME RECEIVED WITH BAD LENGTH: DLCI (n)	3-6
FRAME RECEIVED WITH BAD LENGTH: DLCI (n)	10-68
FRAME TOO LONG	10-68
FRMR (hh/hh/hh)	10-69
FUNCTION NAME: %s, SIG_STATE: %d	10-69
GW.001 Copyright 1984 Massachusetts Institute of Technology	9-97
GW.002 Portable CGW (name) Rel (level) strtd	9-97
GW.003 Unus pkt len (len) nt (net_id)	9-98
GW.004 Sys (type) q adv alloc (adv_len) excd (act_len)	9-99
GW.005 Bffrs: (total) avail (free) idle fair (fair) low (high)	9-100
GW.006 Pkt frm nt (net_id) for uninit prt, disc	9-100
GW.007 Ip err (code) nt (net_id)	9-100
GW.008 Ip ovfl nt (net_id), disc	9-101
GW.009 Nt dwn ip rstrt nt (net_id)	9-101
GW.010 Ip q len (len) no ip buf nt (net_id)	9-102
GW.014 Nt dwn op rstrt nt (net_id)	9-103
GW.017 Intfc hdw mssng nt (net_id)	9-103
GW.018 Strt nt slf tst nt (net_id)	9-104
GW.019 Slf tst nt (net_id)	9-104
GW.020 Nt pss slf tst nt (net_id)	9-104
GW.022 Nt fld slf tst nt (net_id)	9-104
GW.023 Nt dwn nt (net_id)	9-104
GW.025 Nt fld mnt nt (net_id)	9-105
GW.026 Mnt nt (net_id)	9-105
GW.027 No pkt fr mnt nt (net_id)	9-105
GW.028 Snk dsc pkt prt (type) to (host)	9-105
GW.029 Int dis nt (net_id)	9-106
GW.030 (heap) bytes reserved by (subsys)	9-106
GW.031 IP q alloc fl nt (net_id) avl (buffers)	9-106
GW.032 Op err (code) hst (host) nt (net_id)	9-107
GW.033 Op err cnt excd hst (host) nt (net_id)	9-108
GW.034 Rtrns cnt excd hst (host) nt (net_id)	9-109
GW.035 Nt dwn to hst (host) nt (net_id)	9-110

Alarm Index

Alarm	Page
GW.036 Op ovfl to hst (host) nt (net_id)	9-111
GW.037 Nt dwn, disc pkt to hst (host) nt (net_id)	9-112
GW.038 User default name has logged on	9-112
GW.039 Failed logon:ID = default name	9-112
GW.040 to cl dnd nt (net_id)	9-113
GW.041 in cl dnd nt (net_id)	9-113
GW.042 in cl unk addr (dial),/(subdial), rj nt (net_id)	9-113
GW.043 CML state (state), event (event), nt (net_id)	9-113
GW.044 No cnfg nt (net_id)	9-113
GW.045 bd dl net dial_interface_id, nt (net_id)	9-114
GW.046 bd dl dst dest_dial_name, nt (net_id)	9-114
GW.047 idle timer exp nt (net_id)	9-114
GW: alloc busy buffer	9-116
GW: Bd cnf inf nt hdr lnghts	9-114
GW: freeing free buffer	9-116
GW: incompatible L_MAX	9-115
GW: incompatible net table vers	9-114
GW: incompatible P_MAX	9-115
GW: incompatible T_MAX	9-115
GW: no mem for the prot tbl	9-115
H323 Node Wide Parameters Boot Complete	10-69
H323 NODE WIDE PARAMETERS NOT INSTALLED - Out of memory.	10-69
handle_pacing %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	11-6
handle_pacing %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	10-138
HTTPD AUTHENTICATION FAILURE	13-39
HTTPD-General Debug: %s	13-39
HTTPD-General Error: %s	13-39
HTTPD-Internal Error: %s	13-39
HW BOARD FAILURE	7-11
IBEX INIT FAILURE	11-3
ICMP.001 bd cks 0xreceived_ checksum (checksum) (source) -> (dest)	9-116
ICMP.002 ech (source) -> (dest)	9-117
ICMP.003 ech rp (source) -> (dest)	9-117
ICMP.004 unhnd typ (type) (code) (source) -> (dest)	9-117
ICMP.005 unhnd brd typ (type) (code) (source) -> (dest)	9-118
ICMP.006 bd typ (type) (code) (source) -> (dest)	9-118
ICMP.007 addr msk (source) -> (dest)	9-118
ICMP.008 addr msk rep (source) -> (dest)	9-118
ICMP.009 no pkt or mem	9-118
ICMP.010 amb addr msk (source) -> (dest)	9-119
ICMP.011 err code sndng pkt to nt (net_id)	9-119
ICMP.012 rdr (source) -> (dest) to (new_add)	9-119

Alarm	Page
ICMP.013 bd prm off (offset) (source) -> (dest)	9-120
ICMP.014 snd (type) (code) (source) -> (dest)	9-120
ICMP.015 shrt ICMP hdr (len) src (source)	9-120
IDCM Invalid Packet Type(n)	6-11
IGMP.1 RFCM Context Block NULL in function Name.	10-69
IGMP.10 Multicast not enabled, IGMP shall not come up	10-69
IGMP.11	10-69
IGMP.12	10-70
IGMP.13 IP Context Block NULL	10-70
IGMP.14 IGMP Packet received on %d IGMP Circuit	10-70
IGMP.15 IGMP Membership Query on %d IGMP Circuit	7-11
IGMP.16 IGMP Membership Report(VER_1) on %d IGMP Circuit for %s Multicast Address	7-11
IGMP.18 IGMP Membership Leave message on %d IGMP Circuit for %s Multicast Address	7-11
IGMP.19 IGMP Leave for Unknown grp member %s on ckt %d	7-11
IGMP.2 IGMP Module Aborted; not enough RAM	7-12
IGMP.20 IGMP Unknown Packet type %d on ckt %d	7-12
IGMP.21 IGMP Group Membership Timeout	7-12
IGMP.3 Memory allocation for %s failed	10-70
IGMP.4 IGMP Module not up	10-70
IGMP.5 Packet %s Error	10-70
IGMP.6 Getbuff failure	10-70
IGMP.7 Failure to insert a group	10-71
IGMP.9 IGMP Packet dropped for IGMP NOT Active on 5	10-71
Illegal Port Type	2-8
ILLEGAL PORT TYPE FOR D-CHANNEL	2-8
IN-SUFFICIENT MEMORY FOR X25 CALL TRANSLATION TABLES	7-12
INACTIVITY TIME OUT	10-71
InATMARP (ops) received on LCON (n)	8-5
InATMARP (ops) received on LCON (n) with duplicate remote IP Address (add)	8-2
InATMARP (ops) received on LCON (n) with out of LIS remote IP Address (add)	8-2
InATMARP (ops) received with NULL Source IP Address on LCON (n)	8-3
InATMARP (ops) sent on LCON (n)	8-6
InATMARP Reply received with NULL Target IP Address on LCON (n)	8-3
INBOUND LINK BLOCKED	7-12
INBOUND LINK UNBLOCKED	7-12
INCOMING CALL FROM (call num) ON BRI INTERFACE (I/F #1) B (I/F #2) CHANNEL	9-76
INCOMING CALL FROM (number) ON DSL (line)	7-26
INCOMING CALL FROM UNKNOWN NUMBER ON DSL (line)	7-26
INCOMPATIBLE %s DETECTED FOR ISDN	10-71
INCOMPATIBLE (h) DETECTED FOR ISDN	9-77
INCOMPATIBLE DESTINATION	10-71
INCONSISTENT LINK NEGOTIATION	10-71

Alarm Index

Alarm	Page
INCORRECT LOGIN	10-72
Ingress IP ClTcQosMap Prof #<num> does not exist	9-147
INITIALIZATION FAILED - MODULE SNABSC NOT INCLUDED	9-126
INITIALIZATION FAILED - MODULE SNABSC NOT INCLUDED	13-40
INPUT BUFFER OVERRUN	10-72
Insuff Q mgmt channels	9-151
Insuff service channels	9-151
Insuff traffic conditioners	9-150
INSUFFICIENT DYNAMIC MEMORY TO SUPPORT %s CONFIGURATION	11-4
INSUFFICIENT DYNAMIC MEMORY TO SUPPORT %S CONFIGURATION	3-3
INSUFFICIENT MEMORY TO INITIALIZE ENCRYPTION	7-13
INSUFFICIENT MEMORY TO INITIALIZE IPSec MODULE	9-154
INSUFFICIENT MEMORY TO INITIALIZE IPSec MODULE	10-72
INSUFFICIENT MEMORY TO PROTECT STATION	3-6
INSUFFICIENT MEMORY TO SUPPORT SNABSC_CM CONFIGURATION	9-126
INSUFFICIENT MEMORY TO SUPPORT SNABSC_CM CONFIGURATION	13-40
INSUFFICIENT MEMORY TO SUPPORT APPN CONFIGURATION	10-72
INSUFFICIENT MEMORY TO SUPPORT SNABSC_CM CONFIGURATION	11-17
INSUFFICIENT MEMORY TO SUPPORT TN3270 CONFIGURATION	10-72
INSUFFICIENT RAM FOR CONFIGURATION	7-13
INSUFFICIENT RESOURCES TO COMPLETE IPSEC EXCHANGE	10-72
INTER CHARACTER TIMEOUT	10-73
INTIALIZATION FAILED	11-17
INVALID BCSR FOR SLOT %d	11-17
Invalid config of wildcard community profile in policy #xxx	13-39
INVALID DEVICE RESPONDING	3-7
Invalid N(R)	9-21
Invalid number of X.25 data bytes out of range	9-21
Invalid P(R)	9-21
Invalid P(S)	9-22
INVALID PHB (phb), PCK TREATED WITH DEFAULT OF Q'ING & SCH'ING PROF # (n)	10-73
Invalid Port Number	9-22
Invalid Port Subtype	9-22
INVALID PRI SIGNALLING : PORT = %d : STATE = %d SIG. STATE = %d, STIMULOUS = %d	2-8
Invalid Protocol Packet to be sent on VC Multiplexed LCON (n)	8-6
INVALID SESSION MESSAGE IN IDLE STATE FROM SLOT (s)	5-4
Invalid value of X.25 level	9-22
INVALID VOICE SIGNALING : PORT = %d : SIG. STATE = %d, STIMULUS	
IP Interface - (n) - Exceeding Maximum Range Allowed	9-22
IP Interfaces - (x) to (y) - Exceeding Maximum Range Allowed	9-22
IP Parameter Boot Complete	9-44
IP Parameter Boot Failed	9-44

Alarm	Page
IP Tables Boot Complete	9-44
IP Tables Boot Failed	9-44
IP.001 q ovrf (source) -> (dest) nt (net_id)	9-23
IP.002 not V4 hdr version_number nt (net_id)	9-23
IP.003 shrt hdr (hdr_length) pkt ln (pkt_length) nt (net_id)	9-23
IP.004 bd hdr cks (rcsum), (ccsum), (source) -> (dest)	9-24
IP.005 pkt trunc (sleng) pkt ln (tleng) (source) -> (dest)	9-24
IP.006 pkt (source) -> (dest) dsc rsn (cause), nt (net_id)	9-25
IP.007 (source) ->(dest)	9-25
IP.008 no rte (source) -> (dest) dsc	9-26
IP.009 TTL zero (source)-> (dest)	9-26
IP.010 dsc pkt (source) -> (dest) nt (net_id) no IP	9-26
IP.011 unsup mcst (source) -> (dest)	9-26
IP.012 bd nt cl (source)s -> (dest)	9-26
IP.013 unsup bcst (source)s -> (dest)	9-27
IP.015 bad subnet (source)s -> (dest)	9-27
IP.016 nt (sub_add) add fail, bd sbnt	9-27
IP.017 nt (net_add) add fail, tbl ovrfl	9-27
IP.018 nt (net_add) add fail, bd nt	9-27
IP.019 re-add stat rt to (net)	9-28
IP.020 int for (net) add fail, dup addr	9-28
IP.022 add nt (net_ip_add) int (int_ip_add) nt (net_id)	9-28
IP.024 ign stat rt to (net), mask (mask)	9-28
IP.025 add nt (new_net) rt via (cur_net) nt (net_id).	9-28
IP.028 unnum stat rt on non-SL, (nets) thru (nets)	9-29
IP.031 Unnum addr rej, nt (net_id)	9-29
IP.032 fq ovf (source) -> (dest) nt (net_id)	9-29
IP.033 cant frg (source)s -> (dest) nt (net_id)	9-30
IP.034 bd frg (source) -> (dest) foff offset	9-30
IP.035 cant alloc for frg nt (net_id)	9-30
IP.036 rcv pkt prt (prot) frm (source)	9-30
IP.037 brd pkt (source) -> (dest) prot (prot) no srvr	9-31
IP.038 pkt (source) -> (dest) prt (prot) no srvr	9-31
IP.039 GGP echo frm (source) -> (dest)	9-31
IP.040 GGP unhnd opc (opcode), (source) -> (dest)	9-31
IP.041 GGP bd opc (opcode) (source) -> (dest)	9-32
IP.042 illgl ARP sbnt req (source) -> (dest)	9-32
IP.043 rcvd ARP sbnt rqst (source) -> (dest)	9-32
IP.044 ARP sbnt rqst ign (source) -> (dest)	9-33
IP.045 snt ARP rte (source) -> (dest)	9-33
IP.046 unkn opt (opt) frm (source)	9-33
IP.047 opt (opt) bd fmt frm (source)	9-33

Alarm Index

Alarm	Page
IP.048 strict src rt bd nxt hop (source) -> (dest)	9-34
IP.049 bd tmstmp fmt (tstamp) frm (source)	9-34
IP.050 tmstmp ovrf, (source) -> (dest)	9-34
IP.051 rs ovfl, PORT (n) frm (source)	9-34
IP.052 no stor for rs, PORT (n) frm (source)	9-35
IP.053 reas pkt too big (psize), PORT (n) frm (source)	9-35
IP.054 rs TTL exp, PORT (n) frm (source)	9-35
IP.055 rs free, PORT (n) frm (source)	9-35
IP.056 add dflt nt gw (add) nt (net_id)	9-36
IP.058 del nt (net) rt via (gate) nt (net_id)	9-36
IP.059 sbnt (net) dfnd	9-36
IP.060 del sbntd nt (net)	9-36
IP.061 add lcl pkt to ip op q	9-36
IP.062 rcvd ip frg frm (source)	9-36
IP.063 rasmd pkt frm (source)	9-37
IP.064 frg pkt (source) -> (dest)	9-37
IP.065 add frg to op frg q (source) -> (dest)	9-37
IP.066 dsc pkt (source) -> (dest) nt (net_id) no IP on int	9-37
IP.067 RIP disabld on int (add) var len sbnt msks	9-37
IP.068 routing cache cleared	9-38
IP.069 routing cache garbage collecting...	9-38
IP.070 cache entry (dest) cleared	9-38
IP.071 ARP sbnt rqst (source) -> (dest), same sbnt, ign	9-38
IP.072 LL broadcast (source) -> (dest), discarded	9-39
IP.073 canÕt copy (source) -> (dest), discarded	9-39
IP.074 Acc cont # (acte) cache (action), (source) -> (dest), prot (proto)	9-39
IP.075 Acc cont # (acte) cache (action), (source) -> (dest), (proto) port (srcprt)	
IP.076 Acc cont # (acte) (action), (source) -> (dest), port (proto)	9-40
IP.077 Acc cont # (acte) (action), (source) -> (dest), (proto) port (srcprt)	
IP.078 Acc cont miss dropped, (source) -> (dest), port (proto)	9-41
IP.079 Acc cont miss dropped, (source) -> (dest), (proto) port (srcprt) -> (dstprt)	9-42
IP.080	9-42
IP.081 shrt pkt ln (len), (source) -> (dest)	9-42
IP.082 dsc ASB pkt (source) -> (dest) nt %d int %s/ %d not frm shortest path	9-43
IP.083 ASB pkt (source) -> (dest) sending to nt %d int %s / %d	9-43
IP.084	9-43
IP.085 addr (dupaddr) ->int (intf) may conflict with other addr in network	9-43
IpBaRmark Prof #<num> does not exist	9-147
IPCP negotiated address -(x.x.x.x)	9-44
IPSEC MODULE CANNOT RUN: ENCRYPTION MODULE IS DOWN OR MISSING	10-73
IPSEC PROFILE (xx) DOES NOT EXIST	10-73
IPSec PROFILE xx DOES NOT EXIST	9-154

Alarm	Page
IPX ClTcQosMap Prof #<num> does not exist	9-148
IPX Disabled - memory allocation failure during init	10-73
IPX Parameters Boot Complete	9-70
IPX Parameters Boot Failed	9-70
IPX protocol subsystem high priority traps	7-27
IPX Tables Boot Complete	9-70
IPX Tables Boot Failed	9-70
IPX tables boot failed : No memory for IPX context block.	7-13
IPX tables boot failed : No memory for IPX_CTP context block	7-13
IPX.001 Packet from (s_net) (s_node) for (d_net) (d_node) ignored.	9-44
IPX.002 ovf (s_net) (s_node) (d_net) (d_node) nt (net_id)	9-45
IPX.003 bd hst chksm frm (s_net) (s_node)	9-45
IPX.004 err pkt (type) frm (s_net) (s_node)	9-45
IPX.005 no hndlr for skt (dest_soc) typ (type) frm (s_net) (s_node)	9-46
IPX.006 (dest_soc) typ (type) frm (s_net) (s_node)	9-46
IPX.007 no host address set for net (net_id), not enabled	9-46
IPX.008 SAP bad type (type) (s_net) (s_node)	9-47
IPX.009 SAP gen reply from (s_net) (s_node)	9-47
IPX.010 SAP table overflow, discarded type (type) (name)	9-47
IPX.011 SAP service type (type) (name) moved to (new_net) (new_node)	9-48
IPX.012 SAP deleted type (type) (name)	9-48
IPX.013 SAP bad length Nearest Service Query from (s_net) (s_node) length	9-48
IPX.014 SAP nearest query from (s_net) (s_node)	9-49
IPX.015 SAP General query from (s_net) (s_node)	9-49
IPX.016 SAP general Service Query sent, net (net_id)	9-49
IPX.017 No memory for SAP General Service Query of Reply, net (net_id), (count) packet sent	9-49
IPX.018 SAP General Service Reply sent, net (net_id), (count) packets	9-50
IPX.019 NB brd (s_net) (s_node) -> (d_net) (d_node), nt (net_id), (count) hops	9-50
IPX.020 NB too many hops frm (s_net) (s_node) nt (net_id), ign	9-51
IPX.021NETBIOS from (s_net) (s_node) net (net_id), already (con_net)	9-51
IPX.022 NETBIOS from (s_net) (s_node), no memory to copy	9-52
IPX.023 NETBIOS from (s_net) (s_node), non-broadcast net (net_id) unsupported	9-52
IPX.024 NETBIOS from (s_net) (s_node), un-numbered net (net_id) unsupported	9-52
IPX.025 NETBIOS from (s_net) (s_node), no buffer to copy	9-53
IPX.026 NB and dsc, nt (net_id) , rsn (cause)	9-53
IPX.027 bd RIP typ (RIP_opcode) frm (s_net) (s_node)	9-54
IPX.028 RIP resp frm (s_net) (s_node)	9-54
IPX.029 bd nt network in RIP frm (s_net) (s_node)	9-54
IPX.030 nt rttbl ovrfl, dscrd (net)	9-54
IPX.031 nw rt to (net) via (router_net), (router_node), (count) hops	9-55
IPX.032 rt to network aged away	9-55
IPX.033 Rspnd to RIP rqst frm (s_net), (s_node)	9-55

Alarm	Page
IPX.034 RIP rqst frm (s_net), (s_node) shrt, In (pac_len)	9-55
IPX.035 RIP Query sent, net (net_id)	9-56
IPX.036 no mem for RIP pkt nt (net_id), (count) pkts sent	9-56
IPX.037 RIP resp sent nt (net_id) (count) pkts	9-56
IPX.038 (s_net) (s_node) (d_net) (d_node) ign	9-56
IPX.039 RIP delta resp sent nt (net_id), (count) pkts	9-57
IPX.040 RIP resp snd dsc, nt (net_id), rsn (cause)	9-57
IPX.044 SAP delta gen rply nt (net_id), (count) pkts	9-59
IPX.045 SAP new serv typ (type) nm (name) via (net) (node), (count) hops, nt (net_id)	9-60
IPX.046 SAP nearest qry frm (s_net) (s_node) ignored, nt (net_id)	9-60
IPX.047 SAP query snd dsc, nt (net_id), rsn (cause)	9-61
IPX.048 SAP resp snd dsc, nt network ID, rsn (cause)	9-62
IPX.049 SAP no serv typ (type) for (s_net) (s_node) , nt (net_id)	9-62
IPX.050 SAP dead serv type (type) nm (name) from (net) (node), nt (net_id)	9-63
IPX.051 RIP route died to network from (router_net) (router_node)	9-64
IPX.052 RIP resp frm wrong (s_net) (s_node) not (local_net), nt (net_id)	9-64
IPX.053 SAP resp frm wrong net (s_net) (s_node) not (local_net), nt (net_id)	9-65
IPX.054 SAP serv typ (type) nm (name) now via (net) (node), (count) hops, nt (net_id)	9-66
IPX.055 new RIP net network via (router_net) (router_node) (count) hops	9-66
IPX.056 RIP route to network garbage coll	9-67
IPX.057 SAP del typ (type) nm (name), nt (net_id) down	9-67
IPX.058 SAP typ (type) nm (name) garbage coll	9-67
IPX.059 SAP unreach serv typ (type) nm (name) at (serv_net) (serv_node) from (via_net) (via_node) , nt (net_id)	9-68
IPX.060 SAP periodic GSR starting	9-68
IPX.061 SAP periodic GSR completed, (count) pkts	9-68
IPX.062 No mem for SAP periodic GSR pkt (count), delaying, nt (net_id)	9-69
IPX.063 SAP periodic GSR snd dsc, nt (net_id), rsn (code)	9-69
IPX.064 SAP periodic GSR sent, (count) entries, nt (net_id)	9-70
IPX_041 RIP query snd dsc, nt (net_id), rsn (cause)	9-58
IPX_042 SAP gives near reply typ (type) nm (name) to (s_net) (s_node), (net_id)	9-58
IPX_043 SAP nearest qry for typ (type) frm (s_net) (s_node) nt (net_id)	9-59
IPXWAN.1 ipxwan_init called with NULL rfcm Context Block	10-74
IPXWAN.10 Rcvd Tmr Req - option len not 1 for routing type option, lcon %d	10-74
IPXWAN.11 Rcvd Tmr Req - wnode id non-zero with extended node id option set, lcon %d	10-74
IPXWAN.12 Rcvd Tmr Req - option len not 4 for extended node id, lcon %d	10-74
IPXWAN.13 Rcvd Tmr Req - configuration error, lcon %d	10-74
IPXWAN.14 Rcvd Tmr Req - no common routing type, lcon %d	10-74
IPXWAN.15 Rcvd Tmr Resp - wnode id zero, lcon %d	10-75
IPXWAN.16 Rcvd Tmr Resp - multiple routing types marked yes, lcon %d	10-75
IPXWAN.17 Rcvd Tmr Resp - could not set the routing type, lcon %d	10-75
IPXWAN.18 Rcvd Tmr Resp - routing type not supported, lcon %d	10-75
IPXWAN.19 Rcvd Tmr Resp - option len not 1 for routing type option, lcon %d	10-75

Alarm	Page
IPXWAN.2 IPXWAN Module Aborted; not enough RAM	10-75
IPXWAN.20 Rcvd Tmr Resp - header compression not supported, lcon %d	10-75
IPXWAN.21 Rcvd Tmr Resp - no routing type option with yes, lcon %d	10-76
IPXWAN.22 Rcvd Info Req - rcvd wnode id zero, lcon %d	10-76
IPXWAN.23 %s - bad info exchange option, lcon %d	10-76
IPXWAN.24 %s - no info exchange option, lcon %d	10-76
IPXWAN.25 %s - zero netno proposed for numbered RIP/SAP, lcon %d	10-76
IPXWAN.26 %s - non-zero netno proposed for an unnumbered protocol, lcon %d	10-76
IPXWAN.27 %s - the proposed netno is not equal to active netno, lcon %d	10-76
IPXWAN.28 Rcvd Info Resp - rcvd wnode id is incorrect, lcon %d	10-77
IPXWAN.29 Rcvd Info Resp - the proposed netno is already active, lcon %d	10-77
IPXWAN.3 Memory allocation for %s failed\r\n	10-77
IPXWAN.30 Rcvd Info Resp - could not set the active netno, lcon %d	10-77
IPXWAN.31 getbuf failed in %s	10-77
IPXWAN.32 Event %d ignored in state %d, lcon %d	10-77
IPXWAN.33 Old State:%d, Event:%d, New State:%d, lcon %d	10-77
IPXWAN.34 Too many routing types from remote end, lcon %d	10-77
IPXWAN.4 IPXWAN is not active in %s\r\n	10-78
IPXWAN.5 IPX not active in %s\r\n	10-78
IPXWAN.6 %s called for a LAN interface	10-78
IPXWAN.7 %s called with a NULL IPXWANCB	10-78
IPXWAN.8 IPX not up in lcon %d - dropping the packet	10-78
IPXWAN.9 Bad format packet received, lcon %d	10-78
ISAKMP DETECTED DEAD PEER aa.bb.cc.dd	10-18
ISAKMP POLICY (n) DOES NOT EXIST	10-79
ISAKMP PRESHARED KEY (xx) HAS BEEN CHANGED	10-79
ISAKMP PRESHARED KEYS TABLE BOOTED	10-80
ISDN BRI CORE BOOT COMPLETED	10-78
ISDN BRI INTERFACE %d IS ACTIVE	10-78
ISDN BRI INTERFACE %d IS INACTIVE	10-78
ISDN BRI INT. %d %s DISCONNECTED FROM %s, CAUSE: %d	10-79
ISDN BRI INT. %d BOOT COMPLETED	10-79
ISDN BRI SWITCH CONFIGURED OVERRIDE	10-79
ISDN Config Error	10-79
ISDN LINE DOWN:SWITCHED TO Low BANDWIDTH	7-13
ISDN LOOP TEST %s %s %s	10-79
ISDN PRI INTERFACE (i/f) IS ACTIVE	7-25
ISDN PRI INTERFACE (i/f) IS INACTIVE	7-26
ISDN SIGNALING MESSAGE RECEIVED FOR CHANNEL %d	4-9
ISDN SIGNALING MESSAGE RECEIVED FOR CHANNEL %d	4-9
ISDN VOICE ERROR: me_ccs_voice.c Line # %d	11-5
ISDN VOICE: %d CALL TO %s FROM %s FAILED ON PORT %d, %s	11-5

Alarm Index

Alarm	Page
ISDN VOICE: UNSUPPORTED MSG RCV'ed FROM CC, MSG_ID = 0x%x	11-5
ISKAMP POLICY # xx DOES NOT EXIST	9-154
IV USAGE FORCED BY REMOTE ENCRYPTION PEER	10-80
LBU PORT (n) is now servicing multiple ports.	2-9
LCON RX DISCARD - NO NEXT HOP TO %s	10-80
LCON RX DISCARD - NO ROUTE TO %s	10-80
LCON TX DISCARD - UNKNOWN NEXT HOP %s	10-80
LEASED LINE DOWN:SWITCHED TO High BANDWIDTH	7-14
LEASED LINE UP:SWITCHED TO Low BANDWIDTH	7-14
LINE DOWN	7-14
LINE DOWN	7-14
LINE OPERATIONAL	7-14
LINE OPERATIONAL	7-14
LINE OPERATIONAL	7-14
link %d - UNKNOWN STP BPDU received	10-80
LINK DOWN	7-15
LINK DOWN	7-15
LINK DOWN	10-80
LINK DOWN	10-81
LINK DOWN	10-81
LINK IS LOOPED BACK	10-81
LINK UP	7-15
LINK UP	7-15
LLC LT: INVALID FRAME (t) RCVD FROM (w) LOC MAC/SAP (a)(p), REM MAC/SAP (a)(p)	10-81
LLC LT: SESSION (n) STARTED -LOC MAC/SAP (a)(p), REM MAC/SAP (a)(p)	5-2
LLC LT: SESSION (n) TERMINATED (cause) LOC MAC/SAP (a)(p), REM MAC/SAP (a)(p)	5-3
LLC LT: SESSION NOT STARTED - (cause) LOC MAC/SAP (a)(p), REM MAC/SAP (a)(p)	5-2
LOCAL DRAM EXHAUSTED	7-15
LOCAL FLASH COPY COMPLETE	10-81
LOCAL FLASH COPY FAILED	10-81
LOG CLEARED	10-82
LOGIN OK	10-82
LOST (n) MESSAGES IN 60 SECONDS	10-82
LOST MAIN CHANNEL CONNECTION	4-9
LSC - (app) STATION (n) - 5494 CONTROLLER DOWN	3-7
LSC - (app) STATION (n) - 5494 REMOTE CONNECTION ESTABLISHED	3-7
LSC - (app) STATION (n) - 5494 WORKSTATION DOWN, LU ID : (ID)	3-8
LSC - (app) STATION (n) - 5494 CONTROLLER UP	3-8
LSC - (app) STATION (n) - 5494 REMOTE CALL ESTABLISHED	3-9
LSC - (app) STATION (n) - 5494 STATION RECEIVED A REMOTE DISC	3-9
LSC - (app) STATION (n) - 5494 WORKSTATION UP, LU ID : (ID)	3-10
LSC-(app) STATION (n) - 5494 (counter) RETRY LIMIT REACHED	3-11

Alarm	Page
LUA SOCKET CONNECT FAILED	11-17
LUA SOCKET CONNECT FAILED	9-126
LUA SOCKET CONNECT FAILED	13-39
MASTER FAILED TO COPY EXTENDED S/W	7-15
MASTER POLLED EARLY	3-12
MASTER POLLED EARLY	10-82
Max InATMARP Retries over on LCON (n).	8-3
MEMORY ALLOCATION FAILED	7-15
MESSAGES LOST	10-82
Missing BGP/BGPRT module	13-41
MISSING DIM ON BOARD (x), PORT (n)	2-9
MODEM FAULTY OR NOT CONNECTED	7-16
MONITORED NAME IN SWITCHED SERVICE ENTRY	10-82
MOTHERBOARD LAB STRAP INSTALLED	7-16
MSG_EXCESSIVE RX_ERRORS	10-64
MSG_EXCESSIVE_RX_CLEAR	10-64
MSG_EXCESSIVE_TX_CLEAR	10-64
MSG_EXCESSIVE_TX_ERRORS	10-63
MSG_FPGA_INIT_FAILED	10-64
MSG_LOSS_OF_ CARRIER	10-63
MSG_LOSS_OF_ CARRIER_CLEAR	10-64
MSG_TX_LIST_PUT_FAILED	10-63
MULTICLASS FAILURE	14-7
MUX,%s DIALING TO %s ON BRI INT. %d %s CHANNEL	4-10
MUX,INCOMING CALL %s ON BRI INT. %d B%1d CHANNEL	4-10
NCI - PORT (n) VIOLATIONS, PORT DEGRADED	2-9
NCI - PORT (n) VIOLATIONS, PORT DISCONNECTED	2-10
NCI - PORT (n) VIOLATIONS, PORT LOCKED	2-10
NCI PORT (n) VIOLATIONS, NO ACTION	2-10
Network Clock derives from TDM- (i/f)	7-25
Network Clock lost from TDM-(i/f)	7-25
NETWORK DLCI UNASSIGNED: DLCI (n)	3-12
NO BUNDLES AVAILABLE	10-83
NO CHANNELS CONFIGURED	4-10
No classifiers in Egress IP ClTcQosMap Prof #<num>	9-148
No classifiers in Ingress IP ClTcQosMap Prof #<num>	9-148
No classifiers in IPX ClTcQosMap Prof #<num>	9-149
No classifiers in TB ClTcQosMap Prof #<num>	9-149
NO CONFIG FOR STN	3-12
No Ethernet SAK	10-83
NO H323 NODE RECORDS FOUND - Installing Defaults	10-83
No mem for dav xx int ETH yyy	13-40

Alarm Index

Alarm	Page
NO MEMORY - TFTP UPLOAD TO SCRIPT FAILED	10-83
No memory for (type) table	7-16
No memory for Access Control Cache	7-16
No memory for outbound interfaces list of Access control filter	7-16
No memory for outbound LCONs list of Access control filter: Attempt to add duplicate record	7-16
No memory for TABLE (x) record	7-17
NO PROFILE AVAILABLE FOR (name)	10-2
No QoS features configured	9-147
NO ROOM IN FACILITY FOR DCP	10-83
NO STATION FOR SMDS DESTINATION	3-12
No zone for seed routing port	2-11
NODE BOOT COMPLETE	10-83
NODE BOOT CONTINUING - LAST CMEM CHANGE MAY BE LOST	11-3
NODE BOOT DELAYED DUE TO LAST GASP PROCESSING	11-3
Node boot required. The number of MNEM table entries in CMEM does not match the active number.	10-84
Node boot required. The number of PVC table entries in CMEM does not match the active number.	10-84
Node boot required. The number of ROUT table entries in CMEM does not match the active number.	10-84
NODE COLDSTARTED	10-84
NODE KEY CHANGED	10-85
NODE KEY NOT CONFIGURED	10-85
NODE RECORD BOOT FAILED, (cause)	10-85
NODE RESET DUE TO CRASH	10-85
NODE RESET DUE TO DEBUGGER COMMAND	10-85
NODE RESET DUE TO POWER-UP OR RESET SWITCH	7-17
NODE RESET DUE TO WATCHDOG TIMER TIMEOUT	10-85
NODE RESET WITH DEFAULT PASSWORD	10-86
NODE WARMSTARTED	10-86
Not Enough Dynamic Memory - <err_msg>	13-41
NOT ENOUGH MEMORY	7-17
Not enough memory - (err_msg)	10-86
Not Enough memory - (msg)	8-6
Not Enough memory - (msg)	9-72
Not Enough Memory for BGP Community Attributes	13-40
Not enough memory for CRL	10-145
Not Enough Permanent Memory for BGP->RIPv2 Route Import	13-40
Not used.	9-42
NS RUN TIME ERROR- NO FEATURES	10-86
NS RUN-TIME ERROR - CHANNEL OR FEATURE REGISTERED TWICE	4-10
NS RUN-TIME ERROR - DATA STRUCTURE IN ERROR	10-86
NS RUN-TIME ERROR - NO AVAILABLE NS CHANNELS	4-10
NS RUN-TIME ERROR - NO FEATURES	7-17
NS RUN-TIME PARAMETER ERROR	10-86

Alarm	Page
NULL REPORT	10-86
OSPF -> %s	9-19
OSPF -> Configuration Error - %s	9-20
OSPF -> Not Enough Dynamic Memory - %s	9-19
OSPF -> Not Enough Permanent memory - %s	9-19
OSPF -> Route to %s / %d imported from BGP into OSPF Routing Domain	9-20
OSPF -> Route to %s / %d is Not Imported into OSPF due to 'Deny' Policy No. %d	9-20
OSPF -> Route to %s / %d matched to BGP-OSPF Import 'Permit' Policy No. %d	9-20
OSPF -> Route to %s / %d withdrawn by BGP from OSPF Routing Domain	9-20
OSPF.001, Bad length pkt, from (source), type (N)	9-3
OSPF.002, Bad pkt checksum, from (source), type (N)	9-3
OSPF.003, OSPF version, from (source), type (N)	9-3
OSPF.004, Duplicate Router ID, from (source), type (N)	9-4
OSPF.005, No matching ifc for pkt from (source), type (N)	9-4
OSPF.006, Authentication failure, from (source), type (N)	9-4
OSPF.007, No matching nbr for pkt from (source), type (N)	9-5
OSPF.008, Bad pkt type from (source), type (N)	9-5
OSPF.009, No buffer for mcast to (dest)	9-5
OSPF.010, LPTRACE, Received packet type (N) from (source)	9-5
OSPF.011, Sending unicast type (N) dst (dest)	9-5
OSPF.012, Sending mcast type (N), dst (dest), net (net_id)	9-6
OSPF.013, Rxmitting type (N), (source) -> (dest)	9-6
OSPF.014, No FSM match, ifc (i/f) state (state), event (e)	9-7
OSPF.015, State change, ifc (i/f), new state (state) event (e)	9-8
OSPF.016, No match for hlo (virtual link) from (source)	9-8
OSPF.017, Network mask mismatch with (source)	9-9
OSPF.018, Hello interval mismatch with (source)	9-9
OSPF.019, Dead interval mismatch with (source)	9-9
OSPF.020, No FSM match, nbr (add), state (state), event (event)	9-10
OSPF.021, State change, nbr (add), new state (state), event (event)	9-11
OSPF.022, Outstanding DD pkt not avail for nbr (add)	9-12
OSPF.023, Unable to get pkt, to (dest), ifc (i/f)	9-12
OSPF.024, Bad length LS adv from (add)	9-12
OSPF.025, from (add), adv. cksum fl:(t), (dest), (orig)	9-12
OSPF.026, from (add), bad type, adv: (type) (id)	9-12
OSPF.027, from (add), old adv: (type) (id)	9-13
OSPF.028, LUINFO, from (add), old adv: (type), (id)	9-13
OSPF.029, from (add), self update: (type), (id)	9-13
OSPF.030, from (add), new adv: (type), (id)	9-13
OSPF.031, from (add), Old ack for adv: (type), (id)	9-14
OSPF.032, Bad ack from (add) for adv: (type), (id)	9-14
OSPF.033, LS update retransmission to (add)	9-14

Alarm Index

Alarm	Page
OSPF.034, LS ack sent direct to (add)	9-14
OSPF.035, Flushing advertisement: (type), (id)	9-15
OSPF.036, Originating adv: (type), (id)	9-15
OSPF.037, new route to (dest), type (type), cost (cost)	9-15
OSPF.038, NBMA hello sent to dest (add)	9-15
OSPF.039, The OSPF routing protocol is (state)	9-15
OSPF.040, SPF Interface (add) is not an IP address, Interface not installed	9-16
OSPF.041, Non-Broadcast net (add) is not an SPF interface.	9-16
OSPF.042, protocol (disabled): (source) -> (dest), type (type) discarded	9-16
OSPF.043, Duplicate LS ack received from (add)	9-16
OSPF.044, from (add), bad age field, adv (type), (id)	9-17
OSPF.045, non-existent area (area), VL discarded	9-17
OSPF.046, No backbone configured, VL s discarded	9-17
OSPF.047, (dest) now unreachable	9-17
OSPF.048, AS ext adv limit exceeded; origination deferred	9-17
OSPF.050, from (add), Max Age: (type), (id)	9-18
OSPF.051, bad adv/ovflo: (type), (dest), (orig)	9-18
OSPF.052, Stub area mismatch with (source), recvd in stub area, adv	9-18
OSPF.053, from (source), recvd in stub area, adv	9-18
OSPF.054, Internal Programming error	9-19
OSPF.055, Memory allocation failed	9-19
OSPF.056, Timer allocation failed	9-19
OSPFM (n) - DISABLED, DUPLICATE SLOT ON SPFM (con)	9-21
OSPFM (n) - PVC CONNECTED (source) -> (dest)	9-21
OSPFM (n) - PVC CONNECTION FAILED ON (node)	9-20
Out of Memory	7-17
OUTER,ETH PORT,TKR PORT subsystems SRAM related high priority traps	10-87
OUTER,ETH PORT,TKR PORT subsystems SRAM related low priority traps	10-87
OUTER,ETH PORT,TKR PORT subsystems SRAM related medium priority traps	10-87
OUTGOING CALL TO %s ON DSL %d	11-4
OUTGOING CALL TO (call) ON DSL (line)	7-26
Packet is Decrypted on tunnel# (n) with src (x.x.x.x) dst (y.y.y.y)	12-6
Packet is Encrypted on tunnel# (n) with src (x.x.x.x) dst (y.y.y.y)	12-6
PACKET LEVEL RESTART	10-87
Packet pointer is NULL. Can not process the call request	11-3
Packet pointer is NULL. Can not process the call request	10-143
PACKET REASSEMBLY FAILURE	14-8
PACKET REASSEMBLY FAILURE THRESHOLD REACHED	14-8
PACKET REASSEMBLY RESUMED	14-9
PACKET_REPT_SEC_RELEASE_HIGH_ALL [REPORT_HIGH, ÒHIGH PRESERVING DBUFFER INTEGRITY ADDR: 0x%08X 0x%08X 0x%08X 0x%08X 0x%08X]	10-144
PBR cache cleared	2-11

Alarm	Page
PBR cache overflow	2-11
PERMANENT LINKS MUST CONFIGURED AS A DEDICATED LINK IN A PROFILE	10-87
PHONE NUMBER BUSY	10-87
PIM.001, PIM.1: Debug string	9-156
PIM.003, PIM.3: No mem for structure_1 (in function_1)	9-156
PIM.004, PIM.4: CRP ip address has no grp.	9-156
PIM.005, PIM.5: Static RP ip address has no grp	9-156
PIM.006, PIM.6: Inconsistent RP for ip address (us: ip address nbr ip address 's ip address)	9-157
PIM.007, PIM.7: Reg not sent for (IP address, IP Address), hit limit	9-157
PIM.008, PIM.8: Recv type msg from non-nbr ip address	9-157
PIM.009, PIM.9: Reject type msg from ip address. (c:error reason val:value)	9-157
PIM.011, PIM.11: Recv Reg for ip address from ip address, but RP is ip address	9-158
PIM.012, PIM.12: Recv CRP msg on ip address from ip address, but BSR is ip address	9-158
PIM.013, PIM.13: Max Route Hit, (source ip address, group ip address) not created	9-158
PIM.014, PIM.14: Recv pim msg on non-pim if ip address	9-158
ping_entry_deleted	9-121
ping_trans_	
port %d	11-17
PORT (n) (i/o) PORT UTILIZATION > THRESHOLD	2-11
PORT (n) - %s	11-16
PORT (n) - %s: CLEARED	11-16
PORT (n) - ACCESS PORT DOWN	2-11
PORT (n) - ACCESS PORT DOWN	2-12
PORT (n) - ACCESS PORT DOWN	2-12
PORT (n) - ACCESS PORT UP	2-12
PORT (n) - ACCESS PORT UP	2-12
PORT (n) - ACCESS PORT UP	2-12
PORT (n) - ALLOCATED (x) BYTES FOR PPP TRACING	2-13
PORT (n) - AUTOCALL RETRIES EXHAUSTED, REBOOT THE PORT	2-13
PORT (n) - BAD CCC RECEIVED	10-88
PORT (n) - BAD FRAME TYPE (x)	2-13
PORT (n) - BAD FRAME TYPE (x)	2-13
PORT (n) - BAD FRAME TYPE (x)	2-14
PORT (n) - BAD N(R) (n)	2-14
PORT (n) - BAD N(R) (sn)	2-14
PORT (n) - BAD N(R) (sn)	2-14
PORT (n) - BAD P(K)	2-14
PORT (n) - BAD PID IN CALL FROM (remote address)	2-15
PORT (n) - BAD TID IN CALL FROM (remote address)	2-15
PORT (n) - BOOT TO NEW PORT FAILURE, PORT DOES NOT SUPPORT DYNAMIC CREATE	2-15
PORT (n) - BROADCAST OVERRUN	2-15
PORT (n) - CALL CLEARED BY HOST (cause)	2-16

Alarm Index

Alarm	Page
PORT (n) - CALL CLEARED BY NETWORK, CAUSE CODE (x)	2-16
PORT (n) - CALL CLEARED BY REMOTE TNPP PAD	2-16
PORT (n) - CALL REJECTED BY LEVEL3 (cause)	2-16
PORT (n) - CALL REJECTED BY LEVEL3 - (cause)	2-17
PORT (n) - COMMAND SYNTAX ERROR	2-17
PORT (n) - CONNECTED TO HOST	2-17
PORT (n) - CONNECTION TOWARDS HOST IN PROGRESS	2-17
PORT (n) - CONTROL FIELD EMPTY CALL REJECTED	2-18
PORT (n) - CONTROL FRAME FROM HOST, CALL CLEARED	2-18
PORT (n) - CONTROLLER DOWN (device)	2-18
PORT (n) - CONTROLLER OPERATIONAL (device)	2-18
PORT (n) - CONNECTION TOWARDS REMOTE TNPP PAD IN PROGRESS	2-19
PORT (n) - DLE-EOT TIMEOUT, CALL CLEARED	2-19
PORT (n) - DEBUG TRACE IS ON	2-19
PORT (n) - DEVICE UNAVAILABLE (device) DATA LOSS	2-19
PORT (n) - DIAL OUT NOT SUPPORTED, CALL REJECTED	2-19
PORT (n) - DISCONNECTED DUE TO LINE ERRORS	2-20
PORT (n) - DLE EOT RECEIVED CALL CLEARED	2-20
PORT (n) - DYNAMIC PORT BEING CREATED	2-20
PORT (n) - DYNAMIC PORT COMPLETED	2-20
PORT (n) - DYNAMIC PORT STARTED	2-21
PORT (n) - END-TO-END PACKET RELEASED - RX ERROR ORDER	2-21
PORT (n) - ERROR COUNT > THRESHOLD	11-7
PORT (n) - ERROR COUNT > THRESHOLD	11-7
PORT (n) - ERROR COUNT > THRESHOLD	11-8
PORT (n) - ERROR COUNT > THRESHOLD	11-14
PORT (n) - ERROR COUNT > THRESHOLD	11-14
PORT (n) - Failed to register with ISDN Management Entity	11-16
PORT (n) - FAILURE PORT DOES NOT EXIST	2-21
PORT (n) - FAILURE PORT DOES NOT EXIST	2-21
PORT (n) - FAT TIMER EXPIRED, LINE DISCONNECTING	2-22
PORT (n) - FRAME RECEIVED FROM UNKNOWN DLCI: (dddd)	2-22
PORT (n) - FRAMER HW NOT SUPPORTED	11-16
PORT (n) - FRMR (XX/XX/XX)	2-22
PORT (n) - FRMR (XX/XX/XX)	2-22
PORT (n) - FRMR (XX/XX/XX)	2-23
PORT (n) - FRMR (XX/XX/XX/XX/XX)	2-23
PORT (n) - FRMR (XX/XX/XX/XX/XX)	2-23
PORT (n) - FRMR (XX/XX/XX/XX/XX)	2-23
PORT (n) - HOST FRAME SIZE EXCEEDED, CALL CLEARED	2-24
PORT (n) - HP ENQ/ACK TIMEOUT	2-24
PORT (n) - I.430 DIM INSTALLED ON INVALID PORT	2-24

Alarm	Page
PORT (n) - INVITATION TO CLEAR FROM HOST, CALL CLEARED	2-24
PORT (n) - INITIALIZATION FAILED	2-25
PORT (n) - INITIALIZATION FAILED, SOFTWARE BUG DETECTED in (code) at line (line)	2-25
PORT (n) - INPUT BUFFER OVERRUN	2-25
PORT (n) - INPUT QUEUE OVERRUN	2-25
PORT (n) - INSUFFICIENT DYNAMIC MEMORY, PORT DOWN GRADED TO NULL PORT	2-25
PORT (n) - INSUFFICIENT DYNAMIC MEMORY, PORT DOWN GRADED TO NULL PORT	2-26
PORT (n) - INVALID CONTROL FIELD, CALL REJECTED	2-26
PORT (n) - INVALID FRAME FROM POS, CALL CLEARED	2-26
PORT (n) - INVALID MSS FROM HOST, CALL CLEARED	2-27
PORT (n) - INVALID MSS FROM POS, CALL REJECTED	2-27
PORT (n) - LINE DOWN	2-27
PORT (n) - LINE DOWN	2-27
PORT (n) - LINE FAILURE, LINE DISCONNECTED	2-28
PORT (n) - LINE OPERATIONAL	2-28
PORT (n) - LINK BLOCKED	2-28
PORT (n) - LINK BLOCKED	2-28
PORT (n) - LINK BLOCKED	2-28
PORT (n) - LINK UP	2-28
PORT (n) - LINK UP	2-29
PORT (n) - LINK UP	2-29
PORT (n) - LIST IS EMPTY	2-29
PORT (n) - LIST IS NOT EMPTY	2-29
PORT (n) - MNEMONIC IS EITHERBLANK OR NOT CONFIGURED - (cause)	2-30
PORT (n) - NO COMMANDS	2-30
PORT (n) - NO RESPONSE	2-30
PORT (n) - NON-RECOVERABLE INBOUND ERROR	2-30
PORT (n) - NON-RECOVERABLE INBOUND ERROR	2-31
PORT (n) - NON-RECOVERABLE OUTBOUND ERROR	2-31
PORT (n) - NON-RECOVERABLE OUTBOUND ERROR	2-31
PORT (n) - NOT AUTHORIZED TO USE POLLED ASYNC OPTION	2-31
PORT (n) - OUTBOUND LINK BLOCKED	2-31
PORT (n) - OUTBOUND LINK UNBLOCKED	2-32
PORT (n) - OUTPUT BUFFER OVERRUN	2-32
PORT (n) - OUTPUT QUEUE OVERRUN	2-32
PORT (n) - OVERSIZE FRAME (s) FROM REMOTE LINK	2-32
PORT (n) - OVERSIZE FRAME (s) FROM REMOTE LINK	2-32
PORT (n) - OVERSIZE FRAME (s) FROM REMOTE LINK	2-33
PORT (n) - PACKET LEVEL RESTART	2-33
PORT (n) - PORTSTATUS WARNING - (cause)	2-33
PORT (n) - PORT ALREADY DISABLE	2-33
PORT (n) - PORT ALREADY ENABLE	2-33

Alarm Index

Alarm	Page
PORT (n) - PORT BOOT COMPLETE	11-15
PORT (n) - PORT BOOT COMPLETE	11-18
PORT (n) - PORT BOOT COMPLETED	2-34
PORT (n) - PORT BOOT COMPLETE	2-34
PORT (n) - PORT BOOT COMPLETE	2-34
PORT (n) - PORT BOOT COMPLETE	2-34
PORT (n) - PORT BOOT COMPLETE	2-34
PORT (n) - PORT BOOT COMPLETE	2-34
PORT (n) - PORT BOOT COMPLETE	2-35
PORT (n) - PORT BOOT COMPLETE	2-35
PORT (n) - PORT BOOT COMPLETE	2-35
PORT (n) - PORT BOOT COMPLETE	2-35
PORT (n) - PORT BOOT COMPLETE	2-35
PORT (n) - PORT BOOT COMPLETE	2-35
PORT (n) - PORT BOOT COMPLETE	2-36
PORT (n) - PORT BOOT COMPLETE	2-36
PORT (n) - PORT BOOT COMPLETE	2-36
PORT (n) - PORT BOOT COMPLETE	2-36
PORT (n) - PORT BOOT COMPLETE	2-36
PORT (n) - PORT BOOT COMPLETE	2-36
PORT (n) - PORT BOOT COMPLETE	2-36
PORT (n) - PORT BOOT COMPLETE	2-37
PORT (n) - PORT BOOT COMPLETE	2-37
PORT (n) - PORT BOOT COMPLETE	2-37
PORT (n) - PORT BOOT COMPLETE	2-37
PORT (n) - PORT BOOT COMPLETE	2-37
PORT (n) - PORT BOOT COMPLETE	2-37
PORT (n) - PORT BOOT COMPLETE	2-37
PORT (n) - PORT BOOT COMPLETE	2-38
PORT (n) - PORT BOOT FAILED	2-38
PORT (n) - PORT BOOT FAILED, CAUSE: (cause)	2-38
PORT (n) - PORT BOOT FAILURE	2-39
PORT (n) - PORT BOOT FAILURE	2-39
PORT (n) - PORT BOOT FAILURE	2-39
PORT (n) - PORT BOOT FAILURE	2-39
PORT (n) - PORT BOOT FAILURE	2-40
PORT (n) - PORT BOOT FAILURE (cause)	2-40
PORT (n) - PORT BOOT FAILURE (cause)	2-40
PORT (n) - PORT BOOT FAILURE (cause)	2-41
PORT (n) - PORT BOOT FAILURE (cause)	2-41
PORT (n) - PORT BOOT FAILURE - (cause)	2-41
PORT (n) - PORT BOOT FAILURE - (cause)	2-42

Alarm	Page
PORT (n) - PORT BOOT FAILURE - (cause)	2-43
PORT (n) - PORT BOOT FAILURE - (cause)	2-43
PORT (n) - PORT BOOT FAILURE - (cause)	2-44
PORT (n) - PORT BOOT FAILURE - (cause)	2-45
PORT (n) - PORT BOOT FAILURE - (cause)	2-45
PORT (n) - PORT BOOT FAILURE - (cause)	2-46
PORT (n) - PORT BOOT FAILURE - (cause)	2-46
PORT (n) - PORT BOOT FAILURE - (cause)	2-46
PORT (n) - PORT BOOT FAILURE - (cause)	2-46
PORT (n) - PORT BOOT FAILURE - (cause)	2-47
PORT (n) - PORT BOOT FAILURE - (cause)	2-47
PORT (n) - PORT BOOT FAILURE - (cause)	2-47
PORT (n) - PORT BOOT FAILURE - (cause)	2-48
PORT (n) - PORT BOOT FAILURE - (cause)	2-48
PORT (n) - PORT BOOT FAILURE - (cause)	11-15
PORT (n) - PORT BOOT FAILURE - (cause)	11-18
PORT (n) - PORT BOOT FAILURE - (explanation)	2-48
PORT (n) - PORT BUSY OUT	2-48
PORT (n) - PORT BUSY-OUT	2-49
PORT (n) - PORT BUSY-OUT	2-49
PORT (n) - PORT BUSY-OUT	2-49
PORT (n) - PORT BUSY-OUT COMPLETE	2-49
PORT (n) - PORT BUSY-OUT FAILURE (cause)	2-49
PORT (n) - PORT BUSY-OUT FAILED	2-49
PORT (n) - PORT CONNECTION CLEARED	2-50
PORT (n) - PORT CONNECTION CLEARED	2-50
PORT (n) - PORT DISABLE FAILURE (cause)	2-50
PORT (n) - PORT DISABLE FAILURE - (cause)	2-50
PORT (n) - PORT DISABLE FAILED	2-50
PORT (n) - PORT DISABLE FAILURE	2-51
PORT (n) - PORT DISABLE FAILURE	2-51
PORT (n) - PORT DISABLE FAILURE	2-51
PORT (n) - PORT DISABLE FAILURE	2-51
PORT (n) - PORT DISABLE FAILURE	2-51
PORT (n) - PORT DISABLE FAILURE	2-52
PORT (n) - PORT DISABLED	2-52
PORT (n) - PORT DISABLED	2-52
PORT (n) - PORT DISABLED	2-52
PORT (n) - PORT DISABLED	2-52
PORT (n) - PORT DISABLED	2-52
PORT (n) - PORT DISABLED	2-53
PORT (n) - PORT DISABLED	2-53

Alarm Index

Alarm	Page
PORT (n) - PORT DISABLED	2-53
PORT (n) - PORT DISABLED	2-53
PORT (n) - PORT DISABLED	2-53
PORT (n) - PORT DISABLED	2-53
PORT (n) - PORT DISABLED	2-54
PORT (n) - PORT DISABLED	2-54
PORT (n) - PORT DISABLED	2-54
PORT (n) - PORT DISABLED	2-54
PORT (n) - PORT DISABLED	2-54
PORT (n) - PORT DISABLED	2-54
PORT (n) - PORT DISABLED	2-54
PORT (n) - PORT DISABLED	2-55
PORT (n) - PORT DISABLED	2-55
PORT (n) - PORT DISABLED	2-55
PORT (n) - PORT DISABLED	2-55
PORT (n) - PORT DISABLED	2-55
PORT (n) - PORT DISABLED	11-15
PORT (n) - PORT DISABLED	11-18
PORT (n) - PORT ENABLE FAILED	2-55
PORT (n) - PORT ENABLE FAILED	2-55
PORT (n) - PORT ENABLE FAILED	2-56
PORT (n) - PORT ENABLE FAILED	2-56
PORT (n) - PORT ENABLE FAILED	2-56
PORT (n) - PORT ENABLE FAILED - ALREADY ENABLED	2-56
PORT (n) - PORT ENABLE FAILED - ALREADY ENABLED	2-56
PORT (n) - PORT ENABLE FAILURE	2-56
PORT (n) - PORT ENABLE FAILURE	2-57
PORT (n) - PORT ENABLE FAILURE	2-57
PORT (n) - PORT ENABLE FAILURE	2-57
PORT (n) - PORT ENABLE FAILURE	2-57
PORT (n) - PORT ENABLE FAILURE	2-57
PORT (n) - PORT ENABLE FAILURE (cause)	2-57
PORT (n) - PORT ENABLE FAILURE (cause)	2-58
PORT (n) - PORT ENABLE FAILURE - (cause)	2-58
PORT (n) - PORT ENABLED	2-58
PORT (n) - PORT ENABLED	2-58
PORT (n) - PORT ENABLED	2-58
PORT (n) - PORT ENABLED	2-58
PORT (n) - PORT ENABLED	2-58
PORT (n) - PORT ENABLED	2-59
PORT (n) - PORT ENABLED	2-59
PORT (n) - PORT ENABLED	2-59

Alarm	Page
PORT (n) - PORT ENABLED	2-59
PORT (n) - PORT ENABLED	2-59
PORT (n) - PORT ENABLED	2-59
PORT (n) - PORT ENABLED	2-59
PORT (n) - PORT ENABLED	2-60
PORT (n) - PORT ENABLED	2-60
PORT (n) - PORT ENABLED	2-60
PORT (n) - PORT ENABLED	2-60
PORT (n) - PORT ENABLED	2-60
PORT (n) - PORT ENABLED	2-60
PORT (n) - PORT ENABLED	2-60
PORT (n) - PORT ENABLED	2-61
PORT (n) - PORT ENABLED	2-61
PORT (n) - PORT ENABLED	2-61
PORT (n) - PORT ENABLED	2-61
PORT (n) - PORT ENABLED	2-61
PORT (n) - PORT ENABLED	2-61
PORT (n) - PORT ENABLED	2-61
PORT (n) - PORT ENABLED	2-62
PORT (n) - PORT ENABLED	10-88
PORT (n) - PORT ENABLED	11-15
PORT (n) - PORT ENABLED	11-18
PORT (n) - PORT ERROR COUNT > THRESHOLD	2-62
PORT (n) - PORT ERROR COUNT > THRESHOLD	2-62
PORT (n) - PORT ERROR COUNT > THRESHOLD	2-62
PORT (n) - PORT ERROR COUNT > THRESHOLD	2-62
PORT (n) - PORT ERROR COUNT > THRESHOLD	2-63
PORT (n) - PORT ERROR COUNT > THRESHOLD	2-63
PORT (n) - PORT ERROR COUNT > THRESHOLD	2-63
PORT (n) - PORT ERROR COUNT > THRESHOLD	2-64
PORT (n) - PORT ERROR COUNT > THRESHOLD	2-64
PORT (n) - PORT ERROR COUNT > THRESHOLD	2-64
PORT (n) - PORT ERROR COUNT > THRESHOLD	2-65
PORT (n) - PORT INIT FAILURE - (cause)	11-16
PORT (n) - PORT INIT FAILURE - (cause)	11-18
PORT (n) - PORT INIT FAILURE - (cause)	2-66
PORT (n) - PORT INIT FAILURE, CAUSE: (cause)	2-66
PORT (n) - PORT LOST COMMUNICATION WITH DRIVER	11-16
PORT (n) - PORT NOT STARTED - (cause)	2-67
PORT (n) - PORT STAT OVERFLow	2-67
PORT (n) - PORT STAT OVERFLow	2-67
PORT (n) - PORT STATUS WARNING - PORT DISABLED	2-67

Alarm Index

Alarm	Page
PORT (n) - PORT STATUS WARNING - (cause)	2-67
PORT (n) - PORT STATUS WARNING - (cause)	2-68
PORT (n) - PORT STATUS WARNING - PORT DISABLED	2-68
PORT (n) - PORT STATUS WARNING, PORT DISABLED	2-68
PORT (n) - PORT STATUS WARNING (cause)	2-68
PORT (n) - PORT STATUS WARNING (cause)	2-68
PORT (n) - PORT STATUS WARNING - (cause)	2-68
PORT (n) - PORT STATUS WARNING - (cause)	2-69
PORT (n) - PORT STATUS WARNING - (cause)	2-69
PORT (n) - PORT STATUS WARNING - PORT DISABLED	2-69
PORT (n) - PORT STATUS WARNING -(cause)	2-69
PORT (n) - PORT STATUS WARNING	2-69
PORT (n) - PORT STATUS WARNING	2-70
PORT (n) - PORT STATUS WARNING	2-70
PORT (n) - PORT STATUS WARNING	2-70
PORT (n) - PORT STATUS WARNING	2-70
PORT (n) - PORT STATUS WARNING	2-70
PORT (n) - PORT STATUS WARNING	2-70
PORT (n) - PORT UTILIZATION > THRESHOLD	2-71
PORT (n) - PORT UTILIZATION > THRESHOLD	2-71
PORT (n) - PORT UTILIZATION > THRESHOLD	2-71
PORT (n) - PORT UTILIZATION > THRESHOLD	2-71
PORT (n) - PORT UTILIZATION > THRESHOLD	2-71
PORT (n) - PORT UTILIZATION > THRESHOLD	2-72
PORT (n) - PORT UTILIZATION > THRESHOLD	2-72
PORT (n) - PORT UTILIZATION > THRESHOLD	2-72
PORT (n) - PORT UTILIZATION > THRESHOLD	2-72
PORT (n) - PORT UTILIZATION > THRESHOLD	2-72
PORT (n) - PORT UTILIZATION > THRESHOLD	2-73
PORT (n) - PORT UTILIZATION > THRESHOLD	2-73
PORT (n) - PORT UTILIZATION > THRESHOLD	2-73
PORT (n) - PORT UTILIZATION > THRESHOLD	2-73
PORT (n) - PORT UTILIZATION > THRESHOLD	2-73
PORT (n) - PORT UTILIZATION > THRESHOLD	2-74
PORT (n) - PORT UTILIZATION > THRESHOLD	2-74
PORT (n) - PORT UTILIZATION > THRESHOLD	2-74
PORT (n) - REJECTING X25 CALL, ALREADY CONNECTED	2-74
PORT (n) - REMOTE DEVICE IS DOWN	2-74
PORT (n) - REMOTE DEVICE IS UP	2-74
PORT (n) - REMOTE PAD IS NOT TNPP PAD, CLEARING CALL	2-75
PORT (n) - RETRY EXCEEDED, CALL CLEARED	2-75
PORT (n) - RETRY EXCEEDED, LINE DISCONNECTED	2-75

Alarm	Page
PORT (n) - RING NUMBER CONFIGURATION ERROR	2-75
PORT (n) - TERM (ID) STPA FRAME DROPPED	2-76
PORT (n) - THRESHOLD EXCEEDED %s is one of "LES" or "LCV" or "PCV" or "CSS" or "ES" or "BES" or "SES" or "SEFS" or "UAS"	11-16
PORT (n) - UNSUPPORTED FRAME SIZE: OPERATING WITH 1024 BYTES	2-76
PORT (n) - VIRTUAL CALL RETRY EXCEEDED, LINE DISCONNECTED	2-76
PORT (n) - VIRTUAL RETRY EXCEEDED, CALL CLEARED	2-77
PORT (n) - X.28 SERVICE MESSAGE LOST	2-77
PORT (n) - X25 CONNECTION IS UP	2-77
PORT (n) BOOT FAILURE - (cause)	2-77
PORT (n) CPU - HA Communications Failure (condition)	2-78
PORT (n) DATA LOST FROM COMMAND QUEUE	2-78
PORT (n) DATA LOST FROM DATA QUEUE	2-79
PORT (n) FRAME RECEIVED FROM UNKNOWN DLCI: (n)	2-79
PORT (n) FRAME RECEIVED INVALID ADDRESS (dddd)	2-79
PORT (n) FRAME RECEIVED INVALID ADDRESS (dddd)	2-80
PORT (n) HA Warning:	2-80
PORT (n) LINE DOWN	2-80
PORT (n) LINE UP	2-80
PORT (n) LINK DOWN	2-80
PORT (n) LINK DOWN	2-81
PORT (n) LINK UP	2-81
PORT (n) LINK UP	2-81
PORT (n) OUT OF MEMORY - SOME STATIONS NOT CREATED	7-17
PORT (n) PORT BOOT COMPLETE	2-81
PORT (n) PORT BOOT COMPLETE	2-81
PORT (n) PORT BOOT COMPLETE	2-81
PORT (n) PORT BOOT COMPLETE	2-82
PORT (n) PORT BOOT COMPLETE	2-82
PORT (n) PORT BOOT COMPLETE	2-82
PORT (n) PORT BOOT COMPLETE	2-82
PORT (n) PORT BOOT FAILURE (cause)	2-82
PORT (n) PORT BOOT FAILURE (cause)	2-83
PORT (n) PORT BOOT FAILURE (cause)	2-83
PORT (n) PORT BOOT FAILURE - (cause)	2-84
PORT (n) PORT DISABLE COMPLETE	2-84
PORT (n) PORT DISABLE COMPLETE	2-84
PORT (n) PORT DISABLE FAILURE (cause)	2-84
PORT (n) PORT DISABLED	2-84
PORT (n) PORT DISABLED	2-84
PORT (n) PORT DISABLED	2-85
PORT (n) PORT DISABLED	2-85

Alarm Index

Alarm	Page
PORT (n) PORT DISABLED	2-85
PORT (n) PORT DISABLED	2-85
PORT (n) PORT DISABLED	2-85
PORT (n) PORT ENABLED	2-85
PORT (n) PORT ENABLED	2-85
PORT (n) PORT ENABLED	2-86
PORT (n) PORT ENABLED	2-86
PORT (n) PORT ENABLED COMPLETE	2-86
PORT (n) PORT ENABLED COMPLETE	2-86
PORT (n) PORT ERROR COUNT > THRESHOLD	2-86
PORT (n) PORT ERROR COUNT > THRESHOLD	2-86
PORT (n) PORT INITIALIZATION FAILED - (cause)	2-87
PORT (n) PORT INITIALIZATION FAILURE (cause)	2-87
PORT (n) PORT INITIALIZATION FAILURE (cause)	2-87
PORT (n) PORT STATUS WARNING (cause)	2-87
PORT (n) PORT STATUS WARNING - (cause)	2-87
PORT (n) PORT STATUS WARNING, LIMIT EXCEEDED PAGING TERMINAL IS IDENTIFIED AS (t)	2-88
PORT (n) PORT UTILIZATION > THRESHOLD	2-88
PORT (n) PORT UTILIZATION > THRESHOLD	2-88
PORT (n) PROTOCOL ERROR THRESHOLD REACHED (protocol)	2-89
PORT (n) RETRIES (r) VIOLATIONS, NO ACTION	2-89
PORT (n) RETRIES (r) VIOLATIONS, PORT DEGRADED	2-89
PORT (n) RETRIES (r) VIOLATIONS, PORT DISCONNECTED	2-90
PORT (n) RETRIES (r) VIOLATIONS, PORT LOCKED	2-90
PORT (n) Station (s) STATION COMPLETE	2-91
PORT (n) Station (s) STATION Created	2-91
PORT (n) Station (s) STATION STARTED	2-91
PORT (n) SW56K CALL FAILED - NO PHONE NUMBER	2-91
PORT (n) SW56K CALL TO (n) FAILED	2-91
PORT (n) SW56K CALLING (n)	2-92
PORT (n) SW56K CONNECTED TO (n)	2-92
PORT (n) SW56K IN CHANNEL LOOPBACK	2-92
PORT (n) SW56K IN DSU LOOPBACK	2-92
PORT (n) SW56K INCOMING CALL ANSWERED	2-92
PORT (n) SW56K INCOMING CALL IGNORED	2-92
PORT (n) UNSUPPORTED DATABITS: OPERATING WITH 8 DATABITS, NO PARITY	2-92
PORT (n) UNSUPPORTED PARITY: OPERATING WITH 8 DATABITS, NO PARITY	2-93
PORT (n) UNSUPPORTED BAUDRATE: OPERATING AT 9600 BPS	2-93
PORT (n) UNSUPPORTED DATABITS: OPERATING WITH 8 DATABITS, NO PARITY	2-93
PORT (n) UNSUPPORTED FRAME SIZE: OPERATING WITH 1024 BYTES	2-93
PORT (n) UNSUPPORTED PARITY: OPERATING WITH 8 DATABITS, NO PARITY	2-93
PORT (n) UNSUPPORTED BAUDRATE: OPERATING AT 9600 BPS	2-94

Alarm	Page
PORT (n) VIRTUAL MAPPING ERROR, CAUSE: (cause)	2-94
PORT (n), FRAME DISCARDED - (cause), (SA) - (DA)	2-95
PORT (n), LINK DOWN - (cause), (xx) DATA FRAMES LOST	2-96
PORT (n), LINK UP	2-96
PORT (n), PROTOCOL ERROR	2-96
PORT - %d	11-6
PORT - DYNAMIC PORT BEING CREATED	2-97
PORT - DYNAMIC PORT COMPLETED	2-97
PORT - DYNAMIC PORT STARTED	2-98
PORT BOOT COMPLETE	2-98
PORT DISABLED	2-98
PORT ENABLED	2-98
PORT FAILURE	2-98
PORT FAILURE, CAUSE: MISSING BATTERY	2-99
PORT FAILURE, CAUSE: MISSING RINGER SUPPLY	2-99
PORT STATUS WARNING - (cause)	2-99
PORT UTILIZATION > THRESHOLD	2-99
PORT UTILIZATION > THRESHOLD	2-99
Port/Station identifier - FAILED TO MAKE STACK CONNECTION	14-9
PORT_BOOT:SWITCHED TO Low BANDWIDTH	2-99
PORT_DISABLE:SWITCHED TO Low BANDWIDTH	2-100
POSSIBLE DATA LOSS	10-88
POSSIBLE DATA LOSS	10-88
POSSIBLE RACE CONDITION IN SWITCH SERVICES - LINK ACTIVATE TIMER EXPIRED for %s	11-4
POSSIBLE RACE CONDITION IN SWITCH SERVICES - LINK ACTIVATE TIMER EXPIRED FOR %s	10-142
POWER SUPPLY (n) DOWN	7-18
POWER SUPPLY (n) UP	7-18
PPP - port number, PACKET RECEIVED FROM PEER WITH INVALID ENCAPSULATION	14-9
PPP - port number, PPPoE AC SYSTEM ERROR - optional string	14-11
PPP - port number, PPPoE Configuration Error	14-12
PPP - port number, PPPoE DISCOVERY FAILED - NO PADS FROM AC_Name	14-10
PPP - port number, PPPoE DISCOVERY FAILED- CONFIGURED PARAMETER Service-Name or AC-Name CAN NOT BE MATCHED.	14-10
PPP - port number, PPPoE GENERIC ERROR - explanation string	14-11
PPP - port number, PPPoE Initialization Failure	14-12
PPP - port number, PPPoE SERVICE NAME ERROR - optional string	14-11
PPP - port number, PPPoE session id, DISCOVERY STAGE COMPLETED	14-10
PPP - port number, PPPoE SESSION session id TERMINATED cause	14-9
Precedence Array Assignments = %d %d %d %d	10-88
PRESHARED KEY (xx) FOR IPSEC PROFILE (xx) DOES NOT EXIST	10-88
PRI-%d - %s CALL %s %s ON	10-89
PRI-%d - %s CALL %s %s ON PORT %d DISCONNECTED BY 65xx	2-100

Alarm Index

Alarm	Page
PRI-%d - %s CALL %s %s ON PORT %d DISCONNECTED BY NETWORK	2-100
PRI-%d - D CHANNEL ESTABLISHING	4-10
PRI-%d - D CHANNEL UP	4-10
PRI-%d - D CHANNEL DOWN	4-10
PRI-%d - D CHANNEL RESTARTED, ALL CALLS DROPPED	4-11
PRI-%d - INCOMING CALL TO %s FROM %s FAILED ON PORT %d, %s	2-101
PRI-%d - INCOMING CALL TO %s FROM %s FAILED ON PORT %d, %s	2-100
PRI-%d - OUTGOING CALL TO %s FROM %s FAILED ON PORT %d, %s	2-100
PRI-%dB%d - B CHANNEL DOWN	4-11
PRI-%dB%d - B CHANNEL UP	4-11
PRI-%dB%d - INCOMING CALL TO %s FROM %s CONNECTED ON PORT %d	10-89
PRI-%dB%d - INCOMING CALL TO %s FROM %s FAILED, %s	10-89
PRI-%dB%d - OUTGOING CALL TO %s CONNECTED ON PORT (n)	2-100
PRIORITY QUEUE BLOCKED	10-89
Process Msg: PID: (n) Event: (n) x25cause: (n) x25diag: (n) Stat	6-5
Process Msg: PID: (n) Event: (n) x25cause: (n) x25diag: (n) Stat	10-89
Protocol Priority Profile Entry %d in LCON-%d not found	10-89
Proxy %d Ignored. Has duplicated IP address or Mac Address	10-89
Proxy %d Ignored.IP interface not available	10-89
Proxy specifying interface %d Mac Address is deactivated	10-90
purge_queue %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	10-139
purge_queue %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	11-6
PVC DUPLICATED IN PVC TABLE	4-11
PVC NOT CONNECTED TO (des) - (cause)	4-12
QCL Prof #<num> ignored - Duplicate Record for <app_id>	9-151
QFRMR RECEIVED	10-90
QLLC BAD PACKET LENGTH (l)	10-90
QLLC ILLEGAL PKT DETECTED	10-90
QLLC PROTOCOL ERROR (x) (y)	10-90
qllc_packet %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	11-6
qllc_packet %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	10-138
QOS : INITIALIZATION FAILURE - NOT ENOUGH MEMORY	10-91
QOS : NOT OPERATIONAL AS CONFIGURED FOR (application) - (cause)	10-92
QOS : NOT OPERATIONAL AS CONFIGURED FOR (application) - (cause) (ContÕd)	10-93
QOS : TOTAL PERCENTAGE > 100 FOR (application) - NORMALIZED TO 100%	10-93
QOS : TOTAL PERCENTAGE < 100 FOR (application) - PERCENTAGE ASSIGNMENT FOR DEFAULT CLASS OF PROFILE (x) CHANGED TO (value)	10-93
QOS: DISABLED FOR (application) (cause)	10-95
QOS: DISABLED FOR (application) - (cause)	10-94
QOS: DISABLED FOR (application) - (cause)	10-97
QOS: DISABLED FOR (application) - (cause)	10-98
QOS: DISABLED FOR (application) - (cause) (ContÕd)	10-96

Alarm	Page
QOS: INITIALIZATION FAILURE - NOT ENOUGH MEMORY	7-18
QOS: INITIALIZATION FAILURE - NOT ENOUGH MEMORY	10-98
QOS: IP FLOW # (n) USED IN DS C'FIER & MARKER PROF # (n) IGNORED FOR (application)	10-98
QOS: IP FLOW # (n) USED IN IP C'FIER PROF # (n) IGNORED FOR (application)	10-99
QOS: IPX FLOW # (n) USED IN IPX C'FIER PROF # (n) IGNORED FOR (application)	10-99
Radius (Authentication, Authorization, Accounting) Timeout	14-6
Radius Client Boot Complete	14-6
Radius Client Boot Failure	14-6
Radius Failed	14-6
RE-ESTABLISHED IPSEC CONNECTION WITH aa.bb.cc.dd	10-18
RE-ESTABLISHED ISAKMP CONNECTION WITH aa.bb.cc.dd	10-18
Received a E_Disconnect from BRI_PORT	10-99
RECEIVED ENCR. NOTIFY MSG OR MALFORMED PACKET FROM aa.bb.cc.dd	10-18
RECEIVED INVALID CC TPDU	10-99
RECEIVED INVALID CR TPDU	10-99
RECEIVED INVALID TPDU HEADER LENGTH	10-100
RECEIVED INVALID TPDU TYPE	10-100
RECEIVED MULTILINK FRAME WITH INVALID FORMAT	10-100
RECEIVED NULL POINTER	10-100
RECEIVED NULL POINTER	10-100
RECEIVED OUTBOUND PACKET OF UNSUPPORTED PROTOCOL	10-100
RECEIVED UN-AUTHORIZED ISAKMP REQUEST FROM aa.bb.cc.dd	9-154
RECEIVED UNAUTHORIZED ISAKMP REQUEST FROM (aa.bb.cc.dd)	10-101
RECEIVED UNKNOWN PACKET TYPE INDICATOR	10-101
RECEIVED UNKNOWN PACKET TYPE INDICATOR	10-101
record : Attempt to add duplicate record	10-101
REMOTE CONNECTION ESTABLISHED	10-101
Remote IP Address Changed on LCON (n), new IP address (add)	8-2
REMOTE PEER (aa.bb.cc.dd) DID NOT RESPOND TO ISAKMP REQUEST	10-101
REMOTE PEER DOES NOT RESPOND TO ISAKMP REQUEST	9-153
REMOTE PPP IS SILENT	10-102
REPORT_HIGH, ÒCORRUPTED BUFFER DROPPED 0x%08X 0x%08X 0x%08X 0x%08X 0x%08X]	10-144
REQUIRED MODULE (name) (#) NOT FOUND	10-102
RESET FROM REMOTE ENCRYPTION PEER	10-102
rip udp port not avail	9-126
RIP.001 bd ver (ver) frm hst (source)	9-121
RIP.002 rq frm (source)	9-121
RIP.003 trc on tracing_file frm (source)	9-121
RIP.004 trc off frm (source)	9-121
RIP.005 rsp frm (source)	9-122
RIP.006 bd cmd (code) frm (source)	9-122
RIP.007 rsp frm off nt (source)	9-122

Alarm	Page
RIP.008 sbnt rt (dest)_network non-subnt intfc hst (hop_add)	9-122
RIP.009 dyn rt to (dest) frm (hop_add) dis	9-123
RIP.010 nt (dest) unrch via (hop_add), del	9-123
RIP.011 updt nt (dest) hps metric via (hop_add)	9-123
RIP.012 snd rqst (source)	9-124
RIP.013 snd brd to (dest) (count) (routes)	9-124
RIP.014 snd to (dest) (count) (routes)	9-124
RIP.015 cnt all pkt	9-124
RIP.016 snd pkt (dest)	9-125
RIP.017 err (code) sndng pkt nt (net)	9-125
RIP.018 nt rt to (dest) tmd out	9-125
RIP.019 nt rt to (dest) del	9-125
RIP.020 cannot allocate memory for transmission	9-125
RIPv2 is not running in this node	13-41
ROUT MAIN: Command: (event) from (n)	6-5
ROUT MAIN: Command: (event) from (n)	10-102
rout_main: Packet Semaphore Locked %s: Event: %s, Pck Addr: 0x%x	10-143
Route <net_prefix>/<prefix_len> is used to create aggregate route <net_prefix>/<prefix_len>	13-44
Route <net_prefix>/<prefix_len> is used to create aggregate route <net_prefix>/<prefix_len>, matching Profile entry %d	13-45
Route <net_prefix>/prefix_len> is not used to create aggregate route <net_prefix>/<prefix_len>	13-44
Route <net_prefix>/prefix_len> is not used to create aggregate route <net_prefix>/<prefix_len> due to <err_msg> even matching Profile entry %d.	13-45
Route not advertised to peer #xxx due to community #xxx	13-45
Route to <net_prefix>/<prefix_len> imported from BGP into OSPF Routing Table	13-2
Route to <net_prefix>/<prefix_len> withdrawn by BGP from OSPF Routing Table	13-2
Route to <net_prefix>/<prefix_len> withdrawn by BGP from RIPv2	13-42
ROUTER,ETH PORT,TKR PORT subsystems high priority traps	10-102
ROUTER,ETH PORT,TKR PORT subsystems low priority traps	10-102
ROUTER,ETH PORT,TKR PORT subsystems medium priority traps	10-102
rtn_msg: lg_refapp = 0x%x, refapp.S0 = 0x%x	10-103
RUIHC-Compressed Pkt CID # does not exist on LCON (n) Decompressor	6-6
RUIHC-Compressed pkt rcvd but comp typ is TRANSMIT on LCON (n)	6-6
RUIHC-Compression started, LCON (n), srcadd (n), dstadd (n), srcport (n), dstport (n), ssrc (n)	6-6
RUIHC-Compressor Ctxt Overflow, LCON (n)	6-7
RUIHC-Ctxt Ent in NegCache, LCON (n), srcadd (n), dstadd (n), srcport (n), dstport (n), ssrc (n)	6-7
RUIHC-Ctxt Ent Tmout, LCON (n), srcadd (n), dstadd (n), srcport (n), dstport (n), ssrc (n)	6-8
RUIHC-Ctxt St Packet Received, LCON (n)	6-8
RUIHC-Ctxt State packet CID (n)	6-8
RUIHC-Ctxt State Pkt CID size mismatch on LCON (n)	6-9
RUIHC-New CtxtEnt Added, LCON (n), srcadd (n), dstadd (n), srcport (n), dstport (n), ssrc (n)	6-9
RUIHC-No MEM to send Ctxt State packet on LCON (n)	6-9

Alarm	Page
RUIHC-NO Memory LCON (n)	6-10
Running software is %sSize- %d bytes	13-38
RX MESSAGE QUEUE OVERFLOW	10-103
RX_ISR : DEFAULT : CODRET	10-103
RX_ISR : DEFAULT-2 : CODRET	10-103
RX_ISR : P_CONNSDR : CODRET	10-103
RX_ISR : P_DISCSDR : CODRET	10-103
RX_ISR : P_SETUPSDR : CODRET	10-103
Scheduler not available	9-150
SDLC STATION (n) - INSUFFICIENT MEMORY TO PROTECT STATION	3-12
SDLC-(n) STATION (n) - BAD FRAME LENGTH (b)	3-13
SDLC-(n) STATION (n) - BAD FRAME TYPE (h)	3-13
SDLC-(n) STATION (n) - BAD N(R) (r)(e)	3-13
SDLC-(p) STATION (n) - FRMR (cc)(nn)(wxyz)	3-14
sdrvc_traitetbenrep(): loop timed out	10-104
sdrvr_disc(rtn_msg): returned	10-104
Select Condition: Chain: (n) PID: (n) TbleAddr: (n) SETUP: (n)	6-10
Select Condition: Chain: (n) PID: (n) TbleAddr: (n) SETUP: (n)	10-104
Select Destination: (n)	6-10
Select Destination: (n)	10-104
send_outbound %x	10-138
send_outbound %x	11-6
send_queued %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	10-139
send_queued %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	11-7
send_upstream %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	10-139
send_upstream %x upstream pending=%x count=%x downstream pending=%x count=%x queue_size=%x	11-7
Serial board disabled by user	13-39
Serial board enabled by user	13-39
Service Prof #<number> does not exist	9-150
SESSION (s) (p) - NON-RECOVERABLE OUTBOUND ERROR	5-2
SESSION (s) (p) - NON-RECOVERABLE INBOUND ERROR	5-2
SESSION ABORTED (s) - GOT CALL ACCEPT	5-6
SESSION ABORTED (s) - GOT CALL CLEAR	5-5
SESSION ABORTED (s) - GOT CALL REQUEST	5-6
SESSION ABORTED (s) - GOT DATA FROM DEVICE WHILE NOT CONNECTED	5-6
SESSION ABORTED (s) - GOT INVITATION TO CLR	5-5
SESSION ABORTED (s) - GOT SESSION CLOSE	5-4
SESSION ABORTED - INVALID SESSION MESSAGE	5-4
SESSION CLOSED (s)	5-6
SESSION CLOSED (s) - GOT CALL ACCEPT	5-7
SESSION CLOSED (s) - GOT CALL REQUEST	5-7
SESSION CLOSED (s) - GOT INVALID SESSION MESSAGE	5-8

Alarm	Page
SESSION ESTABLISHED WITH SLOT (s)	5-6
SESSION IS IN PROGRESS WITH SLOT (s)	5-4
SG_CA_FAILE	11-13
SG_CONFIGURATION_FAILE	11-9
SG_CONFIGURATION_FAILE	11-11
SG_CONFIGURATION_TIMEDOU	11-9
SG_CONFIGURATION_TIMEDOU	11-11
SG_EXCESSIVE_RX_CLEA	11-10
SG_EXCESSIVE_RX_CLEA	11-12
SG_EXCESSIVE_RX_ERROR	11-10
SG_EXCESSIVE_RX_ERROR	11-12
SG_EXCESSIVE_TX_CLEA	11-10
SG_EXCESSIVE_TX_CLEA	11-12
SG_EXCESSIVE_TX_ERROR	11-10
SG_EXCESSIVE_TX_ERROR	11-12
SG_IA_559_FAILE	11-11
SG_IA_FAILE	11-9
SG_INVALID_STATE_DISABLE	11-10
SG_INVALID_STATE_DISABLE	11-12
SG_INVALID_STATE_ENABLE	11-10
SG_INVALID_STATE_ENABLE	11-12
SG_LOCKUP_ERRO	11-13
SG_LOOPBACK_FAILE	11-10
SG_LOOPBACK_FAILE	11-12
SG_LOSS_OF_CARRIE	11-10
SG_LOSS_OF_CARRIE	11-12
SG_LOSS_OF_CARRIER_CLEA	11-10
SG_LOSS_OF_CARRIER_CLEA	11-12
SG_NO_INITIALIZATIO	11-9
SG_NO_INITIALIZATIO	11-11
SG_NO_SUSPENSIO	11-9
SG_NO_SUSPENSIO	11-11
SG_NO_THROTTLE_TIMER	11-9
SG_NO_THROTTLE_TIMER	11-11
SG_RX_LIST_ERRO	11-13
SG_TDR_FAILE	11-10
SG_TDR_FAILE	11-12
SG_TX_LIST_ERRO	11-13
SG_TX_LIST_PUT_FAILE	11-9
SG_TX_LIST_PUT_FAILE	11-11
SHDSL-%d CONFIGURATION INITIALIZATION FAILURE - %<cause>	2-103
SHDSL-%d PORT (n) - PORT ACTIVE	2-102

Alarm	Page
SHDSL-%d PORT (n) - PORT BOOT COMPLETE	2-101
SHDSL-%d PORT (n) - PORT BOOT FAILURE %s	2-101
SHDSL-%d PORT (n) - PORT CONFIG ERROR (%s)	2-103
SHDSL-%d PORT (n) - PORT DISABLED COMPLETE	2-101
SHDSL-%d PORT (n) - PORT ENABLED COMPLETE	2-102
SHDSL-%d PORT (n) - PORT INACTIVE (LOC)	2-103
SHDSL-%d PORT (n) - PORT INACTIVE (RETRAINING)	2-103
SHDSL-%d PORT (n) - PORT INACTIVE (WATCHDOG TIMEOUT)	2-103
SHDSL-%d PORT (n) - PORT INITIALIZATION FAILURE %s	2-102
SHDSL-%d PORT (n) - PORT RETRYING	2-103
SHDSL-%d PORT (n) - PORT STATUS WARNING - PORT DISABLED	2-102
SLOT (n) - HW BOARD FAILURE, CAUSE: BACKGROUND DIAGNOSTIC	7-18
SLOT (n) BOARD BOOT, CAUSE: WATCHDOG TIMER EXPIRED	7-19
SNABSC_CM CM SYSERR	9-126
SNABSC_CM CM SYSERR	13-40
SNABSC_CM CM SYSERR %x, p1=%x, p2=%x, p3=%x	11-17
SNAP: SYSERR (counter)	10-104
SNMP AGENT - AUTHENTICATION FAILURE	10-104
SNMP AGENT - CONNECTED TO MAIN CHANNEL	10-104
SNMP AGENT - LOST MAIN CHANNEL CONNECTION	10-105
SNMP AGENT - SNMP Agent Cold Start	10-105
SNMP AGENT - SNMP Agent Warm Start	10-105
SNMP Alarm/Trap for Node Configuration	14-12
SNMP CONNection FLow CONTROL (cannot get DBUFFER)	10-105
SNMP CONNection FLow CONTROL (cannot get IORB)	10-105
SNMP CONNection FLow CONTROL (cannot get memory)	10-106
SNMP CONNection is Restarting	10-106
SOFTWARE FAILURE LOGGED	10-106
SOFTWARE FAILURE LOGGED	10-106
SOFTWARE FAILURE LOGGED	10-106
SOFTWARE LOADED FROM ALTERNATE FLASH	10-106
SOFTWARE UPDATE COMPLETE	10-106
SOLICIT ABORT	10-107
SOTCP (n) - Invalid packet (cause)	6-10
SOTCP Boot failed - Insufficient memory	10-142
SOTCP Boot failed - Insufficient memory	11-6
SOTCP Boot Failed: %s	10-142
SOTCP Boot Failed: %s	11-6
SOTCP Data loss due to queue overflow	6-10
SOTCP Data Total SVC Decrement Failed	10-107
SOTCP Dynamic Boot Completed	10-143
SOTCP Dynamic Boot Completed	11-6

Alarm	Page
SOTCP Dynamic Boot Started	10-142
SOTCP Dynamic Boot Started	11-6
SOTCP Init failed - IDCM init failed	6-11
SOTCP Init failed Insufficient memory	6-11
SOTCP Init failed Software absent	10-107
SOTCP Maximum Sessions Reduced to %d - Insufficient memory	10-142
SOTCP Maximum Sessions Reduced to %d - Insufficient memory	11-5
SOTCP Memory allocation failed	6-11
SOTCP New connection with connection id (n)	6-11
SOTCP No matching IP peer for (address)	6-11
SOTCP No more connections	6-12
SOTCP No more TCP sessions	6-12
SOTCP Packet allocation failed	6-12
SOTCP Queue toward TCP blocked	6-12
SOTCP Queue toward TCP unblocked	6-13
SOTCP Remote does not support pkt type	6-13
SOTCP Session closed	6-13
SOTCP TCP Active open failed with (remote address)	6-13
SOTCP TCP Listen failed, trying after a while	6-14
SOTCP TCP receive failed, session aborted	6-14
SOTCP TCP session closed by the remote end	6-14
SOTCP TCP session established with destination (address)	6-14
SOTCP TCP session timed out with (address)	6-14
SOTCP Voice Num SVC Decrement Failed	10-107
SOTCP Voice Total SVC Decrement Failed	10-107
SOTCP-%dC%d - Routing loop or maximum hop count exceeded.	10-142
SOTCP-%dC%d - Routing loop or maximum hop count exceeded.	11-5
SOTCP-%sC%s - Routing loop or maximum hop count exceeded.	10-142
SOTCP-%sC%s - Routing loop or maximum hop count exceeded.	11-6
SOURCE (c) - PVC NOT CONNECTED TO (des) - (cause) SOURCE UNAVAILABLE	4-12
Source port is in Busy Out state	9-2
Source Station Record does not exist	9-2
Specific route <net_prefix>/<prefix_len> is sent to peers due to the permission of <msg>	13-45
SPFM #%d - CONFIGURATION MISMATCH ON REMOTE SPFM	10-107
SPFM #%d - CONNECTION ACTIVE %s -> %s	10-107
SPFM #%d - CONNECTION INACTIVE %s -> %s	10-107
SPFM #%d - DISABLED, DUPLICATE SLOT ON SPFM #%d	10-108
SPFM #%d - DISABLED, MISCONFIGURED OPTION	10-108
SPFM #%d - PVC CONNECTED %s -> %s	10-108
SPFM #%d - PVC CONNECTION FAILED ON %s	10-108
SPFM #%d - SPFM HEADER FORMAT ERROR	10-108
SPFM #%d ENTRY BOOT COMPLETE	10-108

Alarm	Page
SPFM #%d ENTRY BOOT FAILED	10-108
SPFM - RX DATA ON UNKNOWN DLCI SLOT %s(%d)	10-108
SS incoming call on already active link	10-109
SS RUN-TIME PARAMETER ERROR	10-109
SS: ENTRY (x) IS INVALID	7-19
START of bop_bri_tx_ callsetup() : chan_num	10-109
START of sdrvc_traitetbenrep ()	10-109
State set to DISABLED in bop_bri_sm_shutdown3()	10-109
State set to DISABLED in bop_bri_sm_shutdown4()	10-109
State set to DISABLED in bop_ bri_cd_rr_disconn_msg()	10-109
State set to DISABLED in bop_ bri_setup_rr_disconn_msg()	10-110
State set to DISABLED in bop_ bri_sm_shutdown()	10-110
State set to DISABLED in bop_bri_init_chan_cbs()	10-110
State set to DISABLED in bop_bri_sm_shutdown2()	10-110
State set to DISABLED in bop_bri_tx_callsetup()	10-110
State set to DISABLED in bop_bri_tx_disconn_msg()	10-110
State set to DISABLED in bop_bri_tx_E_EiaShutdown()	10-110
State set to DISABLED in bop_bri_validate_call()	10-111
State set to DISABLED in bop_bri_validate_call2()	10-111
STATION (n) - ADDRESS ERROR (%02X)	3-14
STATION (n) - CAN NOT FORWARD - STATION DISABLED	3-15
STATION (n) - CLEARING CALL, REMOTE STATION DOWN RECEIVED	3-15
STATION (n) - CONFIGURATION ERROR:	3-15
STATION (n) - CONFIGURATION ERROR:	3-15
STATION (n) - FRAME RECEIVED FOR DISABLED STATION: DLCI (dddd)	3-16
STATION (n) - HPAD STATION ACTIVE	3-16
STATION (n) - HPAD STATION DOWN	3-16
STATION (n) - HPAD STATION INACTIVE	3-16
STATION (n) - HPAD STATION UP	3-16
STATION (n) - INHIBITED - (controller address) (station address) - NO DSP CONNECTION AVAILABLE	3-17
STATION (n) - LINE	3-17
STATION (n) - LOCAL ERROR (message)	3-18
STATION (n) - OVERSIZE FRAME FROM REMOTE	3-18
STATION (n) - POSSIBLE DATA LOSS - (controller address) (station address)	10-111
STATION (n) - STATION BOOT FAILURE (cause)	3-19
STATION (n) - STATION DISABLED	3-19
STATION (n) - STATION DOWN	3-19
STATION (n) - STATION DOWN	3-19
STATION (n) - STATION DOWN - (address)	3-20
STATION (n) - STATION ENABLE FAILURE	3-20
STATION (n) - STATION ADDRESS DUPLICATED	3-20
STATION (n) - STATION BOOT COMPLETE	3-20

Alarm	Page
STATION (n) - STATION BOOT COMPLETE	3-20
STATION (n) - STATION BOOT COMPLETE	3-21
STATION (n) - STATION BOOT FAILED	3-21
STATION (n) - STATION BOOT FAILURE - (cause)	3-22
STATION (n) - STATION BOOT FAILURE - (cause)	3-23
STATION (n) - STATION BOOT FAILURE - (cause)	3-23
STATION (n) - STATION BOOT FAILURE - (cause) (ContÕd)	3-23
STATION (n) - STATION BUSY-OUT COMPLETE	3-23
STATION (n) - STATION BUSY-OUT FAILURE	3-23
STATION (n) - STATION DISABLED	3-24
STATION (n) - STATION DISABLE FAILURE	3-24
STATION (n) - STATION DISABLE FAILURE	3-24
STATION (n) - STATION DISABLE FAILURE - ALREADY DISABLED	3-24
STATION (n) - STATION DISABLED	3-24
STATION (n) - STATION DOWN	3-25
STATION (n) - STATION DOWN	3-25
STATION (n) - STATION ENABLE FAILURE	3-25
STATION (n) - STATION ENABLED	3-25
STATION (n) - STATION ENABLED	3-25
STATION (n) - STATION ENABLED	3-26
STATION (n) - STATION ENABLED	3-26
STATION (n) - STATION INHIBITED ADDR CONFLICT	3-26
STATION (n) - STATION NOT CONFIGURED	3-26
STATION (n) - STATION OPERATIONAL	3-26
STATION (n) - STATION OPERATIONAL	3-26
STATION (n) - STATION REQUESTED DISCONNECT	3-27
STATION (n) - Station Requested Disconnect	3-27
STATION (n) - STATION STAT OVERFLow	3-27
STATION (n) - STATION STATUS WARNING	3-27
STATION (n) - STATION UP	3-27
STATION (n) - STATION DISABLED	3-27
STATION (n) - STN BOOT COMPLETE	3-28
STATION (n) - STN BOOT FAILURE - %s	3-28
STATION (n) - STN DISABLED	3-28
STATION (n) - STN ENABLED	3-28
STATION (n) - TPAD STATION ACTIVE	3-28
STATION (n) - TPAD STATION INACTIVE	3-28
STATION (n) - UNSUPPORTED FRAME SIZE: OPERATING WITH 1024 BYTES	3-29
STATION (n) AUTOCALL ATTEMPTS EXHAUSTED	3-29
STATION (n) BYPASS STATION DOWN	3-29
STATION (n) BYPASS STATION UP	3-29
STATION (n) DATA ERROR (message)	3-30

Alarm	Page
STATION (n) DQ ERROR (message)	3-30
STATION (n) FRAME RECEIVED FOR DISABLED STATION: DLCI (n)	3-30
STATION (n) INSUFFICIENT MEMORY TO PROTECT STATION	3-31
STATION (n) NETWORK LINK DOWN	3-31
STATION (n) NETWORK LINK UP	3-31
STATION (n) RECEIVED ERROR MSG (message)	3-31
STATION (n) REMOTE CALL ESTABLISHED	3-31
STATION (n) STATION BOOT COMPLETE	3-31
STATION (n) STATION BUSY-OUT FAILED	3-32
STATION (n) STATION DOWN	3-32
STATION (n) STATION ENABLED	3-32
STATION (n) STATION INHIBITED - ADDRESS CONFLICT	3-32
STATION (n) STATION POLL RESUMED	3-32
STATION (n) STATION RECEIVED A REMOTE DISCONNECT	3-33
STATION (n) STATION STATUS WARNING (cause)	3-33
STATION (n) STATION UP	3-33
STATION (n) STATION BOOT COMPLETE	3-33
STATION (n) STATION BOOT COMPLETE	3-33
STATION (n) STATION BOOT FAILURE (cause)	3-34
STATION (n) STATION BOOT FAILURE (cause)	3-35
STATION (n) STATION BOOT FAILURE - (cause)	3-35
STATION (n) STATION DISABLE FAILURE - ALREADY DISABLED	3-36
STATION (n) STATION DISABLED	3-36
STATION (n) STATION DISABLED	3-36
STATION (n) STATION DISABLE FAILED	3-36
STATION (n) STATION DISABLE FAILURE (cause)	3-36
STATION (n) STATION DISABLED	3-37
STATION (n) STATION DISABLED	3-37
STATION (n) STATION DOWN	3-37
STATION (n) STATION ENABLE COMPLETE	3-37
STATION (n) STATION ENABLE FAILED	3-37
STATION (n) STATION ENABLE FAILURE (cause)	3-38
STATION (n) STATION ENABLE FAILURE (cause)	3-38
STATION (n) STATION ENABLE FAILURE - ALREADY ENABLED	3-38
STATION (n) STATION ENABLED	3-38
STATION (n) STATION ENABLED	3-38
STATION (n) STATION MNEMONIC ERROR	3-39
STATION (n) STATION POLL SUSPENDED (cause)	3-39
STATION (n) STATION TIMed OUT	3-40
STATION (n) STATION UP	3-40
STATION (n) STATION UP	3-40

Alarm	Page
STATION (n) SUSPICIOUS CONFIGURATION - ZERO VOICE BANDWIDTH AND VOICE RELAY CIRCUITS PRESENT	3-40
STATION (n) SUSPICIOUS CONFIGURATION - FRAME SEGMENTER ENABLE AND VOICE BANDWIDTH IS ZERO	3-41
STATION (n) TPAD STATION DOWN	3-41
STATION (n) TPAD STATION UP	3-41
STATION (n)- STATION BOOT COMPLETE	3-41
STATION (n)- STATION BUSY-OUT	3-41
STATION (n)- STATION DISABLED	3-41
STATION (n)- STATION ENABLE FAILURE - (cause)	3-42
STATION (n)- STATION ENABLED	3-42
STATION (n)- STATION DISABLE FAILURE - (cause)	3-42
STATION ADDRESS DUPLICATED	3-42
STATION BUSY-OUT	3-42
Station identifier - SOCKET SELECT ATTEMPT WHILE IN STACKING MODE	14-13
STATION INHIBITED - (s1) (s2) - ADDRESS CONFLICT	3-42
SW56K CALL DISCONNECTED	10-111
SW56K FAILED TO DISCONNECT	10-111
SW56K LINE IN SERVICE	10-111
SW56K LINE NOT IN SERVICE	10-111
System Clock derives from port %d	11-17
System Clock lost from	
T1-<%d> - %s ALARM %s	10-112
T1/E1 Int. (i/f) -BES THRESHOLD EXCEEDED	7-24
T1/E1 Int. (i/f) -CSS THRESHOLD EXCEEDED	7-24
T1/E1 Int. (i/f) -ES THRESHOLD EXCEEDED	7-24
T1/E1 Int. (i/f) -LCV THRESHOLD EXCEEDED	7-23
T1/E1 Int. (i/f) -PCV THRESHOLD EXCEEDED	7-23
T1/E1 Int. (i/f) -SEFS THRESHOLD EXCEEDED	7-24
T1/E1 Int. (i/f) -SES THRESHOLD EXCEEDED	7-24
T1/E1 Int. (i/f) -UAS THRESHOLD EXCEEDED	7-24
T1/E1 Int. (i/f)-LES THRESHOLD EXCEEDED	7-23
T1/E1-%d VIRTUAL PORT %d - No T1/E1 memory available	2-104
T1/E1-%d VIRTUAL PORT %d - No T1/E1 memory available	2-104
T1/E1-%d VIRTUAL PORT %d - T1/E1 CARD DOES NOT SUPPORT DATA or SWITCHED DATA PORTS	2-104
T14 TIMER EXPIRED	2-104
T1E1 Int (i/f) - BLUE ALARM	7-23
T1E1 Int. (i/f) - ALARM INDICATION SIGNAL	7-22
T1E1 Int. (i/f) - ALARM INDICATION SIGNAL: CLEARED	7-21
T1E1 Int. (i/f) - BLUE ALARM: CLEARED	7-22
T1E1 Int. (i/f) - CMEM Error (code)	7-20
T1E1 Int. (i/f) - Configuration Mismatch	7-20

Alarm	Page
T1E1 Int. (i/f) - Hardware Failed (DRV Memory)	7-19
T1E1 Int. (i/f) - Hardware Failed (DSL Memory)	7-20
T1E1 Int. (i/f) - Hardware Failed (ME Memory)	7-19
T1E1 Int. (i/f) - Hardware Failed (OS Memory)	7-19
T1E1 Int. (i/f) - LOSS OF FRAME	7-22
T1E1 Int. (i/f) - LOSS OF FRAME: CLEARED	7-21
T1E1 Int. (i/f) - LOSS OF SIGNAL	7-22
T1E1 Int. (i/f) - LOSS OF SIGNAL: CLEARED	7-21
T1E1 Int. (i/f) - RED ALARM	7-23
T1E1 Int. (i/f) - REMOTE ALARM INDICATION	7-22
T1E1 Int. (i/f) - REMOTE ALARM INDICATION: CLEARED	7-21
T1E1 Int. (i/f) - Remote loopback ended	7-21
T1E1 Int. (i/f) - Remote loopback in progress	7-21
T1E1 Int. (i/f) - YELLOW ALARM	7-23
T1E1 Int. (i/f) - YELLOW ALARM: CLEARED	7-22
T1E1 Int.(i/f) - RED ALARM: CLEARED	7-22
T1E1DRV-<%d>: %s - %x hex	10-112
T1E1DRV-<%d>: ERROR: CAUSE-%s	10-112
T1E1DRV-<%d>: L3L4mERROR FROM T1/E1 CARD, Cause : %d	10-112
T1E1DRV: INVALID EXECUTION. Line # %d	10-112
T1E1VG_REPT ALARM	7-19
TB ClTcQosMap Prof #<num> does not exist	9-149
TCP: (high)	6-14
TCP: (low)	6-14
TCP: (sn1) to (sn2) given to app.	6-15
TCP: Act opn sccfl PORT (n)	6-15
TCP: app rcv tmout	6-15
TCP: drop seg PORT (n) (sn) ack num (n) rcv invld ACK	6-15
TCP: drop seg PORT (n) (sn) no ACK present	6-15
TCP: drp seg (sip) -> (desip) PORT (n) rsn (cause) snd ACK	6-16
TCP: drp seg PORT (n) (sn), too big for rcv buff	6-16
TCP: ESTAB: rcvd FIN PORT (n) (sn)	6-16
TCP: excssv num rtries	6-16
TCP: frgn prt illgl close of wndw frgn hst (fip) lcl hst (lip) PORT (n) PORT (s)	6-17
TCP: Frng TCB for frgn hst (fip) lcl hst (lip)	6-17
TCP: Frng TCB for frgn hst (fip) lcl hst (lip)	6-17
TCP: get buf fld - cannot snd pkt\r\n	6-17
TCP: Idle tmr fires frgn hst (fip) lcl hst (lip)	6-17
TCP: illgl optn rcvd in SYN seg	6-18
TCP: Lcl wndw zero	6-18
TCP: LISTEN: rcvd RST PORT (n) (sn)	6-18
TCP: pkt cksum fld pkt = (packet checksum) calc = (calculated checksum)	6-18

Alarm	Page
TCP: prcss FIN in ESTAB|SYN RCVD state frgn hst (fip) lcl hst (lip) PORT (n) PORT (s)	6-18
TCP: prcss FIN in invld state	6-19
TCP: Rcvd ACK for Keep Alive	6-19
TCP: rcvd ACK seg with PORT (n) (sn) in LISTEN, snd RST	6-19
TCP: Rcvd data after close, snd RST (fip) -> (lip) PORT (n) PORT (s)	6-19
TCP: rcvd FIN while in LISTEN PORT (n) (sn), snd RST	6-19
TCP: rcvd invld SYN in wndw (sip) -> (desip) PORT (n) kill cnn	6-20
TCP: Rcvd NACK	6-20
TCP: rcvd old seg PORT (n) (sn) snd ACK	6-20
TCP: rcvd old SYN (sip) -> (desip) PORT (n) snd ACK	6-20
TCP: rcvd out of order seg PORT (n) (sn), add hole at end (hb) to (he)	6-21
TCP: rcvd out of order seg PORT (n) (sn), add hole at end (hb) to (he)	6-21
TCP: rcvd out of wndow seg (sip) -> (desip) PORT (n) snd ACK	6-21
TCP: rcvd pkt (sip) -> (desip) PORT (n) no cnn	6-21
TCP: rcvd PSH PORT (n) (sn)	6-22
TCP: rcvd RST PORT (n) (sn), abort	6-22
TCP: rcvd seg PORT (n) (sn), fill beg hole (hb) to (he)	6-22
TCP: rcvd seg PORT (n) (sn), fill end hole (hb) to (he)	6-22
TCP: rcvd seg PORT (n) (sn), rmv hole %d (hb) to (he)	6-23
TCP: rcvd TCP pkt (sip) -> (desip) PORT (n)	6-23
TCP: recv buf too large (rbs), clipped to (cvrbs)	6-23
TCP: rjct seg PORT (n) (sn) bad ACK in SYNRCVD, snd RST	6-23
TCP: rxmt (sn1) to (sn2)	6-24
TCP: Rxmt tmr fires frgn hst (fip) lcl hst (lip)	6-24
TCP: snd ctrl seg (sn) ack num (n) wndw (s)	6-24
TCP: snd FIN (sn), ack (n)	6-24
TCP: State trnstn frm ESTAB to FIN WAIT (fip) -> (lip) PORT (n) PORT (s)	6-24
TCP: State trnstn to CLOSED (fip) -> (lip) PORT (n) PORT (s)	6-25
TCP: state trnstn to ESTAB	6-25
TCP: state trnstn to SYNRCVD	6-25
TCP: SYN_RCVD SYN_SNT: rcvd RST PORT (n) (sn), rtrn->LISTEN	6-25
TCP: SYNRCVD: rcvd vld seg PORT (n) (sn), enter ESTAB	6-26
TCP: TCP cnn clsd frgn hst (fip) lcl hst (lip)	6-26
TCP: TCP is Restarting	6-26
TCP: TCP snd rst to hst (rip)	6-26
TCP: xmit buf too large (tbs), clipped to (cvtbs)	6-26
TCP: xmt seq num (sn1) to (sn2)	6-27
TCP: zero wndw probe (sn)	6-27
TCP:(medium)	6-27
TDM_CLK Module fail (OS Memory)	7-25
TDMTG_CLK Module fail	
Telnet-Error: (cause)	10-113

Alarm	Page
Telnet-Error: (cause) (ContÕd)	10-114
Telnet-Error: (cause) (ContÕd)	10-115
Telnet-Internal Error: (cause)	10-116
Telnet-Internal Error: (cause) (ContÕd)	10-117
Telnet-Internal Error: (cause) (ContÕd)	10-118
TERMINAL (%d) INITIALIZATION ON BRI INT. %d COMPLETED	10-118
TERMINAL (%d) INITIALIZATION ON BRI INT. %d FAILED: %d	10-118
TFR - CONNECTION ESTABLISHED WITH OTHER TFR	10-118
TFR - CONNECTION FAILURE WITH OTHER TFR (cause)	10-119
TFR - FRAME DISCARDED	10-119
TFR - INSUFFICIENT MEMORY - (degree)	7-27
TFR - QUEUE OVERFLow	10-120
TFR - RECEIVED INCOMPLETE FRAME	10-120
TFR - UNKNOWN CALLER	10-120
TFR BOOT FAILURE	10-120
TFRI - CONNECTION ESTABLISHED WITH TFR FOR THE PT (n)	10-120
TFRI - CONNECTION FAILURE WITH TFR FOR PT (n) - (cause)	10-121
TFRI - FRAME DISCARDED (s) - (d)	10-121
TFRI - INSUFFICIENT MEMORY - INITIALIZED WITHOUT DCP	10-121
TFRI - INSUFFICIENT MEMORY - INITIALIZATION FAILED	10-122
TFRI - SOCKET REGISTRATION FAILED	10-122
TFRI BOOT FAILURE (cause)	10-122
TFTP Server Access Violation with (file name) from (client IP address)	10-145
TFTP Server CMEM Downloading Start with (file name) to (client IP address)	10-145
TFTP Server Disabled on port: port number	10-144
TFTP Server Enabled on port: port number	10-144
TFTP Server Image Downloading Start with (file name) to (client IP address)	10-144
TFTP Server Operation successful: operation name with client IP address	10-144
TFTP:	10-122
TFTP: CMEM access failure\r\n%s	10-123
TFTP: Error in software image file	10-123
TFTP: failure	10-123
TFTP: Flash erasure failure	10-123
TFTP: Flash write failure	10-123
TFTP: Local transfer failure\r\n%s\r\nError text = %s\r\nError code = %d	10-123
TFTP: Operation successful	10-123
TFTP: partial success	10-124
TFTP: Remote transfer failure\r\n%s\r\nError text = %s\r\nError code = %d	10-124
TFTP: Software download already in progress	10-124
TFTP: System failure\r\n%s	10-124
TFTP: UDP registration failure\r\n%s	10-124
THE NUMBER OF SWITCHED SERVICE ENTRIES	10-125

Alarm	Page
THE PEER'S NAME EXCEEDS16 CHARACTERS	10-125
This alarm indicates that the operator the certificate is going to will expire within one month.	10-145
This alarm message indicates that TFTP Server CMEM downloading is started.	10-145
This alarm message indicates that TFTP Server Image downloading is started.	10-144
This alarm message indicates that there is a TFTP Server Access Violation.	10-145
This alarm message indicates that there is not enough memory for a CRL file.	10-145
This alarm message indicates that you cannot setup a TCP connection with the CA.	10-145
This alarm message indicates the server is disabled on the port (n).	10-144
This alarm message indicates the server is enabled on the port (n).	10-144
This alarm message indicates the the Server operation i s successful.	10-144
This is an information message only. No corrective actions are required.	9-42
This is an information message only. No corrective actions are required.	9-42
This is an information message only. No corrective actions are required.	9-43
This is an information message only. No corrective actions are required.	9-43
This message indicates a Digital Certificate general error message.	10-145
TIME OF WEEK DISABLING:SWITCHED TO Low BANDWIDTH	7-27
TKR.001 unexp (type) frm (control) fm (source _MAC) ssap (source_SAP) dsap (dest_SAP) nt (net_id)	9-127
TKR.002 unexp (type) brd frm LLC-control frm (source _MAC) ssap (source_SAP) , dssp (dest_SAP) , net (net_id)	9-127
TKR.003 unkn SNAP mfr code (num) fm (source _MAC) nt (net_id)	9-128
TKR.004 unkn SNAP mfr code (num) fm (source _MAC) nt (net_id)	9-128
TKR.005 unkn SNAP type (type) fm (source _MAC) nt (net_id)	9-129
TKR.006 unkn SNAP type (type) fm (source _MAC) nt (net_id)	9-129
TKR.007 unkn SAP (num) fm (source _MAC) nt (net_id)	9-130
TKR.008 unkn SAP (num) fm (source _MAC) nt (net_id)	9-130
TKR.009 unexp U frm (control) fm (source_MAC) ssap (source_SAP) dsap (dest_SAP) nt (net_id)	9-131
TKR.010 unexp U frm (control) fm (source_MAC) ssap (source_SAP) dsap (dest_SAP) nt (net_id)	9-131
TKR.011 add new RIF to (MAC_add) (RIF header) nt (net_id)	9-132
TKR.012 xtra RIF to (MAC_add) dscd nt (net_id)	9-132
TKR.013 del RIF to (MAC_add) nt (net_id)	9-132
TKR.014 (selftest) fld (error) nt (net_id)	9-133
TKR.015 dwn sts cls nt (net_id)	9-133
TKR.016 dwn adap chk (code) nt (net_id)	9-134
TKR.017 pkt sz (con_size) too big for 4 Mbps, limiting to (size), nt (net_id)	9-134
TKR.018 16 Mbps not supp on dev, net (net_id)	9-134
TKR.019 runt pkt (len) frm (source), net (net_id)	9-135
TKR.020 DN bd ln (actual) (claimed) (source) -> (dest) nt (net_id)	9-135
TKR.021 LOOP rev (source) -> (dest), nt (net_id)	9-135
TKR.022 LOOP odd skp (count), (source) -> (dest), nt (net_id)	9-136
TKR.023 LOOP bd skp (count), (source) -> (dest), nt (net_id)	9-136
TKR.024 LOOP func (func) not forw, (source) -> (dest), nt (net_id)	9-137
TKR.025 LOOP mc fwd dst (f_MAC_add), (source) -> (dest) , nt (net)	9-137
TKR.026 LOOP fwd (source) -> (dest) , nt (net)	9-137

Alarm	Page
TKR.027 LOOP fwd to (f_Enet_add) dsc, rsn (code), nt (net)	9-138
TKR.028 rif table corruption for interface (net)	9-138
TKR.029 rif entry is being removed entry (hwe_add) (type) nt (net)	9-138
TKR.030 MAC frm typ (MAC_frame) unex from (hwe_add) nt (net)	9-138
TKR.031 Main rcd on nt (net)	9-138
TKR.032 test frm (MAC_add), src sap (source_SAP), nt (net)	9-139
TKR.033 xid frm (MAC_add) , sap (source_SAP), nt (net)	9-139
TKR.034 unable to allocate buffer in handler	9-139
TKR.035 new RIF (rif) for (MAC_add) nt (net)	9-139
TN3270: device - LU BOOT COMPLETE	10-125
TN3270: Device CANNOT BOOT; ENTRY NOT DEFINED	10-125
TN3270: device Device Active for n.n.n.n	10-125
TN3270: device Device Inactive for n.n.n.n	10-125
TN3270: device Session Active for n.n.n.n.	10-126
TN3270: device Session Inactive for n.n.n.n	10-126
TN3270: device TCP Session Closed for n.n.n.n	10-126
TN3270: Server Parameters BOOT COMPLETE	10-126
TN3270: TCP Session Opened for n.n.n.n.	10-127
TNL_ENCR - Tunnel queue Flush	12-7
TNL_ENCR - Unknown packet (n)	12-7
TNL_ENCR Channel closed for (x.x.x.x) -> (y.y.y.y)	12-6
TNL_ENCR Channel opened for (x.x.x.x) -> (y.y.y.y)	12-6
TNL_ENCR- Tunnel queue Full	12-6
TOPOLOGY STABLE	10-127
TOPOLOGY UNSTABLE	10-127
ToW: NOT ACTIVE, ENTRY NOT FOUND IN CMEM	10-127
ToW: NOT ACTIVE, INITIALIZED TO DEFAULT	10-127
ToW: NOT ENOUGH MEMORY	10-127
ToW:ACTIVE	10-127
TPA (ident) - CONNECTION UP	10-128
TPA (ident) - CONNECTION DOWN (cause)	10-128
TPA (ident) - CONNECTION IS IN PROGRESS	10-128
TPA (ident) - MAXIMUM AUTOCALL ATTEMPTS FAILURE,	10-128
TPA (n) - CONNECTION DOWN (cause)	10-129
TPA (type)-(s) - PACKET ALLOCATION FAILED	5-8
TPA (type)-(s) - SESSION STATUS MESSAGE COULDN'T SEND TO DEVICE	5-8
TPA (type)-(s1) - SESSION ABORTED (s2) - DATA WHEN OPENING SLOT	5-5
TPA (type)-(s1) - SESSION ABORTED (s2) - GOT ILLEGAL MESSAGE	5-5
TPA (type)-(s1) - SESSION CLOSED (s2) - GOT ILLEGAL MESSAGE	5-7
TPA(FRA)-(s) - CLEARING CALL, BAD RESPONSE	10-129
TPA(FRA)-(s) - CONNECTION DOWN (cause)	10-129
TPA(FRA)-(s) - CONNECTION IS IN PROGRESS (cause)	10-129

Alarm	Page
TPA(FRA)-(s) - CONNECTION UP	10-130
TPA-FRA, IDCM NOT UP	10-130
TPA-FRA, IDCM OR TGO DOES NOT EXIST	10-130
TPA-FRA, NOT ENOUGH MEMORY	10-130
TPA-SDLC, IDCM NOT UP	7-27
TPA-SDLC, IDCM OR TGO DOES NOT EXIST	7-28
TPA-SDLC, NOT ENOUGH MEMORY	7-28
TPA-UDP, DOES NOT EXIST	10-130
TPA-UDP, NOT ENOUGH MEMORY	7-28
TPA-UDP, REGISTRATION WITH SIP FAILED	10-131
TPA-UDP, REGISTRATION WITH UDP FAILED	10-131
TPA-X25, IDCM NOT UP	7-28
TPA-X25, IDCM OR TGO DOES NOT EXIST	7-28
TPA-X25, NOT ENOUGH MEMORY	7-29
TPA2780 CONNECTED	10-131
TPA2780 DISCONNECTED	10-131
TPA3270 CONNECTED	10-131
TPA3270 DISCONNECTED	10-131
TPA_TCP, CONNECTION RETRIES OVER	7-29
TPA_TCP, TCP TIMEOUT, DISREGARDING PACKETS	6-27
TPA_TCP,PACKET ALLOCATION FAILED	7-29
TPA_TCP,QUEUE FULL,PACKET DROPPED	6-27
TPA_TCP,TCP ACTIVE OPEN FAILED	6-27
TPA_TCP,TCP LISTEN FAILED	6-28
TPA_TCP,TCP-SEND FAILEDCONNECTION DROPPED	6-28
TPR SLOT (s) BOOT COMPLETE	10-132
TPR SLOT (s) DISABLED	10-132
TPR SLOT (s) ENABLED	10-132
TPR-BOOT COMPLETE	2-104
TPR-BOOT FAILURE - NUMBER OF SLOTS CHANGED	10-132
TPR-FWD Packet for DEAD slot (s) arrived	10-132
TPR-INIT (s) TPA module (d) does not exist	10-133
TPR-INIT (s) TPA module (d) init failed	7-29
TPR-INIT FAILED	7-29
TPR-SLOT (s) BOOT FAILURE - SLOT TYPE CHANGED	10-133
TR-%d PORT DUPLICATE TOKEN RING NUMBERS	10-33
TR-%d PORT NOT DISABLED	2-104
TR-%d TX HALTED	2-104
TR-(x) AUTO REMOVE ERROR	2-105
TR-(x) BEACON CONDITION	2-105
TR-(x) COMMAND REJECT %x (%x)	2-105
TR-(x) DIAGNOSTIC CHECK	2-105

Alarm	Page
TR-(x) FATAL ERROR	2-106
TR-(x) LOBE WIRE FAULT	2-106
TR-(x) LOSS OF SIGNAL	2-106
TR-(x) LOSS OF SIGNAL CLEARED	2-106
TR-(x) PORT CMD TIMEOUT %x	2-106
TR-(x) PORT DOWN	2-107
TR-(x) PORT INITIALIZATION FAILURE TMS380 OPEN FAILED	2-107
TR-(x) PORT INITIALIZATION FAILURE TMS380 RESET FAILED	2-107
TR-(x) PORT INITIALIZATION FAILURE TMS380 INIT FAILED	2-107
TR-(x) PORT INITIALIZATION SUCCESSFUL	2-108
TR-(x) PORT UP	2-108
TR-(x) REMOVE RECEIVED	2-108
TR-(x) RX COMMAND TIMed OUT	2-108
TR-(x) SINGLE STATION ERROR	2-108
TR-(x) TRANSMIT DIAG	2-109
TR-(x) TRANSMIT ERROR	2-109
TR-(x) TRANSMIT ERROR 2	2-109
TR-(x) TRANSMIT TIMEOUT	2-110
TR-(x) TX BEACON CONDITION	2-110
TR-(x) TX BEACON CONDITION CLEARED	2-110
TR-(x) TX COMMAND TIMed OUT	2-110
TRANSMITTER INACTIVITY TIMEOUT	10-133
TUNNEL No timer available for cache and cache disabled	12-13
TUNNEL Tnl no (n) Bridge Link no (b) - Conf as SR Bridge, Mod not present	12-13
TUNNEL Tnl no (n) Bridge Link no (b) - Conf as TB Bridge, Mod not present	12-13
TUNNEL Tnl no (n) Bridge Link no (b) - Conf as TB SR Bridge, Mods not present	12-13
TUNNEL Tnl no (n) Bridge Link no (b) - Conf Bridge type unsupported	12-13
TUNNEL - Configuration Error - Tnl# (n) ; tnl vir addr (ifc # (1) addr) is already used as src addr by tnl - (m)	12-5
TUNNEL - Configuration Error- Tnl# (n) ; tnl src addr is already used as vir addr by tnl - (m), ifc - (1)	12-5
TUNNEL - Not enough memory - mem Alloc for tnl brdg link params failed	12-3
TUNNEL - Not enough memory - mem Alloc for tunnel encryption failed.	12-3
TUNNEL - Not enough memory - Not Enough Memory to Initialize Module TUNNEL	12-2
TUNNEL - Not enough memory Ð Allocation for Tunnel Table Entry Failed	12-2
TUNNEL - Not enough memory Ð cache is disabled	12-3
TUNNEL - Not enough memory Ð Memory allocation for Tunnel Array failed	12-2
TUNNEL - Not enough memory Ð Memory allocation for Tunnel Context Block failed	12-2
TUNNEL - Not enough memory ÐAllocation of tunnel Table entry failed, TNL No. - (n) onwards not available	12-2
TUNNEL - Tnl pkt rcvd frm (y.y.y.y) to (x.x.x.x) on tnl no (n)	12-6
TUNNEL - Tnl pkt sent frm (x.x.x.x) to (y.y.y.y) on tnl no (n)	12-6
TUNNEL - Tunnel cache cleared	12-7
TUNNEL - Tunnel cache entry x.x.x.x -> y.y.y.y deleted	12-7
TUNNEL - Tunnel cache garbage collecting...	12-7

Alarm	Page
TUNNEL no (n) - Cache is not initialized and can't install cache	12-7
TUNNEL no (n) - Compression not supp. Incoming IP-RUIHC Pkt Drpd	12-11
TUNNEL no (n) - congestion, pkt dropped	12-7
TUNNEL no (n) - Context State Pkt Sent	12-8
TUNNEL no (n) - Incoming IP-RUIHC Pkt drp as tnl ifc is down	12-10
TUNNEL no (n) - Incoming IP-RUIHC Pkt drp as tnl netp is NULL	12-11
TUNNEL no (n) - Incoming IP-RUIHC pkt drp due to Decompression failure	12-11
TUNNEL no (n) - Incoming IPX Pkt drp as tnl ifc is down	12-10
TUNNEL no (n) - Incoming IPX Pkt drp as tnl netp is NULL	12-10
TUNNEL no (n) - Incoming IPX pkt drp due to unsupp payload prtcl	12-10
TUNNEL no (n) - Incoming Pkt drp as encr pkt rcvd on non-encr tnl	12-9
TUNNEL no (n) - Incoming Pkt drp due to err in IP hdr	12-9
TUNNEL no (n) - Not enough memory Ð RUIHC Module Failed to initialize ruihc ptr	12-14
TUNNEL no (n) - Outgng pkt drp ,unavail of mem for fragm	12-9
TUNNEL no (n) - Outgoing Bridge pkt drp due to unsupp payload prtcl	12-8
TUNNEL no (n) - Outgoing IP pkt drp due to unsupp payload prtcl	12-8
TUNNEL no (n) - Outgoing IPX pkt drp due to unsupp payload prtcl	12-8
TUNNEL no (n) - Outgoing pkt drp due to unsupp encap prtcl	12-9
TUNNEL no (n) - Outgoing pkt drp due to unsupp payload prtcl	12-9
TUNNEL no (n) - Pkt dropped due to unsupp payload prtcl	12-8
TUNNEL no (n) - Pkt drp due to err in GRE hdr cksum	12-8
TUNNEL no (n) - Rcvd out of order pkt. Pkt dropped	12-8
TUNNEL no (n) - SR Packet received when Bridge type is TB	12-12
TUNNEL no (n) - STPE Bad Hello Threshold exceeded for tnl no (n)	12-12
TUNNEL no (n) Ð Context State Pkt rcvd	12-11
TUNNEL no (n) Ð Encryption Disabled or Encryption H/W not running	12-14
TUNNEL no (n) Ð Encryption SIMM not UP	12-15
TUNNEL no (n) Ð Incoming Bridge Pkt drp as tnl brdg ptr is NULL	12-11
TUNNEL no (n) Ð Incoming Bridge Pkt drp as tnl bridge link is down	12-11
TUNNEL no (n) Ð Incoming Bridge pkt drp due to unsupp payload prtcl	12-12
TUNNEL no (n) Ð Incoming IP Pkt drp as tnl ifc is down	12-10
TUNNEL no (n) Ð Incoming IP Pkt drp as tnl netp is NULL	12-10
TUNNEL no (n) Ð Incoming IP pkt drp due to unsupp payload prtcl	12-10
TUNNEL no (n) Ð Incoming Pkt drp as non-encr pkt rcvd on encr tnl	12-9
TUNNEL no (n) Ð Incoming Pkt drp due to unsupp encap prtcl	12-9
TUNNEL no (n) Ð Incoming Pkt drp due to unsupp payload prtcl	12-12
TUNNEL no (n) Ð Invalid encryption profile	12-15
TUNNEL no (n) Ð Module Encryption does not Exists	12-14
TUNNEL no (n) Ð Module RUIHC does not Exists	12-14
TUNNEL no (n) Ð Outgoing Bridge pkt dropped by wan	12-12
TUNNEL no (n) Ð Outgoing Bridge Pkt drp as tnl bridge link is down	12-12
TUNNEL no (n) Ð RUIHC Module is unable to Init ruihc profile	12-14

Alarm	Page
TUNNEL no (n) Ð RUIHC Profile not configured	12-14
TUNNEL Pkt rcvd.Accepted	12-13
TUNNEL Pkt sent out. Seq no->(s)	12-13
TUNNEL Table entry no. (n) duplicate of entry no. (m)	12-3
TUNNEL Ð Configuration Error - "IP and IPX tnl ifc (i) not conf for Tnl no (n)	12-4
TUNNEL Ð Configuration Error - "tnl ifc (i) dis or unconfig for Tnl no (n)	12-5
TUNNEL Ð Configuration Error - Bridge Link no (m) not conf for Tnl no (n)	12-5
TUNNEL Ð Configuration Error - In tunnel (n) bridge link no is conflicting with lcon (m) bridge link no	12-3
TUNNEL Ð Configuration Error - In tunnel (n) interface is conflicting with lcon (m) interface	12-3
TUNNEL Ð Configuration Error - Invalid LAN nexthop in tunnel (n)	12-4
TUNNEL Ð Configuration Error - IP tnl ifc (i) not conf for Tnl no (n)	12-4
TUNNEL Ð Configuration Error - IPX tnl ifc (i) not conf for Tnl no (n)	12-4
TUNNEL Ð Configuration Error - LAN interface (i) used by tunnel (n) is not enabled	12-4
TUNNEL Ð Configuration Error - net pntr of vir/tnl ifc no Ð (i) for tunnel no Ð (n) is NULL	12-5
TUNNEL Ð Configuration Error - Tnl no (n) : source address not a NAT ext addr nor an ifc addr	12-4
TUNNEL Ð Configuration Error - Tnl no. (n) 's Lcon no (m) not config	12-4
TUNNEL Ð Configuration Error - Tnl-(n) bridge link clash lcon bridge link configured in lcon-(m)	12-5
TUNNEL Ð Configuration Error - Tnl-(n) tnl ifc clash phys ifc configured in lcon-(m)	12-5
TWO MASTERS ON MULTIPOINT LINK	3-43
TWO MASTERS ON MULTIPOINT LINK - STATION (n)	3-43
TX MESSAGE QUEUE OVERFLOW	10-133
UDP Registration Failure	10-133
UDP.001 pkt (source) #> (dest) port (port n) no srvr	9-140
UDP.002 pkt (source) #> (dest) port (port n) no srvr	9-140
UDP.003 dsc pkt frm (source) bd length (len)	9-140
UDP.004 bd cksm clc (calc_csum) rcv (rcvd_csum)	9-140
UNABLE TO COMPRESS CMEM - CMEM NOT WRITTEN	10-134
UNASSIGNED LCN	10-134
UNESCAPED CHAR FOUND	10-134
UNEXPECTED FRAME	10-134
UNEXPECTED INTERRUPT, SR/VECTNUM $%6.6x	10-134
UNKNOWN CARD TYPE - SLOT %d	7-29
Unreachable network (net) - in entry (p)	10-134
UNSUCCESSFUL CALL THRESHOLD EXCEEDED	2-110
Unsupported or invalid Protocol Packet received on rfc1483_LLC_SNAP LCON (n)	9-71
Unsupported or invalid Protocol Packet to be sent on rfc1483_LLC_SNAP LCON (n)	8-6
UPDATING SOFTWARE	10-134
USER MESSAGE LOST	10-135
USER_DISABLE: SWITCHED TO Low BANDWIDTH	7-29
UTILIZATION DOWN:SWITCHED TO Low BANDWIDTH	7-30
UTILIZATION UP:SWITCHED TO High BANDWIDTH	7-30
V.25 BIS CALL FAILURE - (cause)	10-135

Alarm	Page
V.25 BIS ERROR - (cause)	10-135
V.25 BIS PROTOCOL MISMATCH	10-136
V.25 BIS UNKNOWN ERROR	2-111
VAN JACOBSON COMPRESSION FAILED ON INBOUND PACKET	6-28
VIRTUAL MAPPING ERROR, CAUSE: %s	10-136
VIRTUAL MAPPING ERROR, CAUSE: %s	10-136
VOICE CALL: CALLING (cnum), CALLED (cdnum), SRC (source), DEST (destination), CLR (reason), TIME (t) sec	2-111
VOICE CALL: CALLING (cnum), CALLED (cdnum), SRC (source), DEST (destination), CLR (reason), TIME (t) sec	2-112
VOICE RECORD CONVERSION	10-136
VOICE RECORD CONVERSION COMPLETED	10-136
VOICE RECORD CONVERSION FAILED	10-136
VOICE SWITCHING RECORD CONVERSION COMPLETED	10-137
VOICE SWITCHING RECORD FAILED CONVERSION	10-137
VOICE- SIGNALING TRACE/DEBUG:	10-137
VOICE-%d %s	10-137
VOICE-%d SIGNALING TRACE: %s	10-137
VOICE-(x) VSM COMMAND: EID (x), OPCODE (x), PAYLOAD (x)	10-138
VOICE-(x) VSM RESPONSE: EID (x), OPCODE (x), PAYLOAD (x)	2-112
VPMT entry for port %d missing or invalid	11-14
VPMT Module fail (OS Memory)	7-25
VPMT Module fail (VPMT Memory)	7-25
VPMT Module fail (VPMT_CB Memory)	7-25
vrrp : address<addr> cannot be configured on int (intf) vrid (vrid)	14-13
vrrp : duplicate VRID (vrid) on int (intf)	14-13
vrrp : failed to allocate memory for a VRRP structure	14-13
vrrp : int (intf) vrid (vrid) advertisement interval mismatch	14-14
vrrp : int (intf) vrid (vrid) advertisement recvd from (ip_addr)	14-14
vrrp : int (intf) vrid (vrid) advertisement sent	14-14
vrrp : int (intf) vrid (vrid) gen debug (detail)	14-14
vrrp : int (intf) vrid (vrid) invalid authentication from (ip_addr)	14-14
vrrp : int (intf) vrid (vrid) ip address mismatch	14-14
vrrp : int (intf) vrid (vrid) pkt discarded due to (reason)	14-14
vrrp : int (intf) vrid (vrid) state change from (old_state) to (new_state)	14-14
vrrp : virtual ip (addr) matches real address on int (intf)	14-13
WRONG MESSAGE ADDRESS	3-43
XDLC - (p) (n) - ADDRESS ERROR (a)	3-43
XDLC - (p) (n) - BAD FRAME LENGTH (id)	3-44
XDLC - (p) (n) - BAD FRAME TYPE (id)	3-44
XDLC - (p) (n) - BAD N(R) (n)	3-44
XDLC - (p) (n) - FRMR (f) (ps) (d)	3-45
XDLC - (p) (n) - MX25 STATION DOWN	3-45
XDLC - (p) (n) - MX25 STATION UP	3-45

Alarm	Page
XDLC - (p) (n) - OVERSIZE FRAME FROM REMOTE	3-46
XDLC - (p) (n) - STAT OVERFLow	3-46
XDLC - (p) (n) - TPAD STATION ACTIVE	3-46
XDLC - (p) (n) - TWO MASTERS ON MULTIPOINT LINK	3-47
XDLC - (p) (n) -TPAD STATION INACTIVE	3-47
XLB MODULE INITIALIZED	10-138
XN.001 (prot) trunc pkt frm (net)/(node), xns (xns_len) phys (phys_len)	9-141
XN.002 (prot) non-zero TC frm (net) /(node) (tc)	9-141
XN.003 (prot) bd rtng cksum frm (net) /(node), (rcvd_csum) (cmp_csum)	9-141
XN.004 (prot) hop cnt ovflo frm (net) /(node) to (dest)	9-142
XN.005 (prot) no gwy frm (net) /(node) to (dest)	9-142
XN.006 (prot) wstd hop frm (net) /(node) to (dest	9-142
XN.007 (prot) dst hst 0 frm (net) /(node) to (dest)	9-143
XN.008 (prot) (s_net) /(s_node)-> (d_net) /(d_node)	9-143
XN.009 (prot) pkt too lng to frwd (p_size) > (m_size) nt (net_id) frm (net) /(node)	9-143
XN.010 (type) frm (s_net) /(s_node) for (d_net) /(d_node) dsc, rsm (code)	9-144
XN.011 (prot) intrfc (net)/(node) net (net_id) up	9-144
XN.012 (prot) del nt (d_net) rt via (gw) nt (net_id)	9-144
XN.013 (prot) tbl ovrfl, dst (d_net)	9-145
XN.014 (prot) echo type (op) to skt socket frm (s_net) /(s_node)	9-145
XN.015 (prot) bd src (s_net)/(s_node) nt (net_id)	9-145
XN.016 (prot) bad net 0 (s_net)/(s_node) - (d_net)/(d_node)	9-146
XN.017 (prot) no mem for err pkt	9-146
XN.018 (prot) short (len) pkt frm (s_net)/(s_node) (?) net (net_id)	9-147
xx IS CONNECTED TO ANOTHER AP, COMPRESSION IS NOT ALLOWED	9-77