Cisco Voice Network Switching Installation and Operation

Release 3.0 FT Draft
Revised April 1998

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-xxxxxxxxxxxxx=
Text Part Number: 78-xxxx-xx

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco’s installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.

- Move the equipment to one side or the other of the television or radio.

- Move the equipment farther away from the television or radio.

- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The following third-party software may be included with your product and will be subject to the software license agreement:

CiscoWorks software and documentation are based in part on HP OpenView under license from the Hewlett-Packard Company. HP OpenView is a trademark of the Hewlett-Packard Company. Copyright © 1992, 1993 Hewlett-Packard Company.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Network Time Protocol (NTP). Copyright © 1992, David L. Mills. The University of Delaware makes no representations about the suitability of this software for any purpose.

Point-to-Point Protocol. Copyright © 1989, Carnegie-Mellon University. All rights reserved. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

The Cisco implementation of TN3270 is an adaptation of the TN3270, curses, and termcap programs developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981-1988, Regents of the University of California.

Cisco incorporates Fastmac and TrueView software and the RingRunner chip in some Token Ring products. Fastmac software is licensed to Cisco by Madge Networks Limited, and the RingRunner chip is licensed to Cisco by Madge NV. Fastmac, RingRunner, and TrueView are trademarks and in some jurisdictions registered trademarks of Madge Networks Limited. Copyright © 1995, Madge Networks Limited. All rights reserved.

XRemote is a trademark of Network Computing Devices, Inc. Copyright © 1989, Network Computing Devices, Inc., Mountain View, California. NCD makes no representations about the suitability of this software for any purpose.

The X Window System is a trademark of the X Consortium, Cambridge, Massachusetts. All rights reserved.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

Cisco Voice Network Switching Installation and Operation

9802R

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

About This Manual

Welcome to the Installation and Operation manual for the Cisco Voice Network Switching (VNS) system.

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. For further information about the Cisco CD-ROM package, see the section Cisco CD-ROM.

This preface includes the following sections:

- Objectives
- Audience
- Organization
- Related Documentation
- Cisco CD-ROM
- Conventions
- New Features in VNS Release 3.0

Objectives

This publication will step you through the initial site preparation, installation, and configuration of the VNS and the Voice Network Switching system.

Audience

This publication is designed for the person installing the VNS, who should be familiar with electronic circuitry and wiring practices and have experience as an electronic or electromechanical technician. It is also intended for the network administrator who will configure the VNS and provision the network to support voice SVCs. The installers and network administrators should also be familiar with Cisco IGX™ 8400 series wide-area switch and Cisco IPX® wide-area switch, voice connections, and Cisco wide area switching networks. During the initial installation of a VNS, it is also helpful to have a system administrator on-hand who is familiar with your network and UNIX servers.

Organization

This publication contains the following chapters:

Chapter 1 **Introduction to Voice Network Switching**

This chapter describes Voice Network Switching, the VNS processor, and basic VNS features. It concentrates on the interfaces between a PBX and the VNS and the VNS and the Cisco switch and WAN switching network.

Chapter 2 **Site Requirements**

This chapter describes the equipment and site conditions that should be in place when you get ready to set up your VNS.

Chapter 3 **Unpack and Inspect the VNS**

This chapter describes unpacking your VNS shipping package.

Chapter 4 **Rack Mounting the VNS**

This chapter describes how to install your VNS into a rack, typically with a Cisco IGX™ 8400 series wide-area switch (or a Cisco IPX® wide area switch).

Chapter 5 **Connecting Power to the VNS**

This chapter describes how to connect AC or DC power to your VNS and power it up.

Chapter 6 **VNS Interface Connections**

This chapter describes how to connect the VNS physical interfaces to a terminal, a Cisco wide-area switch, and a Cisco StrataView Plus workstation.

Chapter 7 **Understanding the VNS Configuration Interface**

This chapter describes the VNS Configuration Interface, a command line interface (CLI), and its menus, options and parameters.

Chapter 8 **VNS Network Operation**

This chapter describes some of the common procedures encountered during the operation of a VNS network, particularly the provisioning of a VNS network through the VNS Configuration Interface.

Appendix A **Cable Information**

This appendix provides information about the AC power cables and the null modem cable.

Appendix B **Troubleshooting**

This appendix provides some VNS troubleshooting hints as well as a list of the VNS SNMP Traps.

Appendix C **Call Detail Records**

This appendix provides information about the format and content of the Call Detail Records (CDRs) that are kept by the VNS for each call.

Appendix D **Dial-In Support**

This appendix provides instructions for connecting a modem to the VNS to provide remote access for customers support.

Appendix E **Reinstalling VNS Interface Drivers**

This appendix provides instructions for reinstalling the interface drivers for the Frame Relay Card and the E1 Network Interface Cards (E1 NICs). These drivers are factory installed and should normally not have to be reinstalled in the field.

Appendix F **Upgrading to VNS 3.0 Software**

This appendix provides instructions for upgrading VNS software.

Appendix G **SPNNI Operation**

This appendix provides some guidelines for calculating the Frame Relay bandwidth needed for the connection between two VNSs controlling separate domains.

Appendix H **VNS Terminology**

This appendix defines the terms that help you understand the Voice Networking Switching enhancement to Cisco WAN switching networks. It includes some common networking terms that have specific meaning for the VNS.

Appendix I **Channel Associated Signaling Voice Switching**

This appendix describes Voice Network Switching for PBXs using Channel Associated Signaling (CAS). It also describes the special configuration procedures for the IGX’s Universal Voice Module with Model B or higher firmware which is required for CAS-to-QSIG conversion.

Appendix J **VNS Configuration Sheets**

This appendix provides some blank VNS configuration worksheets which can be copied and used during configuration of your system.

Related Documentation

- *Cisco StrataView Plus Operations* providing for procedures for using the StrataView Plus network management system.
- The appropriate release of the Cisco WAN switching network publication set, including:
    - *Cisco WAN Switching System Overview Manual* providing an introduction to Cisco WAN switching networks.
    - *Cisco BPX 8620 Reference* providing a general description and technical details of the Cisco BPX® 8600 series wide-area switch.
    - *Cisco IPX Reference* providing a general description and technical details of the IPX® wide-area switch.
    - *Cisco IPX Installation* providing installation instructions for the IPX switch.
    - *Cisco IGX 8400 Series Reference* providing a general description and technical details of the IGX™ 8400 series wide-area switch.
    - *Cisco IGX 8400 Series Installation* providing installation instructions for the IGX switch.
    - *Cisco MGX 8220 Reference* providing a general description and technical details of the MGX™ 8220 edge connector.
    - *Cisco WAN Switching Command Reference* providing detailed information on operating the BPX switch, IGX switch, and IPX switch through their command line interfaces.

Cisco CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more up to date than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Conventions

This publication uses the following conventions to convey instructions and information.

Command descriptions use these conventions:

- Commands and keywords are in boldface.
- Arguments for which you supply values are in italics.
- Elements in square brackets ([ ]) are optional.
- Alternative but required keywords are grouped in braces ({ }) and are separated by vertical bars (|).

Examples use these conventions:

- Terminal sessions and information the system displays are in screen font.
- Information you enter is in **`boldface screen font`**.
- Nonprinting characters, such as passwords, are in angle brackets (< >).

- Default responses to system prompts are in square brackets ([ ]).

Warning This warning symbol means *danger.* You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translated versions of this warning, refer to the *Regulatory Compliance and Safety Information* document that accompanied the product.)

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in the manual.

New Features in VNS Release 3.0

The major features of Voice Network Switching, release 3.0, covered in this manual include:

- Support for AT&T 4ESS ISDN protocol variant per AT&T Technical Reference TR41459
- Configurable cause codes
- Support for the Generic Functional Procedures as described in the QSIG protocol specification ISO/IEC 11572
- Improved procedures for configuring number translation
- Support for the IGX's Universal Voice Module (UVM card)
- Break-Out/Break-In (BOBI) feature which allows PBXs using QSIG to make calls through a Cisco VNS WAN switching network to a user connected to the European ISDN DSS1 public network. It also allows users on the European ISDN public network to call into a QSIG PBX through the Cisco VNS private network.
- Improved VNS Configuration Interface delete and modify functions

The feature that was added to Voice Network Switching in Release 2.2 and covered in this manual is:

- CAS2.2 which is a variation of VNS QSIG protocol that supports switching for PBXs which use Channel Associated Signaling. This feature is supported in conjunction with the IGX's Universal Voice Module (UVM) with Model B or higher firmware. This version of the UVM, which provides CAS-to-QSIG conversion, is supported in switched software release 8.5.

The Voice Network Switching features that were added to VNS in Release 2.1, and are covered in this manual, include:

- Q931A (Japanese ISDN) which adds another signaling protocol variant that Voice Network Switching supports.
- Database validation which provides automatic and periodic checking of the VNS database's integrity. This new feature also permits an operator to manually validate the database through the VNS Configuration Interface.
- Wildcard addressing routing for QSIG 2.1 allows an operator to enter wildcards as characters in VNS addresses. This feature simplifies addressing and speeds up call routing.
- Numerical sorting of addresses in the VNS database, which permits the VNS database address records to be browsed systematically.

- D channel preferred routing allows the operator to specify preferred routes for the D channel signalling between a PBX and the VNS and between VNSs in separate service areas (domains).
- D channel status provides a visible indication on the StrataView Plus network management system to indicate when a D channel has failed.
- Call Detail Records have been enhanced to indicate if the record is for either a voice or data call. These records also include four digits to indicate the year in date- and-time stamps to prevent problems when the year 2000 comes around.
- Break-Out/Break-In (BOBI) feature which allows PBXs using DPNSS to make calls through a Cisco VNS network to a user connected to the European ISDN DSS1 public network. It also allows users on the European ISDN public network to call into a DPNSS PBX through the Cisco VNS private network.
- Support for European ISDN DSSI (ETSI) the signaling variant used by the European public ISDN network.
- Multi-homed links support for two or more links to the same end-user site (CPE or PBX).
- Multiple service areas which allows each VNS system to be assigned to control one or more nodes (i.e., IGX or IPX switch). This allows the VNS network to be divided up into more efficient domains.
- Multi-level logins provides user-access verification to control access and use of the VNS Configuration Interface. In other words, the use of the VNS Configuration Interface is password controlled.

In addition, this manual introduces the following product name changes:

- The Cisco BPX® 8600 series wide-area switch was previously known simply as the Cisco StrataCom BPX switch.
- The Cisco IGX™ 8400 series wide-area switch was previously known simply as the Cisco StrataCom IGX switch.
- The Cisco IPX® wide-area switch was previously known simply as the Cisco StrataCom IPX switch.
- The Cisco MGX™ 8220 edge connector was previously known as the Cisco StrataCom AXIS interface shelf.

Introduction to Voice Network Switching

This chapter provides an introduction to Voice Network Switching. It contains the following sections:

- Overview
- VNS System Components
- Signaling
- Cisco WAN Switching Networks
- VNS Operation
- VNS to StrataView Plus Workstation
- Redundant Pairs
- Configuration and Provisioning
- Call Detail Records
- Technical Assistance
- VNS Hardware and Software

Overview

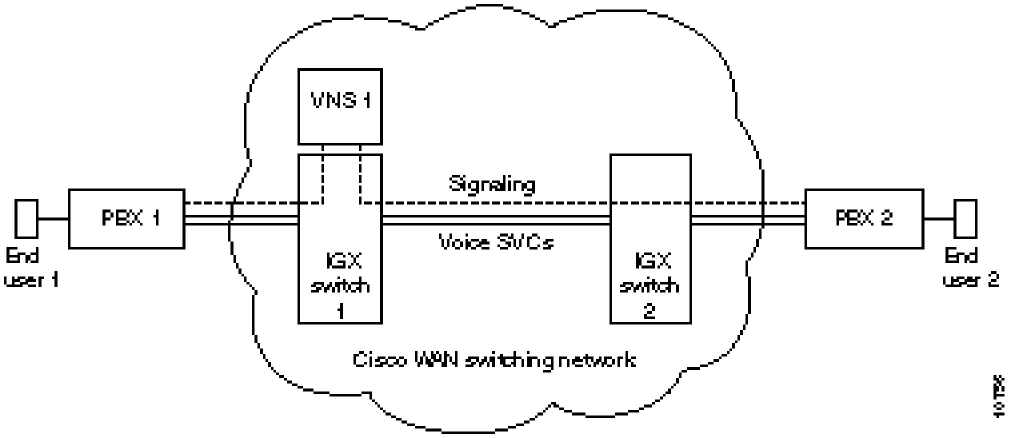
The Voice Network Switching (VNS) application provides switched virtual circuits (SVCs) for voice or data calls over a Cisco WAN switching network. For VNS applications, the Cisco WAN switching network is typically built of Cisco IGX™ 8400 series wide-area switches or Cisco IPX® wide-area switches. With the VNS application in a Cisco WAN switching network, private branch exchanges (PBXs) using Digital Private Network Signaling System (DPNSS), QSIG, Q931A (Japanese ISDN), or AT&T 4ESS ISDN signaling protocols will be able to establish voice calls on demand, just as if they are dialing a public switched telephone network. Voice Network Switching will also switch calls from PBXs using Channel Associated Signaling (CAS), when it is used in conjunction with the IGX's Universal Voice Module with Model B or higher firmware, which performs CAS-to-QSIG conversion. The supported signaling protocols are all variations of the Integrated Services Digital Network (ISDN) signaling protocol. Voice Network Switching provides for the direct connection of DPNSS-, or QSIG-, or Q931A-based PBXs, reducing the need for tandem connections. In other words, with the addition of Voice Network Switching, the Cisco WAN switching network assumes many of the functions of a transit PBX, that is, tandem switching functions. This reduces the number of E1 trunks required to interconnect PBXs and enables the replacement of tandem PBXs.

A VNS network also saves network bandwidth by consolidating traffic over fewer physical interfaces, and through the use of Voice Activity Detection (VAD) and Adaptive Differential Pulse Code Modulation (ADPCM) voice compression provided by IGX/IPX switches. That is to say, a VNS network allows the use of a Cisco WAN switching network's standard voice service features to be applied to switched voice circuits from DPNSS, QSIG, Q931A, or AT&T 4ESS ISDN PBXs. Cisco's standard voice services save network resources by providing a voice compression ratio of up to 10:1.

Note The VNS was designed to work with a network of IGXs or IPXs. Although most of the examples in this manual show an IGX switch, an IPX switch could just as easily have been used.

As shown in Figure 1-1, Voice Network Switching provides a signaling mechanism to establish and maintain SVCs between PBXs across a Cisco WAN switching network. The VNS and the Cisco WAN switching network provide the network side of the ISDN user-network interface. Figure 1-1 illustrates that there is a separate signaling channel to manage the setup and disconnection of the SVC calls. The signaling channel actually stretches to the PBXs because the PBXs exchange signaling messages with the network. This signaling channel, often referred to as a D channel, is indicated by the dashed line, and can be thought of as a virtual signaling network, or signaling plane over-laid on the traditional Cisco WAN switching network. The solid line indicates the end-user traffic, the actual voice SVCs, between the two PBXs.

Figure 1-1 Basic VNS SVC Call



In this simple illustration, a typical call setup would follow this sequence:

Step 1 An End-User 1 at PBX 1 makes a call to End-User 2 at PBX 2.

Step 2 PBX 1 initiates a Call setup message, which is in DPNSS, QSIG, Q931A, or AT&T 4ESS ISDN format; this message is passed from IGX switch 1 to VNS 1.

Step 3 VNS 1 processes this message, including determining whether this will be a data or a voice call.

Step 4 VNS 1 instructs IGX switch 2 to build the circuit from PBX 1 to PBX 2, similar to adding a connection (addcon) for a standard network.

Step 5 When the circuit is built, IGX switch 2 passes a message to VNS 1, which relays this information to PBX 2.

Step 6 When the End User at PBX 2 answers the call, a connect message is sent from PBX 2 to VNS 1.

Step 7 VNS 1 sends a connect message to the End User at PBX 1, and the connection setup is completed.

And a typical call disconnect would follow this sequence:

Step 1 When either party hangs up, the release message is again sent from the associated PBX through the signaling channel to the attached VNS.

Step 2 The circuit is removed by the VNS which created it, and a call release message is sent to the other end user.

Step 3 After the end user acknowledges the release message, the call is cleared.

The originating VNS also generates a Call Detail Record, which includes the calling and called party numbers, call setup time and call duration. CDRs are kept in files which can be periodically collected by another host, such as the StrataView Plus (SV+) Network Management Station (NMS).

Each VNS also keeps other statistics for maintenance and diagnostic purposes.

VNS System Components

Voice Network Switching is implemented with two or more VNS servers deployed in a Cisco WAN switching network. The VNS server, referred to simply as a VNS in this manual, is a rack-mounted adjunct processor co-located with a Cisco wide-area switch. VNS servers are always sold in redundant pairs.

VNS System

The VNS system consists of two identical VNS servers, which can be configured to perform as a redundant pair. Each VNS server is a closed, scalable multitasking platform with the following features:

- 140 MIPS CPU
- 128 Megabytes of memory
- 2 Gigabyte hard disk

The VNS comes in four models:

- VNS-AC (AC powered)
- VNS-DC (DC powered)
- VNS-AC-E (AC powered)
- VNS-DC-E (DC powered)

These models are functionally equivalent. The -E versions of the VNS are newer models that will replace older (VNS-AC and VNS-DC) versions; only -E models are being shipped at this time. The slight differences between the models will be pointed out in this documentation where it is appropriate.

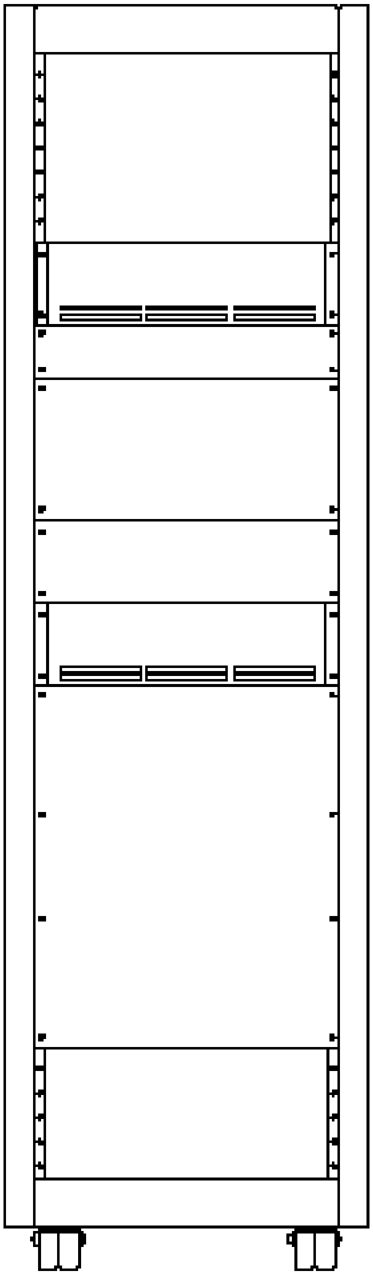
The VNS is typically connected to a co-located Cisco wide-area switch (an IGX or IPX switch in this application) and is often mounted in the same rack, as shown in Figure 1-2. The VNS is connected to the Cisco wide-area switch through a Frame Relay Card, an E1 channelized Network Interface Card (E1 NIC), and an Ethernet (that is, 802.3) interface.

The redundancy feature of VNS systems are described in the section, Redundant Pairs.

Table 1-2 at the end of this chapter lists the VNS hardware and software model numbers.

Note The Frame Relay Card interface is only used in networks with multiple service areas or domains.

Figure 1-2 Rack-Mounted VNS



VNS processors (that is, VNS servers) are installed as a redundant pair, with one active and one in the standby mode. This redundancy minimizes network downtime due to equipment failures and maintenance activity. When a switchover from the active to the standby VNS occurs, existing signaling will be switched over to the newly active unit, which will assume the same provisioning and configuration as the original active unit. The principal redundancy features are:

- 1:1 co-located warm redundancy
- Hardware failure and software resource protection monitoring
- Role resolution protocol between active and standby VNSs
- Configuration data synchronization with real-time and bulk updates
- Call Detail Record (CDR) data synchronization between active and standby VNSs with real-time and bulk updates
- Reassignment of signaling channels to the standby whenever the active unit fails

Interfaces

The VNS uses four main physical interfaces:

- **Terminal port** for the direct connection of a terminal, such as a VT-100, to provide access to local configuration and VNS Command Line Interface (CLI).
- **Ethernet port** (10Base-T) for connection to the local standby VNS, the local IGX or IPX switch, and a local SV+ Workstation. Telnet sessions can be established through the Ethernet port. Telnet sessions perform the same functions as can be performed with a directly-connected terminal.
- **Frame Relay Card** (RS449) for connection to a Frame Relay Module (FRM or FRP) on the co-located Cisco wide-area switch. The Frame Relay port provides the VNS signaling channel to other VNSs in the Cisco WAN switching network. Cisco provides two Frame Relay Card cables. One connects the RS449 connector to a V.35 interface; the other connects the RS449 connector to an X.21 interface.

Note The Frame Relay Card interface is only used when there are multiple VNS service areas (or domains) in a network.

- **E1 Network Interface Cards (E1 NICs)** (75-ohm BNC connectors) for connection to the co-located nodes Channelized Voice Modules (CVM) or Universal Voice Modules (UVM) on the IGX switch (or CDPs on IPX switch). These E1 channels to the Cisco wide-area switch provide the path for the DPNSS, QSIG, or Q931A signaling (that is, the D channel) from the PBXs connected to the Cisco wide-area switch. There are two E1 NICs, which are referred to as Voice Port 1 and Voice Port 2, installed in each VNS; they both do not have to be connected to the node, however. (The E1 PRIs from the PBXs are typically terminated on another CVM in a Cisco wide-area switch.)

The VNS also supports the following application interfaces:

- **SNMP** to configure and monitor the VNS. (Note that the VNS Configuration Interface [VNS CLI] uses this SNMP interface to configure the VNS.)
- **FTP** (file transfer protocol) for uploading statistics, Call Detail Records (CDRs), and downloading new software releases and revisions.
- **Telnet** for running the VNS Configuration Interface remotely.

VNS Software

VNS software includes the following components:

- The Solaris 2.4 UNIX Operating System for the VNS.
- Integrated SNMP agents providing configuration and system information.
- VNS processes which manage initialization, redundancy, configuration, event handling, and switched circuit activity.
- Call Processor which handles the signaling between the PBX and the VNS.
- MIB II (per IETF RFC1213) system and interfaces groups, and a VNS II proprietary MIB.

Signaling Variants

The signaling between the VNS and the PBXs is based on ISDN variants. There are six signaling variants supported in VNS Release 3.0:

- AT&T 4ESS ISDN protocol variant in accordance with Technical Reference 41459 - AT&T Network ISDN Primary Rate Interface and Special Application, User-Network Interface Description (AT&T, August 1996). The VNS will supports the symmetrical slave without channel negotiation option. In addition, the VNS will support Basic Call with detection of Bearer Capability information for voice and data, pass calling and connection line ID, and calling and connected line ID restriction.
- Digital Private Network Signaling System (DPNSS) in accordance with BTNR (British Telecommunications Network Requirement) No. 188, Issue 5, Vols. 1-5, December 1989. (This document covers the VNS DPNSS Release 2.1).
- QSIG based on ETSI QSIG standards. (This document covers the VNS QSIG Release 2.1.)
- European ISDN (ETSI)
- Q931A, also known as Japanese ISDN, based on JT-Q.931-a (layer 3), JT-Q.921-a (layer 2), and JT-i.431-C (layer 1...JT) specifications as described by TTC. (This document covers Q931 Release 2.1.)
- CAS 2.2 is a VNS QSIG protocol designed to work with the IGX's Universal Voice Module (UVM) with Model B firmware to provide Voice Network Switching for PBXs using CAS signaling. The UVM supports CAS switching in switched software release 8.5. CAS switching is described in Appendix I, Channel Associated Signaling Voice Switching.

Note VNS Release 3.0 adds the AT&T 4ESS ISDN variant to the protocols previously supported by Voice Network Switching. The protocols previously supported include QSIG 2.1, DPNSS 2.1, and Q931A (Japanese ISDN) 2.1, as well as CAS2.2. All of these protocol releases, which are independent of one another, are covered in this document. Where appropriate, differences between the AT&T 4ESS ISDN, QSIG 2.1, DPNSS 2.1, and Q931A 2.1 are pointed out. DPNSS 2.1 is compatible with switched software release 8.4, while QSIG 2.1 and Q931A 2.1 are compatible switched software release 8.2. (The release note, or Customer Service, will identify the appropriate switched software release for each VNS protocol.)

Generic Functional Procedures

VNS Release 3.0 also supports the generic functional protocol for the control of supplementary services and additional network features as defined by ETSI specification for the QSIG protocol, ETS300-239. The generic functional procedures are used to transport supplementary service invocations and responses from end-to-end. Acting like a transit PBX, the VNS supports related and call independent procedures, including support for the FACILITY message and Facility Information Elements.

Software Release Feature Matrix

VNS Release 3.0 consists of protocol packages: QSIG 2.1,QSIG 3.0, DPNSS 2.1, Q931A 2.1, CAS 2.2, and AT&T 4ESS ISDN, which are purchased separately. These VNS protocol packages (that is, feature software) support different sets of features. Some features are supported by all protocol packages; other features are supported by only one protocol. All the features are described in this document; where appropriate, this document will point out which software package supports the feature, and which does not. Features which are not mentioned or which were part of previous VNS (formerly DNS) releases are considered to be supported by all software packages. In Chapter 7, Understanding the VNS Command Line Interface, those menu fields which are not supported by a particular software package will be pointed out.

Table 1-1 lists the features supported by each protocol package. The feature is listed in the first column. An X in the second, third, or fourth columns indicates that this feature is supported by QSIG 2.1, QSIG 3.0, DPNSS 2.1, Q931A 2.1, or AT&T 4ESS ISDN.

Table 1-1 BOBI or QSIG Software Feature Matrix

Feature	QSIG 2.1	QSIG 3.0	DPNSS 2.1	Q931A 2.1	CAS 2.2[1]	AT&T 4ESS ISDN
Break-Out/Break-In (BOBI)	X	X	X			
Multi-homed E1 links	X	X	X	X	X	X
CVM Redundancy[2]	X	X	X	X	X	X
Config Save and Restore	X	X	X	X	X	X
Multiple Service Areas	X	X	X	X	X	X
Hard-coded Cause Codes	X	X			X	X
Wildcard addressing and routing	X	X			X	X
Wildcard in translation rules		X				
Database integrity	X	X	X	X	X	X
Numerical sorting of addresses	X	X	X	X	X	X
D-Channel Preferred Routing	X	X	X	X	X	X
D-Channel Status	X	X	X	X	X	X
Year 2000 Compatibility	X	X	X	X	X	X
Voice or Data CDR Records	X	X	X	X	X	X
New CLI and other Enhancements	X	X	X	X	X	X
Configurable Cause Codes		X				
Generic Functions		X				

[1] CAS 2.2 is QSIG protocol designed to work with the IGX's UVM and provide CAS Voice Switching. This feature is described in Appendix I, Channel Associated Signaling Voice Switching.

2. The CVM Redundancy feature also applies to the UVM card.

VNS Configuration Interface

The VNS Configuration Interface is run from the VNS multitasking platform, either from a directly connected terminal or remotely through a telnet session. The VNS Configuration Interface, also known as the VNS Command Line Interface (CLI), provides a mechanism for the operator to configure the VNS and provision VNS services. Using a SNMP interface to VNS, the CLI can:

- Configure the VNS database
- Provision (or delete) addresses in the database
- Get the VNS operational status

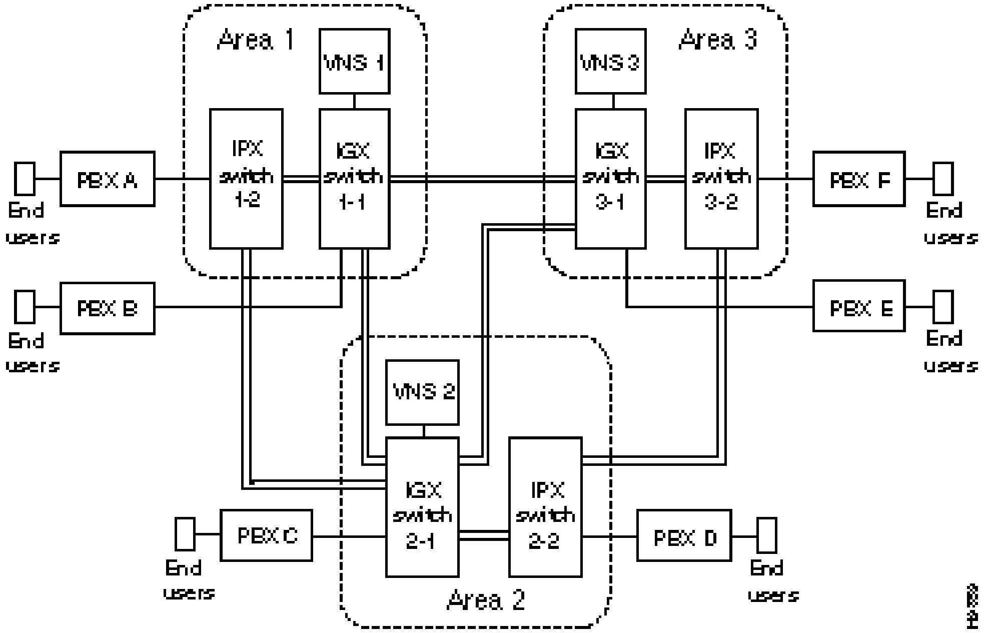
VNS Area

Each VNS (or redundant pair of VNSs) are assigned to control a group of one or more nodes, i.e., an IGX or IPX switch. These nodes are considered the VNS's service area (or domain). The VNS will be directly attached to one of the nodes in its area. The VNS processes call setup or release requests for calls originating in its area, or calls received from another area but destined for this one. VNS areas do not overlap. This feature is referred to as multiple domains.

The VNS exchanges heartbeat messages with all of the IGX or IPX switches in its area. The heartbeat allows the VNS to maintain a status of each node in its area. The VNS detects if a node goes out of service or returns to service.

Figure 1-3 illustrates a network with three VNS areas. Although it is not shown in the figure, the VNSs in each area will be installed as redundant pair in each area. There is VNS system, redundant pair of VNSs, serving each individual service area (or domain).

Figure 1-3 VNS Areas



In Figure 1-3, each VNS has an IGX switch and an IPX switch in its area. VNS 1 has IGX switch 1-1 and IPX switch 1-2, and VNS 2 has IGX switch 2-1 and IPX switch 2-2, and so on. VNS 1 would exchange heartbeat messages with IGX switch 1-1 and IPX switch 1-2. Each IGX/IPX switch is connected to one PBX with its complement of end users. So in Area 1, VNS 1 would be responsible for processing call setups for all calls from PBX A and PBX B. It would also handle calls destined for PBX A and PBX B. Similarly, VNS 2 would be responsible for call setups for PBX C and PBX D, and VNS 3 would be responsible for PBX E and PBX F.

There do not have to be multiple VNS areas in a VNS network. In this case, there is only a single VNS deployed in the network. Therefore, there does not have to be a signaling overlay network, and there do not have to frame relay connections between VNSs. The VNS’s Frame Relay (RS-422 to V.35 or X.21) card will not have to be connected to the node.

Signaling

Voice Network Switching was designed to work with four forms of message-oriented common-channel signaling often used by PBXs:

- DPNSS
- QSIG
- ETSI
- Q931A (Japanese ISDN)
- AT&T 4ESS ISDN

These messages set up, maintain, and terminate voice channel connections. They also support the operation of many PBX supplementary services or features, including calling name and number display, network call forward, network call redirect, centralized attendant, centralized voicemail, etc. These signaling protocols support a set of capabilities that are very desirable in an enterprise voice network. Cisco wide-area switches function as transit nodes for these networks, receiving call control and feature messages from PBXs via the signaling-channel connection and forwarding them across the signaling overlay network to the appropriate destination PBX.

DPNSS, QSIG, and Q931A are variants of ISDN D-channel signaling. QSIG is based on ISDN Q.921/931 standards. DPNSS is a pre-ISDN standard protocol, developed by British Telecommunication (BT) in the 1980s. QSIG was originally specified by ECMA, then was adopted by European Telecommunications Standards Institute (ETSI) and the ISO. It is becoming a world-wide standard for PBX interconnection. ETSI is also used as the name for European ISDN. Q931A is based on Japanese ISDN standards. All of these protocols (DPNSS, QSIG, ETSI, and Q931A are supported by a different signaling stack in the VNS. Thus in VNS, signaling stack refers to the particular signaling protocol to be supported by the UNI port or the VNS.)

Each E1 Network Interface Card (NIC) in an VNS server can interface with 30 signaling channels. (The second E1 NIC card in the VNS provides redundancy.)

Note CAS switching, which is not an ISDN variant or message oriented protocol, is also supported by VNS Release 3.0. This support requires the IGX UVM-C card and switched software release 8.5. This feature is described in Appendix I, Channel Associated Signaling Voice Switching.

Cisco WAN Switching Networks

Cisco WAN switching networks are public or private networks built around Cisco cell-switching nodes. These nodes utilize Cisco ’s patented FastPacket technology and/or standards-based Asynchronous Transfer Mode (ATM) and are designed to support multiple applications integrating voice, constant and variable-bit rate data, video, frame relay, and ATM services on one multimedia wide area network.

Permanent Virtual Circuits (PVCs)

A virtual circuit only allocates a physical connection when there is data to send. The connection between two devices is set up at the start of transmission, or when the network is configured. A PVC is similar to a dedicated private line because the connection is set up on a permanent basis. Frame relay PVC standards are well defined.

The *Cisco WAN Switching System Overview* contains further information about Cisco WAN switching networks and frame relay circuits

Frame Relay PVCs

Frame Relay PVCs are used in the Voice Network Switching application for the signaling channels between VNSs. Frame relay PVCs are identified by their Data Link Connection Identifier (DLCI), which identify logical connections within a shared physical channel. Network nodes normally route frames through a network based on their DLCIs. Frames with the same DLCI are associated with a single logical channel, or PVC.

Switched Virtual Circuits

With a switched virtual circuit, there must be some signaling mechanism to build a connection each time the user (i.e., PBX) needs it. In addition, when the call is disconnected, there must be a mechanism for the orderly disconnection of the call, and the network’s resources must be relinquished. During a disconnect, the Cisco WAN switching network sweeps through its connection tables and removes the connection. (Typical call setup and call disconnect sequences were described earlier.)

On the edge of the Cisco WAN switching network, i.e., from the PBX to the network, the signaling mechanism is either DPNSS, QSIG, Q931A, or AT&T 4ESS ISDN protocol. Within the Cisco VNS network, from VNS-to-VNS and VNS-to-IGX/IPX switch, this signaling mechanism is handled by a Cisco Proprietary Network-to-Network Interface (SPNNI).

Note VNS-to-VNS signaling is only needed when there are multiple VNS areas or domains.

VNS Operation

Setting up and tearing down SVCs is a complicated process. To simplify this process, we will describe the three main interfaces:

- PBX to VNS
- VNS to VNS
- VNS to Node (IGX/IPX switch)

PBX to VNS

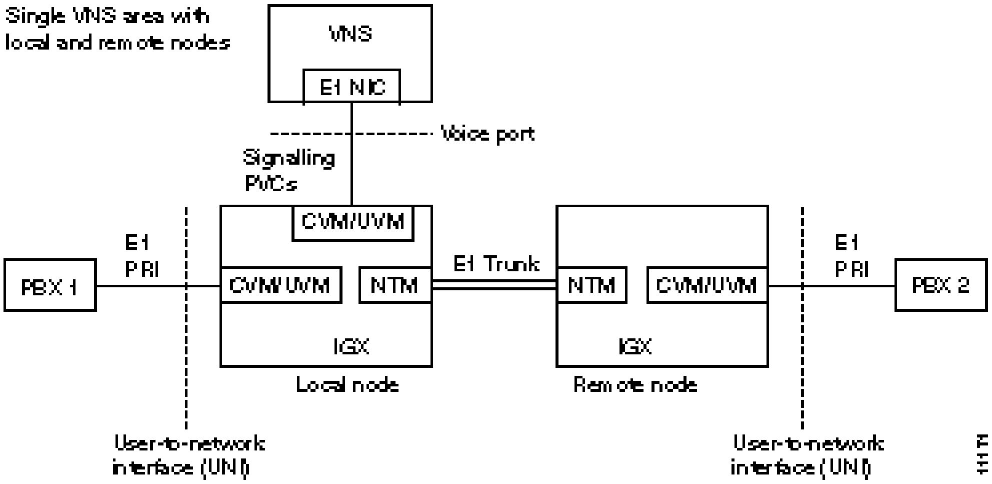
For the VNS application, the PBX connects to a Cisco wide-area switch (e.g., IGX switch) through a Channelized Voice Module (CVM), a Universal Voice Module (UVM), or an IPX's Channelized Data PAD (CDP), which terminates an E1 PRI. The E1 PRI contains both the bearer channels with user's voice or data and a D channel, the signaling channel. The bearer channels should be routed to the far-end or which ever termination point the user is trying to call. Before that can happen, the network must setup the call or calls. The signaling channel, the D channel, carries the messages to begin the call setup process.

Therefore, the D channel must be routed to the VNS responsible for the node to which the PRI is connected. In Figure 1-4, there is one VNS with two nodes, local and remote, in its area. There are two PBXs, PBX 1 and PBX 2, attached to these nodes. Both of these PBXs have E1 PRI interfaces terminating on a CVM in an IGX switch. In the E1 PRI, the signaling channel, typically timeslot 16 (TS16), must be routed to the VNS over a PVC. There must be a signaling channel configured (i.e., a PVC added) for every PBX in a VNS's domain.

So in Figure 1-4, there would be two PVCs providing signaling channels to the VNS. The first would be a local connection, i.e., a DACS connection on the local node connecting the CVM connected to the PBX 1 to the CVM connected to the VNS's E1 NIC. The other signaling channel would be from the CVM on the remote node connected to the PBX 2 to the VNS E1 NIC. This PVC would be carried over the E1 trunk in Figure 1-4. (Remember an E1 NIC can manage up to 30 signaling PVCs.)

As shown in Figure 1-4, the PBX to VNS network (i.e., Cisco wide-area switch) interface is referred to as a User-to-Network Interface (UNI). This interface is also referred to as a UNI port. Both signaling channels and voice channels are carried across the UNI port. The connection between the VNS's E1 NIC and the node's CVM or UVM(or CDP in an IPX) is referred to as a Voice Port in VNS terminology.

Figure 1-4 VNS Domain with Two Nodes



Note Specific technical information about the CVM (and UVM) can be found in the *Cisco IGX 8400 Series Installation* and *Cisco IGX 8400 Series Reference* manuals. Specific technical information about the CDP can be found in *Cisco IPX Installation* and *Cisco IPX Reference* manuals. Note that the limitations of the UVM card, such as only 16 channels for LDCELP available on port 1, as described in the C*isco IGX 8400 Series Reference*, apply to UVMs employed in VNS networks.

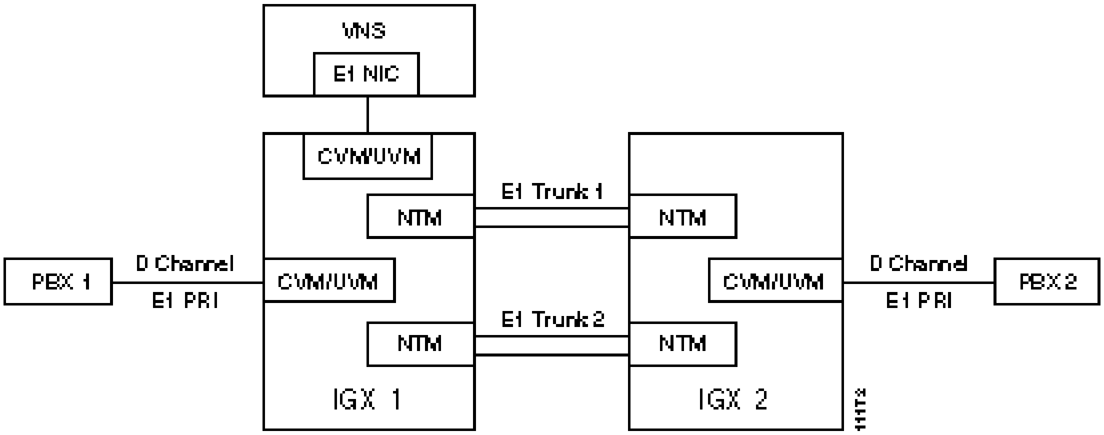
Configurable Cause Codes

When a call is terminated abnormally, some PBXs can re-route the call on a different trunk based on the cause code that is contained in the Disconnect, Release, or Release complete message. Often, the re-route has to be done for different disconnection causes, but PBXs can be configured to re-route on a limited set of cause codes. For this reason, the VNS provides a way to map any cause code to a different cause code. Since different PBXs use different cause codes to trigger re-routing, the cause code mapping must be done on a per-port or a PBX-type basis. The VNS creates a cause code mapping file that is associated with a specific port during configuration. This same file can be associated with all the ports connected to the same type of PBX. The file is created and edited through the VNS Configuration Interface. For more information, see Cause Code Mapping in Chapter 7.

Port D-Channel Preferred Routing

Often the UNI port is on a node which is not directly attached to the VNS doing the signaling for that area. In this case, which is illustrated in Figure 1-5, the signaling channel (that is, D channel) may be routed to the VNS by more than one path. In this example, the D channel from BPX 2 could be routed to the VNS through either E1 Trunk 1 or E1 Trunk 2. The VNS Configuration Interface allows you to configure a preferred route for the D-channel connection between the PBX (that is, UNI port) and VNS. In this example, you could configure a preferred route over E1 Trunk 1 or E1 Trunk 2. The Port Preferred Route option allows you to specify up to 9 hops in the preferred route. This option allows the network operator to avoid network congestion and to provide load balancing and resiliency across network trunks. This feature is described further in Chapter 7 in the section Configuring Preferred D Channel Routes.

Figure 1-5 Port D Channel Preferred Routing



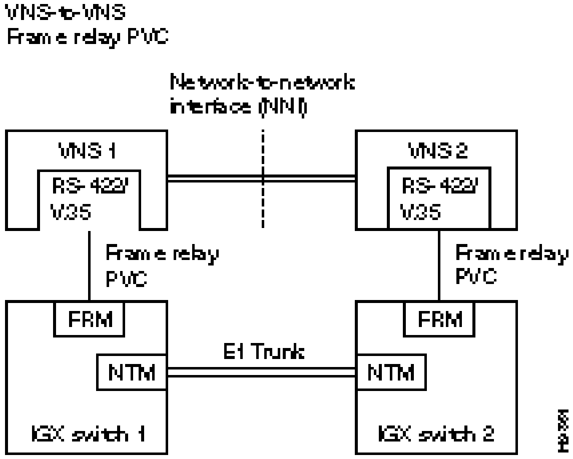
VNS to VNS

In a Voice Network Switching network with multiple domains, every VNS must be able to communicate with every other VNS in the network. This full-mesh topology provides the overlaying signaling plane necessary for the network to route and deliver SVCs. This messaging plane provides flow control mechanisms, so that once a call is admitted, it will be reliably delivered to the destination. (The VNS-to-VNS interface is only required when there are multiple VNS areas.)

In Figure 1-6, VNS 1 and VNS 2 are in different areas. They each reside over their own domain. (They could have other nodes in their respective domains, but they aren't shown here.) They are both directly attached to an IGX switch through a Frame Relay Module (FRM). There must be a frame relay PVC configured between these two VNSs. When there is a Frame Relay PVC established between the two VNSs, they are considered to be locally adjacent.

The logical connection between the two VNSs, indicated by the dashed line in Figure 1-6, is considered a network-to-network interface (NNI). In a VNS network, this is a Cisco Proprietary NNI (SPNNI) protocol, and thus this connection is often referred to as a SPNNI connection. One end of this interface will be configured as the user side (user-spnni) and the other side will be configured as the network side (network-spnni). SPNNI is media (or physical layer) independent and both reliable and efficient.

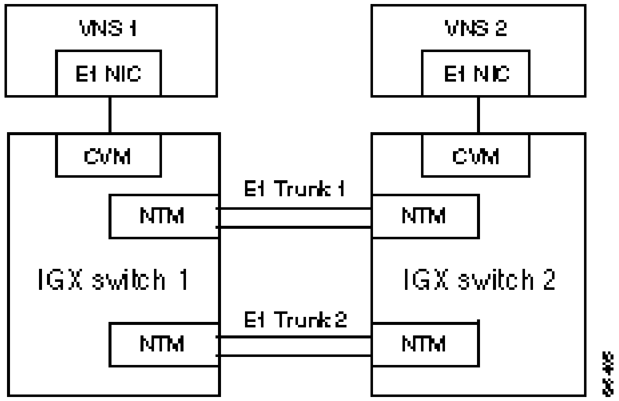
Figure 1-6 VNS to VNS PVC



Local Adjacency Preferred Routing

The SPNNI connection between two locally adjacent VNSs will often traverse several routing nodes which are not shown in Figure 1-6. In such a case, there will be more than one possible route between the locally adjacent VNSs. Figure 1-7 illustrates a simple case where there is more than one possible path for routing the SPNNI connection between locally adjacent VNS 1 and VNS 2. The VNS Configuration Interface allows you to configure a preferred route for the SPNNI connection between these locally adjacent VNSs. In this example, it will allow you to specify the route over E1 Trunk 1 or E1 Trunk 2. The Local Adjacency Preferred Routing option allows you to specify up to 9 hops in the preferred route. This option allows the network operator to avoid network congestion and to provide load balancing and resiliency across network trunks. This feature is described further in Chapter 7 in the section Local Adjacency Preferred Route Information.

Figure 1-7 Local Adjacency Preferred Route



SPNNI Operation

The actual SPNNI connection between two locally adjacent VNSs is added through the VNS Configuration Interface. The VNS adds the connection as a default Frame Relay PVC. Occasionally the default Frame Relay connection default parameters will have to be modified to accommodate network traffic. Appendix G, SPNNI Operation, provides further information about modifying the Frame Relay parameters between locally adjacent VNSs.

VNS to Node (IGX/IPX Switch)

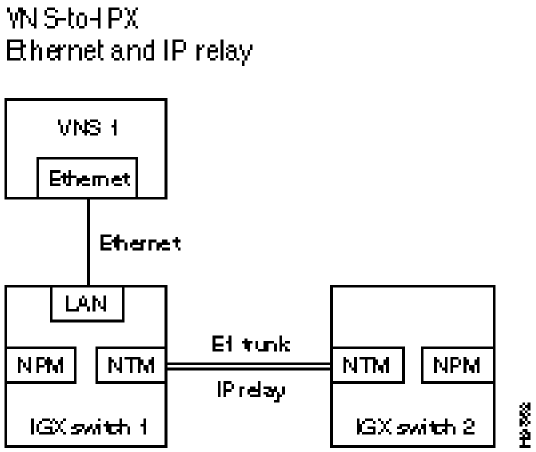
A VNS finally must be able to communicate with the nodes, e.g., the Nodal Processor Module (NPM) in an IGX switch (or NPC in an IPX switch), in its area. (Nodal Processor Modules are commonly referred to as Network Processor Modules.) The VNS-IGX interface provides IP connectivity used for exchanging IP messages between the VNS and both local and remote nodes.

These IP based messages are exchanged for the following purposes:

- Exchange circuit build commands and responses.
- Report circuit/port/card status to the VNS. The VNS needs to be informed of all the interface outages so that it can clear all the calls that go through those interfaces outages.
- Exchange heartbeat messages. The VNS needs to detect when the node or has gone out of service so that it can clear all the calls that go through the downed equipment.

The VNS issues commands, such as build or remove a circuit, through its ethernet connection. These messages are typically between the VNS and the NPM (or NPC) and use the message network and protocols already built into Cisco WAN switching networks. When the VNS communicates with a remote node, i.e., a node in its domain to which it does not have a direct Ethernet connection, it uses IP Relay, a Cisco proprietary messaging protocol. With IP Relay, the local node, e.g., the IPX’s NPC, acts as a router which relays the message, an IP packet, to the remote node’s NPM. Figure 1-8 illustrates a VNS with 2 nodes in its domain. It is directly connected to IGX switch 1, and communicates with IGX switch 2 using IP Relay.

Figure 1-8 VNS to Node



VNS to StrataView Plus Workstation

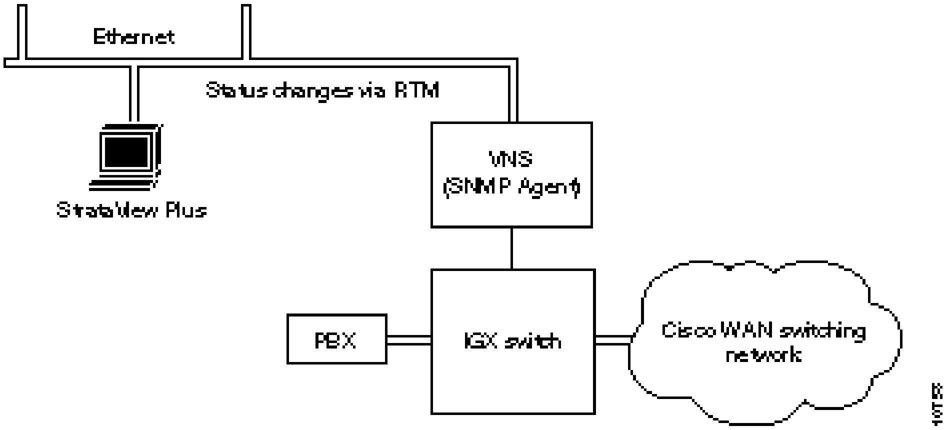
The VNS communicates with the StrataView Plus Network Management System primarily to provide status information. StrataView Plus processes and logs all traps reported by the VNS. The VNS, which receives and process traps from the IPX, uses the Cisco Robust Trap Mechanism (RTM) to send SNMP Traps to the StrataView Plus workstation. As shown in Figure 1-9, the VNS is typically connected to an StrataView Plus workstation through an Ethernet connection.

Note If the SV+ Workstation is collecting statistics, it is recommended that it not be connected to the same Ethernet segment as the VNS. In this case, the SV+ Workstation should be remotely located from the VNS and its co-located node.

HP OpenView, running with StrataView Plus, also provides a menu option to check the status of the D-channel and SPNNI-channel signaling channels. The D-Channel Status and SPNNI-Channel Status windows are described in Appendix B, Troubleshooting.

Since the VNS processes traps, it is registered as a SNMP manager in the Cisco WAN switching network. This leaves room for 7 Cisco StrataView Plus systems in the network.

Figure 1-9 VNS to StrataView Plus Workstation



VNS Network Icons

VNS icons are added through a manual configuration procedure to the StrataView Plus network topology maps. The icons can represent both the active and standby VNSs in a redundant pair. This icon shows only the existence of the VNS. The VNS icon is only visible on the StrataView Plus workstation where it was added.

StrataView Plus does not manage the VNS object. StrataView Plus does, however, receive SNMP Traps from the VNS and will display the status of the VNS with different colors as follows:

Green	Normal
Yellow	Minor alarm
Red	Major alarm
Brown	VNS unreachable

When a D channel fails or a failure is cleared, the node (IGX or IPX switch) will send SNMP traps to the VNS. The VNS processes these traps and generates a trap which it sends to StrataView Plus. (The D channel trap processing only occurs for the DPNSS protocol because the QSIG protocol already has a mechanism in place to handle D channel failures.) StrataView Plus will display the alarm and change the VNS icon color in the topology map.

The procedure for adding a VNS icon to StrataView Plus is described in Chapter 6 in the section, Adding a VNS Object to the SV+ Topology Maps.

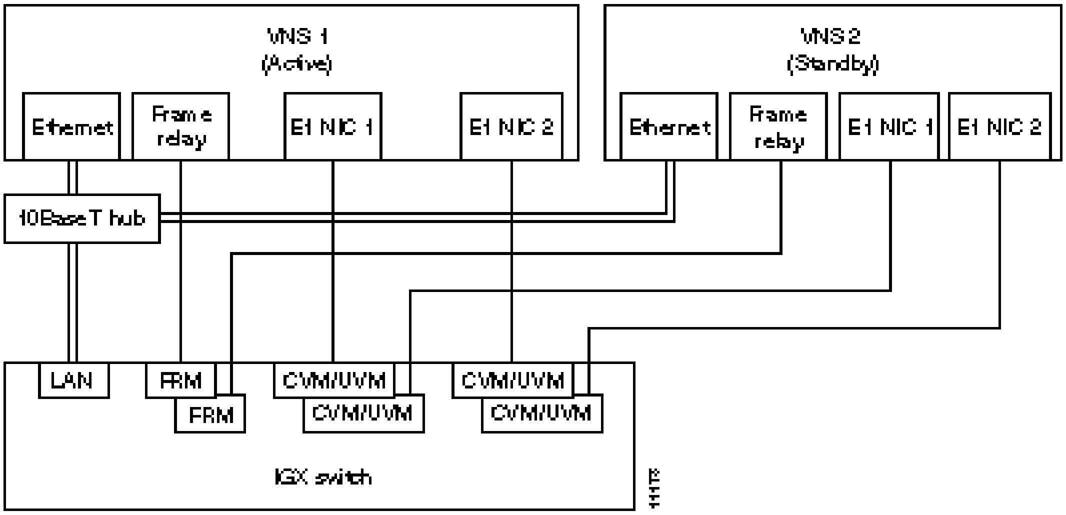
Redundant Pairs

Each VNS domain can be serviced by a VNS redundant pair, that is a VNS system. As shown in Figure 1-10, one VNS is configured as the active, the other is configured as standby. The redundant pair of VNSs are connected over an ethernet for the following functions:

- To resolve their redundancy roles
- For the active VNS to update the standby VNS
- For the standby VNS to check the sanity of the active VNS

The VNSs will change roles, i.e., switchover, when the active VNS is no longer in normal operation or when the network operator changes its mode through the CLI. The former case will be detected by the standby VNS missing RR Keep Alive messages from the active VNS; the later case is indicated by the SNMP SET on the VNS role MIB message received from the CLI. When a switchover occurs, existing SVC calls created by the active VNS will be cleared, PBX-to-VNS signaling PVCs will be switched over to the newly active unit, which will assume the same provisioning and configuration as was maintained by the previous active VNS.

Figure 1-10 VNS Redundant Pair



Although there are two E1 NICs installed in every VNS, they both do not have to be connected to the node. And although Figure 1-10 shows the active and the standby VNSs connected to different FRM cards, they do not have to be. They could be connected to different physical ports on the same card. (A CDP on an IPX switch has only one physical port.) The VNSs are typically connected to one another and to the node through a 10BaseT ethernet hub.

CVM Redundancy

The CVM redundancy feature provides optional VNS-based redundancy that is not based on normal CVM-based redundancy. With normal CVM-based redundancy, each E1 NIC card in a VNS has to be connected through a Y-cable to two CVM (or UVM) cards in the node. So theoretically to provide redundancy for all the nodes CVM cards attached to the VNS, a redundant pair of VNSs with 4 E1 NIC cards would require 8 CVM ports.

The VNS CVM redundancy feature eliminates the need for redundant CVM (or UVM) ports attached to each E1 NIC card. This feature, which is enabled or disabled in the VNS Configuration Interface, processes CVM card failure SNMP Traps from the node. When a CVM fails, the VNS receives a Trap. The VNS determines if the failed CVM is attached to a VNS E1 NIC. If the failed CVM is attached to the VNS, and the standby VNS is up and not in a failed state, the VNS will trigger a switchover to the redundant standby VNS.

Note The CVM Redundancy feature applies to UVM cards as well.

Configuration and Provisioning

Before the Voice Network Switching network can provide SVCs in response to a call from a PBX, the individual VNSs must be both configured and provisioned.

VNS configuration includes:

- Setting the VNS up for the local environment.
- Configuring PVCs between the PBX E1 PRIs and the VNS.
- Configuring PVCs between every VNS in the network. (This step is only necessary when there are multiple VNS areas.)

Provisioning, which is done mainly through the VNS Configuration Interface, a command line interface (CLI), includes the following tasks:

- Adding cards to an IGX switch, configuring the card, and entering the information to the VNS's service database.
- Configuring ports and entering the information in the VNS database.
- Assigning addresses to B channels (bearer) channels on the E1 PRI.
- Propagating new addresses (or prefixes) to other VNSs.

Network Addressing

The VNS command line interface allows you to assign address prefixes of up to 30 digits for a VNS area, and individual addresses at a UNI port of up to 40 digits. These addresses identify the end-users participating in call attempt as the called party or calling party. These addresses are a telephone-number-like format and assigned according to the VNS-user's numbering plan.

Wildcard Addressing

The VNS allows the use of wildcards (*) when configuring addresses and address prefixes in a network. This simplifies addressing and speeds up call routing. In addition, a wildcard can be used to replace a pattern of digits for situations where the addresses originating from or destined to a specific port or service area require a common transformation. Wildcard addressing is described further in Chapter 7, Understanding the VNS Configuration Interface.

Numerical Sorting of Addresses

Configured addresses are stored as Address Information records in the VNS Database. These records are displayed in descending order with the largest numerical address displayed first. Thus an Address Information record of 8000 is displayed for 7999 which is displayed before 900, etc. There is further information about Address Information records in Chapter 7 in the section Address Information.

Address Screening

The VNS allows you to screen addresses, that is, filter calling party and called party numbers. Using the VNS Configuration Interface, you can create lists of calling party (source addresses) or called party (destination addresses) which you will either allow or disallow on a per-UNI-port basis. There is further information about address screening in Chapter 7 in the sections Address Screening Information and Screening Type Information.

Address Translation

The VNS provides address (that is, number) translation to route public network telephone numbers over a VNS private networks. This translation feature can be used to translate a public number to a private number for Break-In and a private number to a public number for Break-Out. Number translation is configured with the VNS Configuration Interface and is described further in Chapter 7 in the section Transformation Rules Information. The Break-Out/Break-In (BOBI) feature is described in this chapter in the section, Break-Out/Break-In Feature.

VNS Database

The VNS Configuration Interface is a series of menus that are used to configure and provision the VNS. When a menu is completed and saved, it becomes a record in the VNS database, which is stored on the VNS disk. You can use the VNS Configuration Interface to browse the database as well as to modify it.

Database Integrity

The VNS provides a database integrity mechanism to allows you to have confidence that the VNS database is intact and uncorrupted. The database integrity mechanism uses checksums on individual records in the VNS database to detect incomplete database, a partial database, or corrupt fields in database records.

The VNS database integrity is checked during the following operations:

- When the VNS is initialized
- When the database is modified through the Configuration Interface
- Before the database is backed up
- Before the database is copied to a standby VNS in a redundant pair

- When the Configuration Interface is invoked
- When an operator uses the Validate Data Base option on the VNS Configuration Interface

Caution .Database corruption that occurs on a power failure can be corrected only by restoring the database from a backup. The database integrity mechanism will only detect such a failure; it can not prevent or recover from it. Therefore, you should perform database backups on a regular basis. The procedure for backing up your database is described in Chapter 8 in the section Saving and Restoring the VNS Database.

In a redundant pair of VNSs, the database checksums files are also updated from the active VNS to the standby VNS along with the database.

There is further information about the VNS Configuration Interface Validate Database option in Chapter 7 in the section Validate Data Base.

Configuration Save and Restore

Configuration and provisioning information is saved on the VNS in a database file. The VNS provides commands for saving this database file in a flat-file format which can be transferred (FTPed) to another platform, such as a SV+ Workstation, as a backup or archive file in case the current database is corrupted. (Note that the VNS Configuration and Restore procedure is not the same as the SV+ Config Save and Restore feature.) This backup database can then be restored on the VNS. Chapter 8 contains procedures for using the Configuration Save and Restore feature.

Multihomed E1 Links

Multihoming is the provisioning of two or more links to the same end-user CPE. A site may be multi-homed to multiply the bandwidth capacity to meet increased traffic requirements. In addition to increased bandwidth, multihoming provides the following benefits:

- Increased hit-ratio of successful calls
- Load-sharing
- Backup circuits (site redundancy), etc.

Figure 1-11 illustrates a simple example of multihoming. In this case, CMV1 on IGX switch 1 and CVM2 on IGX switch 2 are multihomed to one another. Both CVM ports have been configured for the same port address, Address 100. (Although in this example both CVM ports are shown connected to the same PBX, they could be connected to separate PBXs; although this is typically not done.)

Figure 1-11 Multihoming

When the Far-End places a call to Address 100, the VNS will process the call. When the VNS detects a call to address 100, i.e., to a multihomed port, it will step through an algorithm to determine which CVM port to use to reach Address 100. This algorithm takes into consideration the prevailing conditions of each port and other criteria, such as:

- Port with least errors.
- Port with most bandwidth available.
- Port with the least amount of transients (that is the fewest amount of calls to it).
- Or a round-robin alternation between each port. Round-robin will provide traffic balancing for a pair of multihomed ports. When it is selected, the VNS will alternate calls between the ports as well as using current prevailing conditions, such as a port being down or not having the bandwidth available for a call at that time.

These selection criteria are specified during the configuration of the port with the VNS Configuration Interface. The user-configurable parameters include:

- Select Policy used to specify either the Port with least errors, the Port with most bandwidth available, the Port with least amount of transients, or a simple round-robin alternation pattern.
- Weightage provides a weight for the selection policy when there are more than one type of Select Policy applied to each multihomed pair.

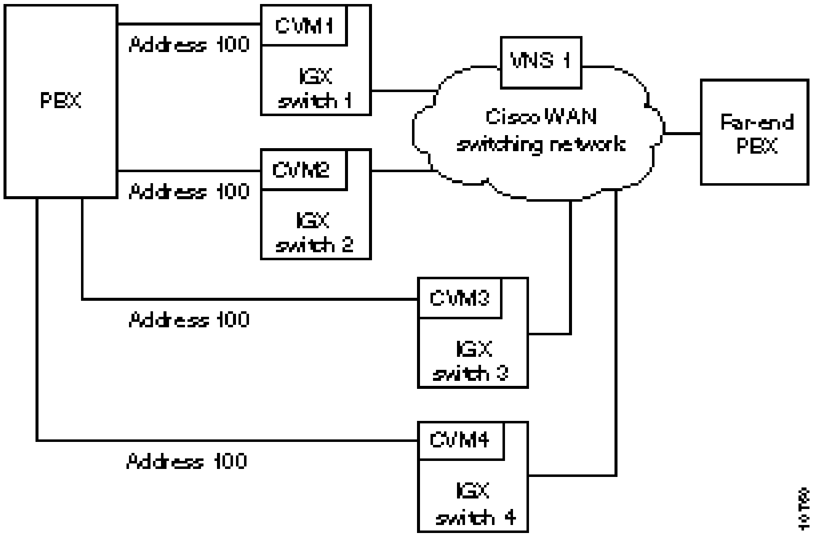
UNI ports are always multihomed in pairs. If the IGX switch 1 CVM1 is multihomed with the IGX switch 2 CMV2, it implies that CVM2 is also multihomed with CVM1. But CVM2 could be independently multihomed with CVM1, using a different set of port selection criteria; therefore each pair of multihomed ports will require two records in the VNS database.

Multihoming to a Single Primary Port

A typical use of multihoming is to multihome several ports to a single primary port. In Figure 1-12 for example, three separate ports will be multihomed to a single primary port. In this case, the primary port will be IGX switch 1 CVM1. There will be three multihomed pairs:

1. IGX 1 CVM1 is multihomed to IGX 2 CVM2
2. IGX 1 CVM1 is multihomed to IGX 3 CVM3
3. IGX 1 CVM1 is multihomed to IGX 4 CVM4

Figure 1-12 Multihoming to a Single Primary Port



Note Note: you could not multihome IGX 1 CVM1 to IGX 2 CVM2, IGX 2 CVM2 to IGX 3 CVM3, and IGX 3 CVM3 to IGX 4 CVM4 to achieve the same results.

When the Far-End places a call to Address 100, the VNS will process it. After determining that it is a call to address 100, i.e., to a multihomed port, the VNS will step through an algorithm to determine which CVM port to use to reach Address 100. In this case, when determining the CMV port to route the call through, the VNS would step through all the selection criteria for each of the multihome pairs. Then it would route the call through the appropriate port.

Multihoming configuration parameters are discussed further in Chapter 7 in the sections Multihome Port Configurations and Multihome Policy Configurations.

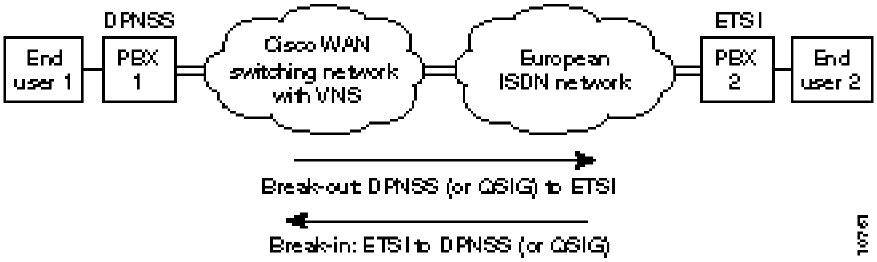
Break-Out/Break-In Feature

Voice Network Switching supports the Break-Out/Break-In (BOBI) feature. BOBI allows interworking between Euro ISDN (ETSI) and DPNSS or between ETSI and QSIG. As shown in Figure 1-13, this feature allows a user connected to a DPNSS (or QSIG) PBX to call out (Break-Out) to the European public ISDN network through the Cisco WAN switching. Conversely, it also allows a user on the European public ISDN network to call in (Break-In) to a user connected to a DPNSS (or QSIG) PBX through the Cisco WAN switching. As described in the section, Address Translation, the VNS address translation feature can be used to transform public network address formats to VNS private network formats, and vice versa.

BOBI allows calls to be routed long distances using private facilities. BOBI calls can:

- Originate within or outside the private network
- Can terminate within or outside the private network
- Can originate and terminate outside the private network

Figure 1-13 Break-Out/Break-In Feature


DPNSS
End user 1
PBX 1
Cisco WAN switching network with VNS
European ISDN network
ETSI
PBX 2
End user 2
Break-out: DPNSS (or QSIG) to ETSI
Break-in: ETSI to DPNSS (or QSIG)

With the BOBI feature, there are six types of connections:

- DPNSS to DPNSS (as was available with Release 1.0)
- DPNSS to ETSI (Euro-ISDN) (Break-Out)
- QSIG to ETSI (Euro-ISDN) (Break-Out)
- ETSI (Euro-ISDN) to DPNSS (Break-In)
- ETSI (Euro-ISDN) to QSIG (Break-In)
- ETSI to ETSI

The VNS maps the DPNSS to ETSI (Euro-ISDN) according to BTNR 189I Interworking between DPNSS1 and ISDN Signaling Systems, December 1993. The VNS maps QSIG to ETSI according to ETS 300 102 and ETS 300 172.

Call Detail Records

The VNS creates and stores Call Detail Records (CDRs) for voice (or data) SVCs that it establishes. CDRs are created at the originating-end VNS once a call is set up. CDRs identify whether it is a voice or data call, the calling and called numbers, the local and remote node names, date and timestamp, elapsed time in seconds and Call Failure Class (that is, cause codes).The CDRs are stored in a file and retrieved at a fixed interval by the StrataView Plus workstation or by any server attached to the Ethernet. The VNS Configuration Interface allows you to configure CDR File Counts and CDR File Intervals which define the number of CDR files generated and the interval for which a CDR file will be generated.

There is further information about Call Detail Records in Appendix C, Call Detail Records.

Technical Assistance

If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco’s Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Dial-In Support

Cisco recommends that a modem be attached to the VNS to provide remote access for our Product Support and Technical Assistance Center (TAC). With an attached dial-in modem, Product Support can log in remotely and resolve potential problems. (Modem access is required during field trials of Voice Network Switching.) Appendix D contains further information about Dial-In Support.

VNS Hardware and Software

The currently available hardware and software options of the Voice Network Switching (VNS) are listed in Table 1-2.

Table 1-2 VNS Models and Options

VNS Model Numbers	Description
VNS-AC-E (or -DC-E)	Voice Network Switching (VNS) system (newer models) Redundant pair of VNS servers Ordering options are provided for AC or DC systems
Voice Network Switching (VNS) Feature Software	
VNS-SW-QSIG-2.1	QSIG release 2.1 protocol feature
VNS-SW-QSIG-3.0	QSIG release 3.0 protocol feature
VNS-SW-DPNSS-2.1	DPNSS protocol feature
VNS-SW-Q931A-2.1	Q931A (Japanese ISDN) protocol feature
VNS-SW-CAS-2.2	VNS QSIG protocol modified to work with the IGX UVM with model B firmware (switched software release 8.5) and provide CAS Voice Switching. See Appendix I, Channel Associated Signaling Voice Switching, for details about this feature.
Voice Network Switching (VNS) Additional Port License	
VNS-LIC10-PRI	CDP/CVM T1/E1 port software license--additional 10 ports

Site Requirements

This chapter provides information about the site requirements required installing a VNS system. Normally, the VNS is co-located with an IGX or IPX switch and installed in the same rack; the node's rack requirements are covered in the appropriate *Cisco IGX 8400 Series Installation* or *Cisco IPX Installation* publications.

This chapter contains the following sections:

- Electrical Power Source
- Environment
- Rack Requirements
- Terminal
- 10BaseT Ethernet Hub

Electrical Power Source

An AC or DC power source must be easily accessible within 6 feet of the VNS. The VNS must be powered from a dedicated branch circuit. An easily accessible disconnect device should also be included in the facility wiring.

Caution Cisco recommends that a battery-backup or uninterruptable power source (UPS) be provided for the VNS in case of power failures.

AC Power

The AC Power input must meet the requirements listed in Table 2-1. The VNS automatically adjusts to input voltages within its range.

Table 2-1 AC Power Input

	Minimum	Nominal	Maximum
Input voltage	90 VAC	120/208 VAC	264 VAC
Line frequency	47 Hz	50/60 Hz	63 Hz

DC Power

The DC power input must meet the requirements listed in Table 2-2.

Table 2-2 DC Power Input

	Minimum	Nominal	Maximum
Input voltage	-40 VDC	-48 VDC	-60 VDC

Ground

DC Ground a 48V DC power feed, if used, on the positive 48 volt and safety ground pins. Ensure that the VNS frame, and all other frames, are attached to an isolated ground connection.

The nominal operating voltage of the DC-model VNS is –48V DC. The DC source should be capable of supplying 5 amperes. Only power supplies complying with SELV requirements in EN60950 may be connected to the -48 VDC input.

AC An insulated grounding conductor that is identical in size to the grounded and ungrounded branch circuit supply conductors is to be installed as part of the branch circuit that supplies the device. This conductor has green insulation with yellow stripes.

Circuit Breakers

A 15A DC circuit breaker is recommended for the 48 VDC power source which supplies DC power to the DC version of the VNS. In North America, this circuit breaker should conform to NEC (ANSI/NFPA 70) and CEC (Part 1, C22.1) for protection against excess currents, short circuits, and earth faults.

A 20A AC circuit breaker is recommended for the 120/208 VAC power source which supplies AC power to the AC version of the VNS. In North America, this circuit breaker should conform to NEC (ANSI/NFPA 70) and CED (Part 1. C22.1) for protection against excess currents, short circuits, and earth faults.

Environment

The site must be capable of maintaining a maximum ambient temperature of 50º C while the system is operating (recommended range is 20° C to 30° C). Cooling airflow direction is from front to rear.

Rack Requirements

You can mount the VNS into standard 19” rack or a 23-inch racks. (*Cisco IGX 8400 Series Installation* or *Cisco IPX Installation* documents have information about Cisco-supplied cabinet.) The VNS is 5 1/4 inches high. The VNS has front mounting flanges and is shipped with attachable rear and mid-mounting brackets.

19-Inch Rack

You can mount the VNS into a standard 19-inch rack (17.75 “ +0.12 and -0.00 inches between the rails), such as Cisco-supplied cabinet, which contains two front and rear mounting rails.

23-Inch Rack

To install a VNS in a 23-inch rack, you need to provide adapter brackets to adjust the width of the rack opening to 17.75 (+0.12 and -0.00) inches. Adapter brackets for installation of 19-inch equipment are commercially available.

Center Mount Rack

The VNS chassis contains two sets of holes, with attached PEM nuts, for the installation of mid-mounting brackets. These sets of holes are set back, 5 and 10 inches, from the front of the unit.

Terminal

If you are using a terminal to configure your VNS, communication parameters should be set for VT100, 9600 baud, parity none, 8 bits, and 1 stop bit.

Note During field trials, Customer Service requires that a modem be attached to the VNS to provide them with dial-in access. Appendix D contains further information about Dial-In Support.

10BaseT Ethernet Hub

Installation of the VNS typically requires an additional 10BaseT hub to connect the VNS’s Ethernet port to the IGX or IPX switches’ LAN port. The10BaseT hub must be purchased separately.

Unpack and Inspect the VNS

This chapter describes the contents of your VNS system shipping package and the physical characteristics of the VNS front and back panels. It includes the following sections:

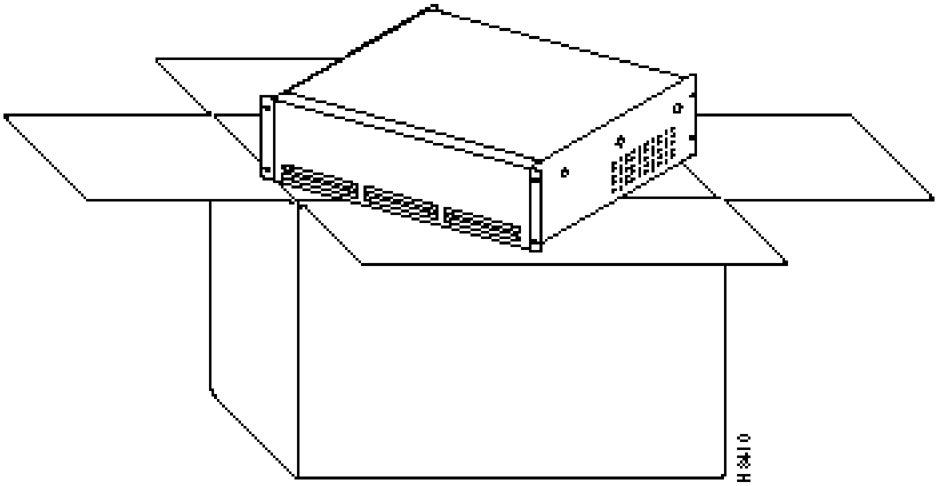
- Unpack the VNS
- Examine the VNS
- Observe Safety Measures

Unpack the VNS

If the shipping container is damaged, or if any of the various shipping indicators show improper handling of the container, contact your local shipping representative.

Figure 3-1 illustrates the unpacking of the VNS.

Figure 3-1 Shipping Contents



The shipping container contains:

- VNS Processor (Either VNS-AC-E or VNS-DC-E)
- AC power cord
- 10Base-T Ethernet Cable
- RS449 to V.35 cable for Frame Relay Card (part number 72-1415-01)
- RS449 to X.21 cable for Frame Relay Card (part number 72-1416-01)
- 2 Pair 75-Ohm E1 coaxial cables (one pair for each E1 Network Interface Card)
- Rear-mounting brackets and fasteners (2 sets) for mounting
- Optional Motorola V.34R Modem

And a publication:

- *Cisco Voice Network Switching Installation and Operation*, Release 3.0

Note The VNS software is factory-installed. Software upgrades are made available on Cisco Connection On-line (CCO). Contact Cisco Customer Service to find out how to get software upgrades for your product.

Note The RS449 to V.35 cable or the RS449 to X.21 cable are ordered independently.

Examine the VNS

This section provides descriptions the front and rear-panels of the two VNS models:

- VNS-AC-E
- VNS-DC-E

The external physical differences in the VNS models are pointed out in this section.

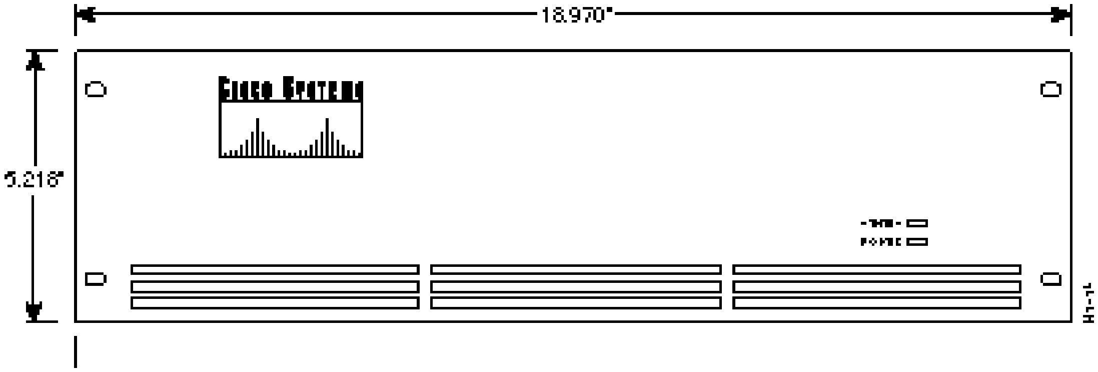
VVNS-AC-E and VNS-DC-E Front Panel

The VNS-AC-E or VNS-DC-E front panel, illustrated in Figure 3-2, are identical. They display the Cisco logo, the product name, and have the following two indicators:

- Power-On indicator indicates that the power is on.
- Status indicator is a tri-colored LED that indicates system status. The status indications are:
  - Off–VNS is off.
  - Blinking red–Unit booting, unit shutting down, factory installed soft-switch cable missing.
  - Red–Unit temperature gets too high.
  - Green--Unit powered on and ready.
  - Yellow–Reserved for future use.

  These status indications apply to both the front- and rear-panel Status LEDs.

Figure 3-2 VNS-AC-E or VNS-DC-E Front Panel



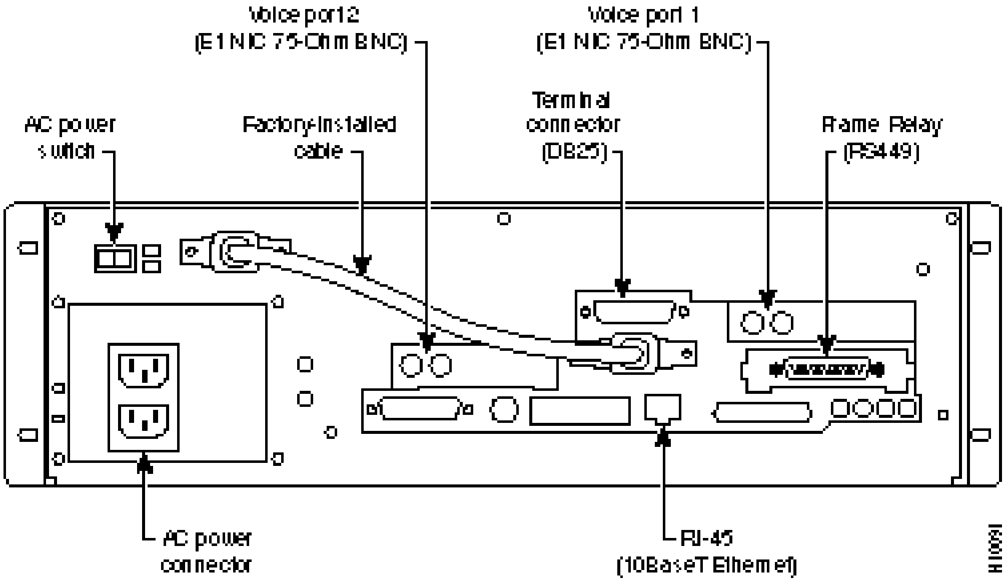
VNS-AC-E and VNS-DC-E Rear Panels

This section contains descriptions of the VNS-AC-E and VNS-DC-E rear panels.

VNS-AC-E Rear Panel

The VNS-AC-E contains the components and connectors shown in Figure 3-3. The Power On/Off Switch is to the left of the AC-Power Input connector.

Figure 3-3 VNS-AC-E Rear Panel



The VNS-AC-E has the following connectors and switches:

- AC Power Switch providing both graceful and emergency shutdown capability
- AC Power Connector (Single IEC 20)
- Power-On LED lights green when there is power to the unit
- Status LED providing the same indications as the front-panel Status LED
- Frame Relay Card RS449 connector
- Voice port 1 (E1 Network Interface Card) 75-ohm BNC connectors
- Voice port (E1 Network Interface Card) 75-ohm BNC connectors
- Ethernet Port RJ-45 Connector (referred to as a 10BaseT connector)
- Two Serial Port DB25 Connectors (for attaching a local terminal)

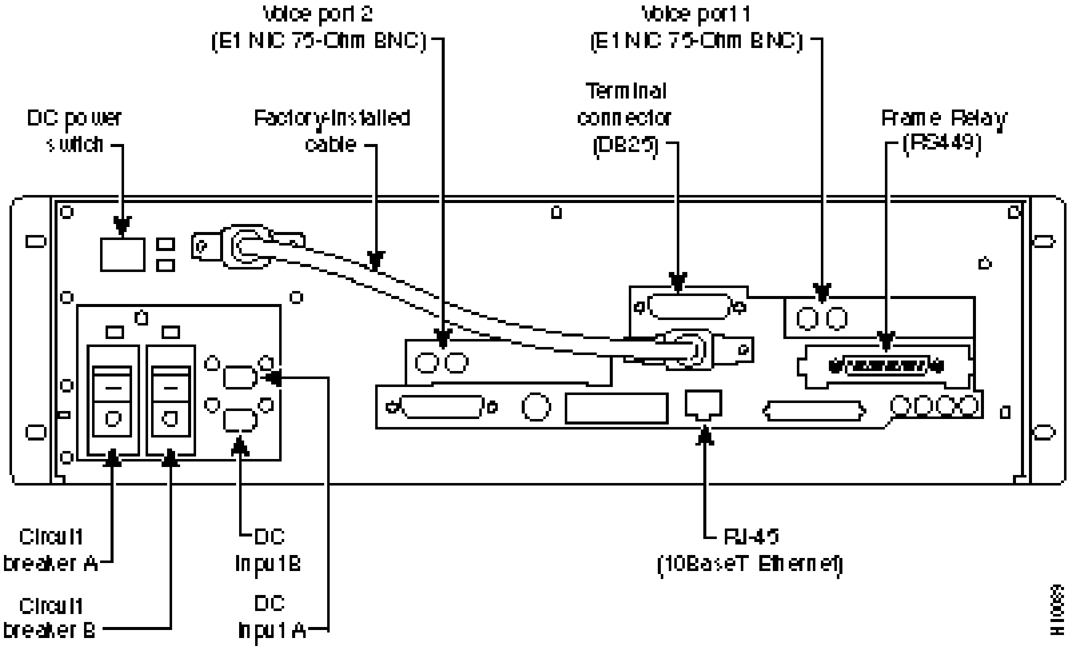
Note The factory-installed cable shown in Figure 3-3 is known as the soft-switch cable. It is installed from one of the DB25 connectors to a DB15 connector next to the AC power switch. If it is not installed, the Status LEDs will blink red.

Note Unlabeled connectors are not used in VNS applications.

VNS-DC-E Rear Panel

The VNS-DC-E rear panel contains the components and connectors shown in Figure 3-4. As shown, the VNS-DC-E has inputs for two DC power inputs (DC Input A and DC Input B). Typically these DC inputs are from separate DC power sources to provide for protection against a DC power source failure. Each DC input has its own circuit breaker.

Figure 3-4 VNS-DC-E Rear Panel



The VNS-DC-E has the following connectors and switches:

- DC Power Switch providing both graceful and emergency shutdown capability
- Two DC Power Connectors (Euro-style plugable terminal connector receptacles)
  (Phoenix P/N DFK-MSTB 2,5/3-GF-5.08)
- Power-On LED lights green when there is power to the unit
- Status LED providing the same indications as the front-panel Status LED
- Two circuit breakers:
  - Breaker A GOOD green LED is on when circuit breaker A is not tripped, off when circuit breaker is tripped
  - Breaker B GOOD green LED is on when circuit breaker B is not tripped, off when circuit breaker is tripped
- Frame Relay Card RS449 connector
- Voice port 1 (E1 Network Interface Card) 75-ohm BNC connectors

- Voice port (E1 Network Interface Card) 75-ohm BNC connectors
- Ethernet Port RJ-45 Connector (referred to as a 10BaseT connector)
- Two Serial Port DB25 Connectors (for attaching a local terminal)

Note Unlabeled connectors are not used in VNS applications.

Note The factory-installed cable shown in Figure 3-4 is known as the soft-switch cable. It is installed from one of the DB25 connectors to a DB15 connector next to the DC power switch. If it is not installed, the Status LEDs will blink red.

E1 Network Interface Card LEDS

The only status indicators on the rear panel of the VNS are the four LEDs on each E1 NIC. Figure 3-5 illustrates the location and the color of these LEDS. Table 3-1 describes what each LED indicates.

Figure 3-5 E1 NIC LEDs

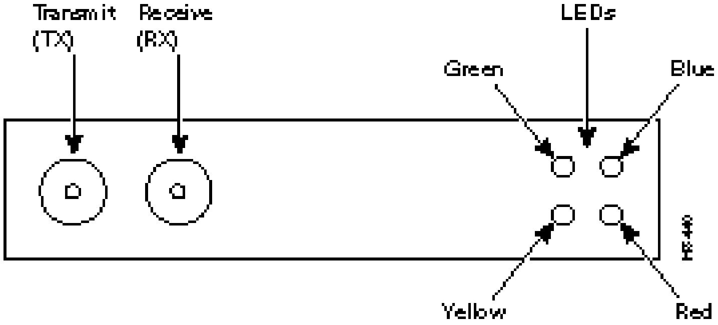


Table 3-1 E1 NIC LEDs

LED	Function
Green	Link is active.
Blue	Loss of sync.
Red	Loss of carrier.
Yellow	Remote alarm.

Observe Safety Measures

To ensure safe performance as well as to maintain the integrity of your VNS, please observe a few safety measures as you proceed with this installation.

- Do not modify the internal or electrical assembly of VNS equipment.
- Protect the VNS from overheating; ensure that openings in the equipment are not blocked or covered. Never place the unit near any source of heat.
- Handle with care; rough treatment may damage sensitive components.
- Always turn off the power to the VNS before moving it.

Rack Mounting the VNS

This chapter describes three mounting methods for positioning your VNS in a rack.The different mounting procedures are described in different sections. This chapter contains the following sections:

- Rack Types
- Rack Mounting the VNS-AC-E or VNS-DC-E
- Rack Mounting the Redundant VNS

Caution Installation should be performed by authorized personnel only.

Rack Types

You can flush mount the VNS into a 19- or 23-inch rack, or you can center mount it. For either mounting method, you need to allow enough clearance space at the front of the rack to enable removal and replacement of the VNS.

19-Inch Rack

You can mount the VNS into a standard 19” rack (17.75” +0.12 and –0.00 inches between the rails), such as Cisco-supplied cabinet, which contains two front and rear mounting rails. The VNS has a front mounting flange and rear-mounting brackets that will align with the mounting rails.

23-inch Rack

To use a 23-inch rack for INS installation, you need to provide adapter brackets to adjust the width of the rack opening to 17.75 (+0.12 and -0.00) inches. Adapter brackets for installation of 19-inch equipment are commercially available.

Center Mount Rack

The VNS can be mid-mounted by using the holes at the sides of the VNS chassis.

Rack Mounting the VNS-AC-E or VNS-DC-E

Caution The VNS is a single, enclosed unit and weighs approximately 60 lbs. Use two people when it is necessary to lift it into place.

To rack mount the VNS-AC-E or VNS-DC-E, follow these steps:

Step 1 From the front of the rack, slide the VNS-AC-E or VNS-DC-E into the rack and secure the holes in the front mounting flanges to the holes in the rack mounts.

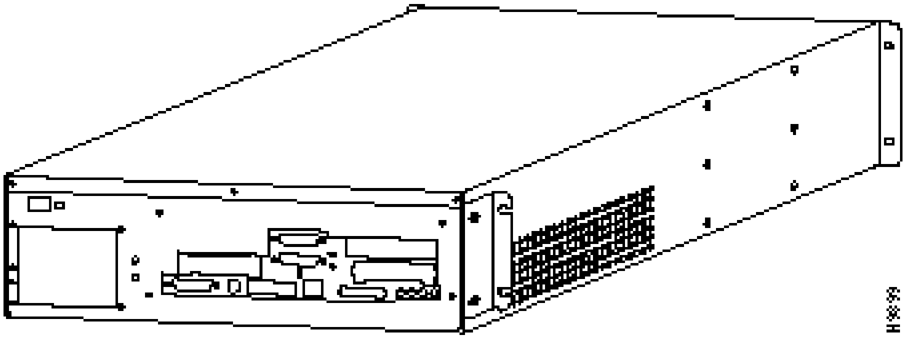
Step 2 From the rear of the rack, position the rear-mounting brackets, shown in Figure 4-1, on the outside of the VNS-AC-E or VNS-DC-E chassis.

Step 3 Loosely secure the rear-mounting bracket to the VNS-AC-E or VNS-DC-E chassis using the screws that were supplied.

Step 4 Secure the rear-mounting brackets to the rack's mounting posts.

Step 5 Tighten the four screws holding the rear-mounting brackets to the VNS-AC-E or VNS-DC-E chassis.

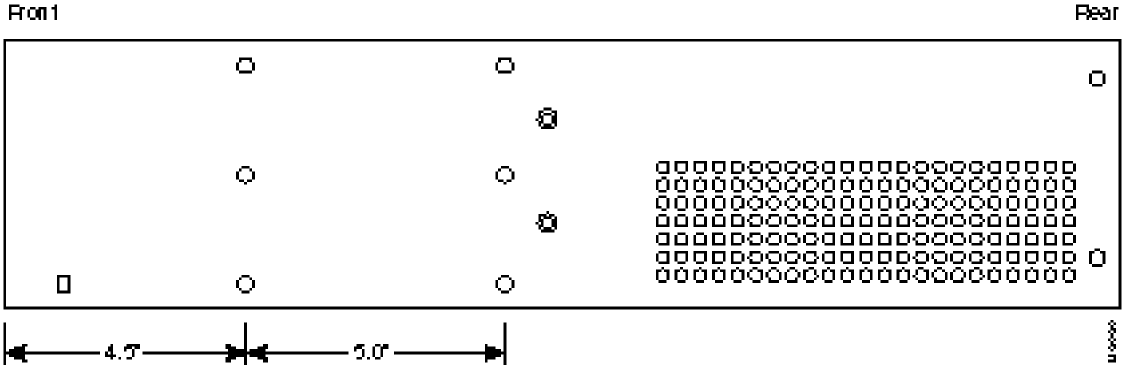
Figure 4-1 Rear-Mounting Brackets Attached to Chassis



To mid-mount the VNS-AC-E or VNS-DC-E, follow these steps:

Step 1 Attach the mid-mount right-angle brackets to the VNS-AC-E or VNS-DC-E chassis using the mounting holes shown in Figure 5-5. (Make sure to use the same set of holes, either 4.5-inch or 10-inch, on each side.)

Figure 4-2 Mid-Mounting Holes and Right-Angle Bracket



Step 2 From the front of the rack, slide the VNS-AC-E or VNS-DC-E into the rack until the Mid-Mounting brackets are up against the rack posts.

Step 3 Secure the holes in the Mid-mounting Right-Angle brackets to the holes in the rack mounts.

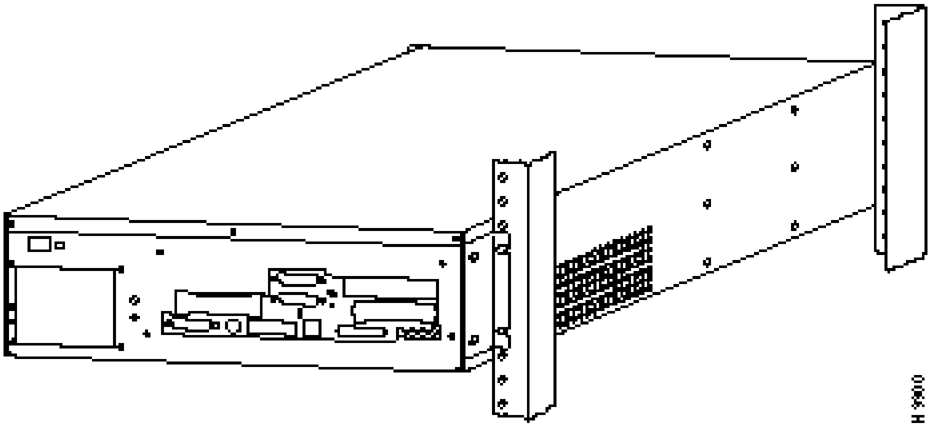
Step 4 From the rear of the rack, position the mid-mounting brackets on the outside of the VNS-AC-E or VNS-DC-E chassis.

Step 5 Loosely secure the rear-mounting bracket to the VNS-AC-E or VNS-DC-E chassis using the screws that were supplied.

Step 6 Secure the rear-mounting brackets to the rack's mounting posts.

Step 7 Tighten the four screws holding the rear-mounting brackets to the VNS-AC-E or VNS-DC-E chassis.

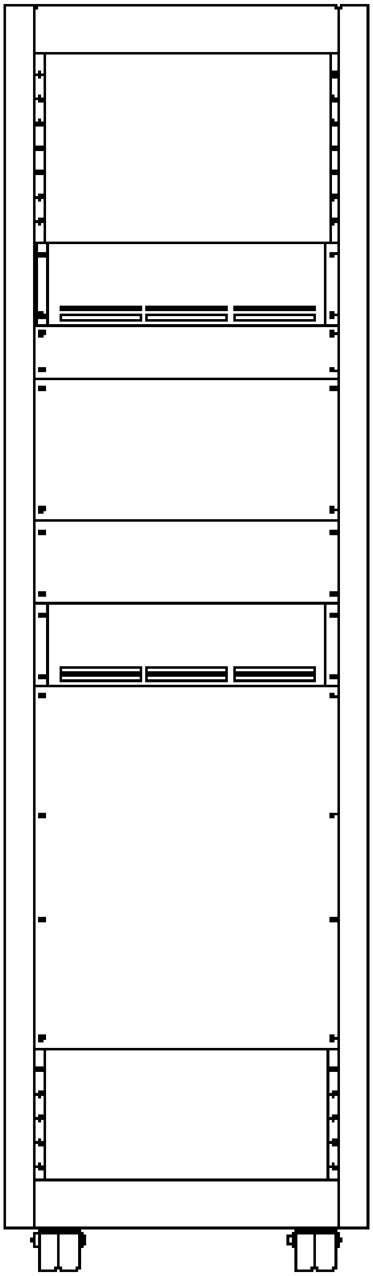
Figure 4-3 Rack-Mounted VNS



Rack Mounting the Redundant VNS

The redundant, or second VNS in a redundant pair, is rack mounted in the same rack as the IGX/IPX switch exactly like the first VNS. Figure 4-4 illustrates a redundant pair of VNS's in a typical rack.

Figure 4-4 VNS in Rack



Connecting Power to the VNS

This chapter assumes that your VNS is racked, cabled, and ready for startup. You are now ready to connect AC or DC power, turn on the VNS, and access a UNIX login prompt. Guidelines for VNS shutdown are also provided at the end of this chapter. This chapter includes the following sections:

- Connect AC Power to the VNS-AC-E
- Connect DC Power to the VNS-DC-E
- Connecting Power to a Redundant VNS
- Powering Up the VNS
- Shutting Down the VNS

Caution VNS power outages can result in service failures and can be difficult to recover from. Cisco recommends that the VNS always be connected to redundant power sources or a battery backup system.

Connect AC Power to the VNS-AC-E

The VNS AC power cord is designed to work with single-phase power systems. Appendix A, Cable Information, provides further information about the AC Power cable supplied with your VNS.

The AC-Power connector and the ON/OFF Switch are on the left-side of the rear panel as shown in Figure 5-1.

To connect AC power to the VNS-AC-E, follow these steps:

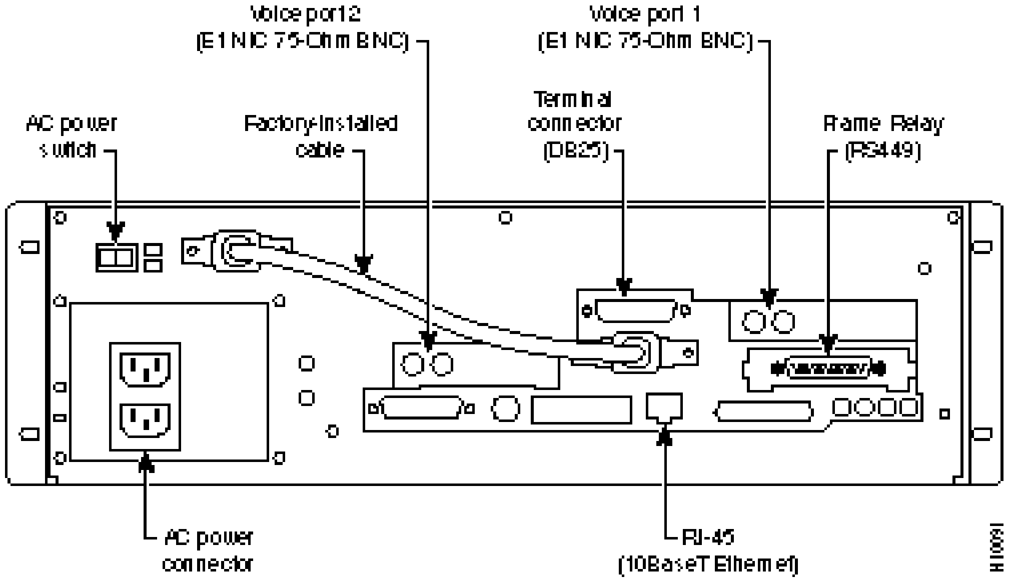
Step 1 Make sure the power switch is in the Off position, by pressing the side of the On/Off Switch labeled 0.

Step 2 Attach the power cord to the AC Input connector.

Step 3 Attach the other end of the power cord to the AC power source.

Step 4 Turn power on by pressing the side of the On/Off Switch labeled 1.

Figure 5-1 AC-Power Switch and Connector



Connect DC Power to the VNS-DC-E

The DC Input Connectors and On/Off Switches are on the rear panel as shown in Figure 5-2. The two DC Input connectors are EURO Block three-pin male receptacles. Female EURO mating connectors are provided in the VNS-DC accessories bag which was part of the shipping kit.

To connect DC power, follow these steps:

Step 1 Make sure that both DC power inputs are off by pressing the 0-side of their circuit breakers.

Step 2 Make sure the DC source is off.

Step 3 The cable from the DC-power source should have 3 insulated #14 AWG wires (stranded); the insulation should be stripped back 0.25” (6 mm) on each wire end, where you connect the female EURO connectors supplied in the accessories bag.

Step 4 Observe the way the polarized female EURO connectors will mate with the DC input connector. Insert each wire into the correct hole in the female Euro connector (see Figure 5-2). Secure each wire by tightening the screws in the connector. As you face the rear panel, both DC input connectors are oriented as follows:

Pin 1: -48 VDC, is on the left as you face the unit

Pin 2: Safety Ground

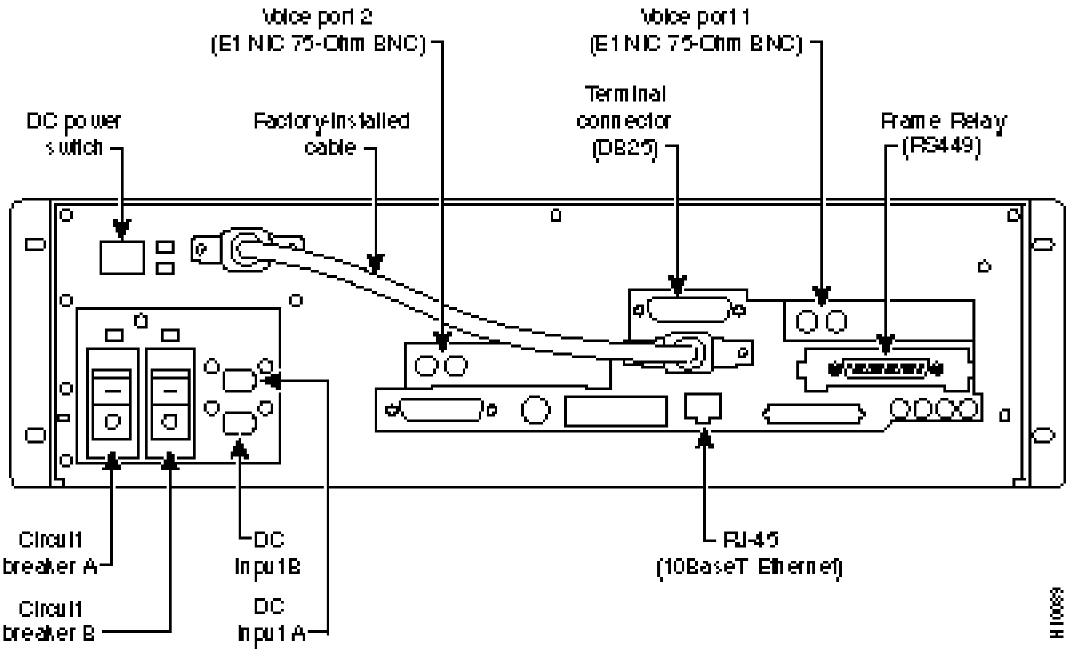
Pin 3: -48 VDC Return

Step 5 Insert one (or both) female EURO connectors now connected to the cable from the DC source into DC Inputs A and/or B.

Step 6 Turn on the DC source.

Step 7 Turn on DC power to the VNS by pressing the 1-side(s) of the DC circuit breakers, Power A, and/or Power B, as required. The press the 1-side of the DC power switch.

Figure 5-2 DC Power Switches and Connectors



Connecting Power to a Redundant VNS

You connect power to the redundant VNS, or second VNS in a redundant pair, exactly as you did for the first VNS.

Powering Up the VNS

The first time you power on your VNS, you should perform the procedures described in the next chapter, VNS Interface Connections. These procedures include connecting a terminal to the VNS, connecting it to the IGX or IPX switch, and connecting it to a StrataView Plus workstation and creating a VNS Object on the StrataView Plus Maps.

Before turning on the VNS, it is a good idea to read through Chapter 6, VNS Interface Connections, and Chapter 7, Understanding the VNS Configuration Interface, to understand the sequence of operations that have to be completed to bring up a VNS system for the first time. Once either the DC- or AC-model VNS has been turned on with the On/Off switch, it will began to start running automatically. If a terminal has been connected, the UNIX login prompt appears at an attached terminal interface.

Shutting Down the VNS

Once the VNS is powered up, you must be careful how you shut it down. During the normal operation of VNS-AC-E or VNS-DC-E and the IGX or IPX switch, the VNS is typically not turned off. However, in the rare cases where it might be necessary to turn off the VNS, both AC or DC power switches provide for graceful or emergency shutdowns:

Graceful Shutdown

To gracefully shut down VNS-AC-E or VNS-DC-E, where VNS processes are stopped and the file system is protected, momentarily press the DC Power Switch. The graceful shutdown will take approximately 30 seconds.

Emergency Shutdown.

In an emergency situation where it is necessary to remove power from the VNS-AC-E and VNS-DC-E immediately, press and hold the Power Switch down for approximately 5 seconds. The VNS will shutdown without going through the 30-second graceful shutdown.

For the AC unit, the power cord inlet is the disconnecting device.

CHAPTER 6

VNS Interface Connections

This chapter describes making the interface connections between a VNS and the Cisco wide-area switch (IGX or IPX switch) and the Cisco StrataView Plus workstation. It includes the following sections:

- Physical Interfaces
- Connecting a Terminal
- Connecting the E1 NICs to the Node
- Connecting the Frame Relay Card to the Node
- Connecting to an Ethernet Segment
- Connecting the Redundant VNS
- Configuring the Node
- Synchronizing Time
- Ping the VNS
- Adding a VNS Object to the SV+ Topology Maps
- Removing the VNS Object From the Topology Map
- Adding VNS Users

Physical Interfaces

After you have rack mounted the VNS and connected the power, you must connect the physical interfaces to it. These interfaces, which are shown in Figure 6-1, are:

- Terminal
- Two E1 Network Interface Cards (Channelized E1), also know as Voice Port 1 and Voice Port 2
- Frame Relay Card (RS449 connector to either V.35 or X.21)
- Ethernet, 10BaseT

Note The Frame Relay Card is only connected to a node when there are multiple VNS service areas (or domains) in the WAN switching network.

Figure 6-1 VNS Physical Interfaces

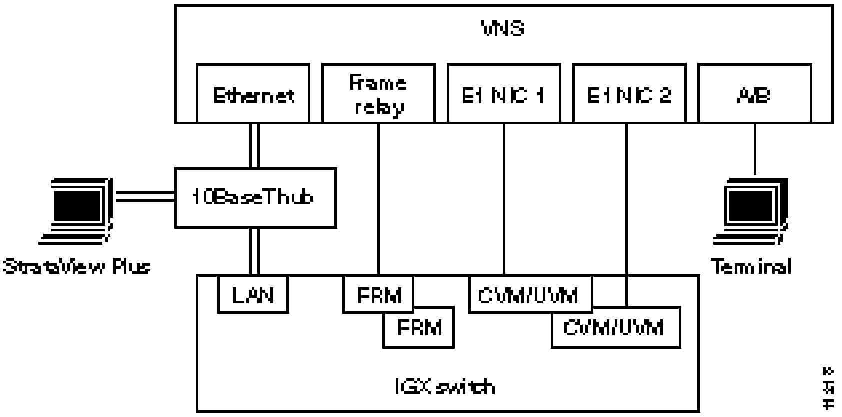
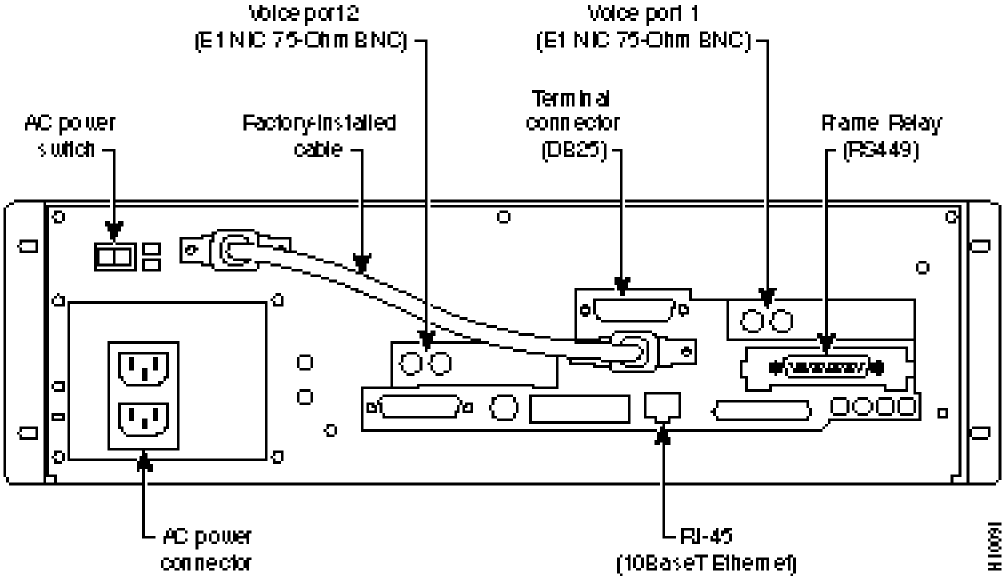


Figure 6-1 illustrates the VNS directly connected to an IGX switch. With an IGX switch, the Frame Relay Card is connected to an IGX's FRM, and the E1 NICs are connected to an CVM or UVM cards. If the directly connected node is an IPX switch, the Frame Relay Card would be connected to an FRP (Frame Rely PAD), and the E1 NICs would be connected to CDPs (Channelized Data PADs).

Figure 6-2 shows the location of the interface connectors for VNS-AC-E physical interfaces; the interface connectors are in the same location on a VNS-DC-E model.

Figure 6-2 VNS-AC-E Interface Connectors



Note Voice Port 2 may require BNC extenders to be able to access these connectors.

Connecting a Terminal

You can attach a terminal (or PC running a terminal emulation program, such as ProCom), to the VNS to perform some of the configuration locally.

Attach your terminal cable, typically a *null modem cable*, to the A/B (Terminal) connector on the VNS's back panel, as shown in Figure 6-2. This is an asynchronous ttya port on the UNIX-based VNS. Your terminal or PC and emulation software must be set to match the VNS's communication parameters:

- Terminal emulation for VT100
- 9600 baud
- Parity none
- 1 stop bit

Caution A terminal (or PC) which has been connected to a VNS Terminal port should not have its power recycled because this can cause the VNS to enter a different mode.

The VNS terminal port has been set up at the factory. If you have trouble displaying VNS files and menus cleanly, you might reset the following parameters:

```
stty rows 24
stty erase ^h
setenv TERM vt100
```

Also if you are connected to the VNS through an XTERM session, you should run the following command:

```
eval ‘resize’ or resize
```

This lets XTERM know about the number of rows and columns.

Connecting the E1 NICs to the Node

The E1 NICs (Channelized E1) connect to either an IGX's CVM with a BC-E1 back card, or UVM BC-UVI-2E1EC backcard, or an IPX's CDP with a BC-E1 back card. Each E1 NIC has two 75-ohm BNC connectors, one for transmit and one for receive, as shown in Figure 6-3. (Figure 6-2 illustrates which E1 NIC is referred to as Voice Port 1 and which is referred to Voice Port 2.)

To connect an E1 NIC to the node, follow these steps:

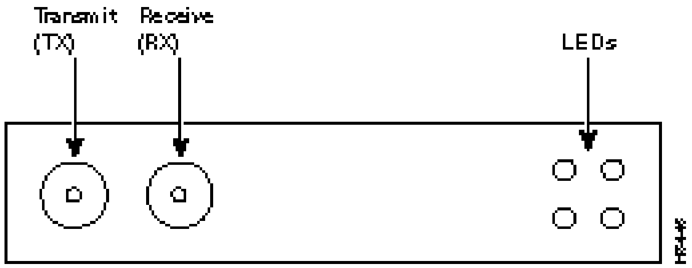
Step 1 Determine which physical port on the node is considered Voice Port 1. This port will be connected to Voice Port 1 on the VNS as shown in Figure 6-2.

Step 2 Connect a 75-ohm coax cable from the transmit (TX) connector on the VNS's E1 NIC to the RX (receive) connector on the node's CDP/CVM/UVM BC-E1 card.

Step 3 Connect a 75-ohm coax cable from the receive (RX) connector on the VNS's E1 NIC to the TX (transmit) connector on the node's CDP/CVM/UVM BC-E1 card.

Step 4 If both E1 NICs are being connected to the node, repeat Steps 1 to 3 for Voice Port 2 and the second E1 NIC in you VNS.

Figure 6-3 E1 NIC Rear Panel



Configuring the Voice Port on the Node

The Voice Port on the node is either a IGX's CVM (or UVM) or a IPX's CDP. These cards must be upped and configured, with the **upcd** (up card), **upcln** (up circuit line**)**, and **cnfcln** (configure circuit line) commands, like any other card on the IGX or IPX switch. You can find detailed descriptions of the IGX's or IPX's command line interface in the *Cisco WAN Switching Command Reference*.

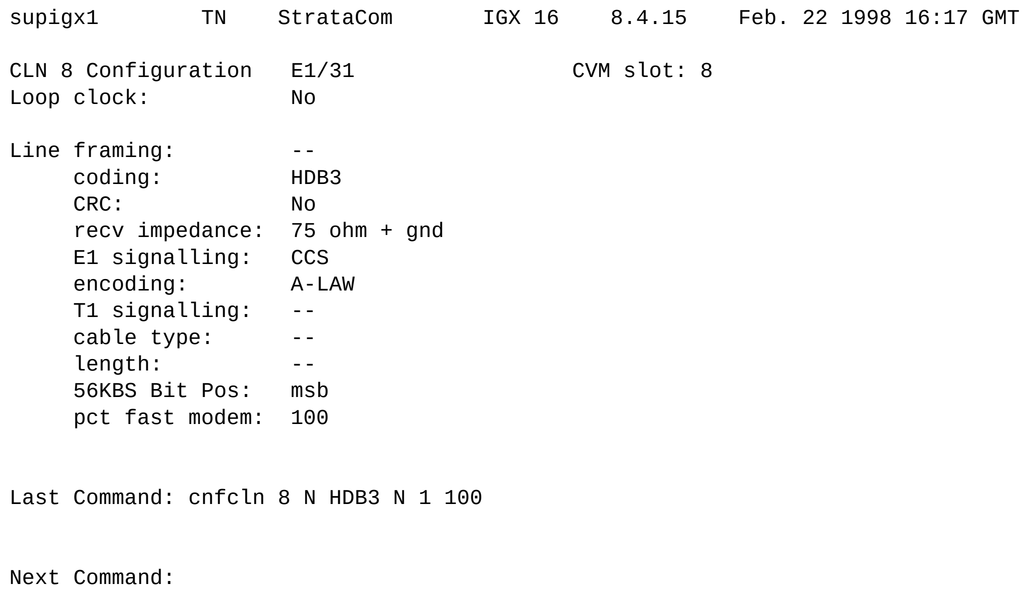
At the node (i.e., IGX/IPX switch), the circuit line between the node and the VNS should be configured with the **cnfcln** (configure circuit line) command for:

- No Loop clock
- HDB3 line coding
- No CRC
- 75 ohm + ground E1 receive impedance
- CCS E1 signaling
- A-Law encoding
- msb 56kbs bit position
- 20 (%) pct fast modem

Figure 6-4 illustrates a typical IGX **cnfcln** menu with the parameters set for connecting to a VNS E1 NIC. (This example is for a CVM card, a UVM card will have a similar configuration.)

The signaling channels over this physical interface are configured through the VNS command line interface, covered in Chapter 7, Understanding the VNS Configuration Interface, and Chapter 8, VNS Network Operation.

Figure 6-4 E1 Configuration for CVM Port connected to E1 NIC



```
supigx1        TN    StrataCom       IGX 16    8.4.15    Feb. 22 1998 16:17 GMT

CLN 8 Configuration   E1/31                 CVM slot: 8
Loop clock:           No

Line framing:         --
     coding:          HDB3
     CRC:             No
     recv impedance:  75 ohm + gnd
     E1 signalling:   CCS
     encoding:        A-LAW
     T1 signalling:   --
     cable type:      --
     length:          --
     56KBS Bit Pos:   msb
     pct fast modem:  100


Last Command: cnfcln 8 N HDB3 N 1 100


Next Command:
```

Connecting the Frame Relay Card to the Node

The Frame Relay Card is used to connect to other VNSs when there are multiple VNS service areas. The Frame Relay Card (RS449 connector) connects to an IGX’s FRM with a Frame Relay Interface (FRI) V.35 (or X.21) back card, or an IPX’s FRP with a Frame Relay Interface V.35 (or X.21) back card. The Frame Relay Card has an RS449 physical connector.

Cisco supplies two types of cables to connect the Frame Relay Card to the node. One cable has an RS449 connector for the VNS and a V.35 connector for the node’s V.35 Frame Relay Interface (back card). The other cable has an RS449 connector for the VNS and an X.21 connector for the node’s X.21 Frame Relay Interface (back card). These cables are ordered independently along with the VNS.

To connect the VNS’s Frame Relay Card to the node, follow these steps:

Step 1 Connect the RS449-end of the cable (ordered with the VNS) to the RS449 connector on the VNS, shown in Figure 6-2.

Step 2 Connect the V.35- or X.21-end of the cable to the appropriate port on the node’s Frame Relay Interface (V.35 or X.21) back card.

Configuring the Frame Relay Port

The frame-relay LMI parameters for the VNS side of the frame-relay connection to the node (IGX switch, IPX switch, etc.,) are set in a UNIX file, fr_config. This factory has configured this file for no LMI. If you wish to choose Strata-LMI or Annex D LMI, follow these steps:

Step 1 Log in to the VNS.

Step 2 If they are running, stop the VNS processes using the VNS CLI as described in Chapter 5 in the section Shutting Down the VNS.

Step 3 Change directory (cd) to /usr/net/fr.

Step 4 Execute ./frstop

Step 5 Edit (vi) *fr_config*.

Step 6 Change the following line (configuration line at the beginning of the file):

```
HOST RS449 clock 0 N393 0 INARP NO

to ONE of the following forms:

HOST RS449 clock 0 GOF N393 4 INARP NO  # Strata-LMI
HOST RS449 clock 0 N393 4 INARP NO         #  Annex D
```

Step 7 Save the modified *fr_config* file (:ZZ).

Step 8 Execute ./frstart

Step 9 Restart the VNS processes.

The LMI default Timer/Counter values are:

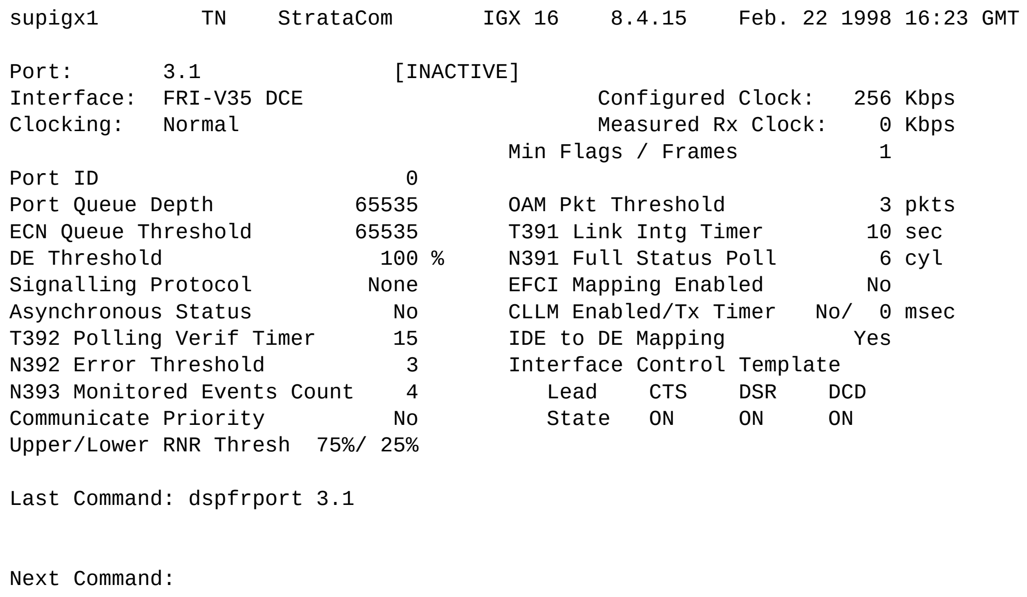
- N391 6
- N392 3
- N393 4
- T391 10
- T392 15

The default values should be appropriate for most applications. If needed, these values may be changed by inserting the appropriate identifier-and-value pair in the configuration line (similar to the "N393 4" Step 6 above).

The node’s Frame Relay Port must be upped and configured, with the **upfrport** (up Frame Relay Port) and **cnffrport** (configure Frame Relay Port) commands, like any other port on the node. You can find detailed descriptions of using the IGX’s or IPX’s command line interface in the *Cisco WAN Switching Command Reference*.

You must also configure the Frame Relay Port (FRP, FRM, FRSM) to match the LMI set on the VNS. Depending on the type of node, the node’s Frame Relay Port will be configured with the appropriate IPX switch, IGX switch, MGX 8220 configuration command, such as **cnffrport** for an IGX FRM. Figure 6-5 illustrates a typical Frame Relay Port configured for no LMI.

Figure 6-5 Frame Relay Port Configuration



```
supigx1        TN    StrataCom       IGX 16    8.4.15    Feb. 22 1998 16:23 GMT

Port:       3.1               [INACTIVE]
Interface:  FRI-V35 DCE                       Configured Clock:   256 Kbps
Clocking:   Normal                            Measured Rx Clock:    0 Kbps
                                       Min Flags / Frames           1
Port ID                        0
Port Queue Depth           65535       OAM Pkt Threshold            3 pkts
ECN Queue Threshold        65535       T391 Link Intg Timer        10 sec
DE Threshold                 100 %     N391 Full Status Poll        6 cyl
Signalling Protocol         None       EFCI Mapping Enabled        No
Asynchronous Status           No       CLLM Enabled/Tx Timer   No/  0 msec
T392 Polling Verif Timer      15       IDE to DE Mapping          Yes
N392 Error Threshold           3       Interface Control Template
N393 Monitored Events Count    4          Lead    CTS    DSR    DCD
Communicate Priority          No          State   ON     ON     ON
Upper/Lower RNR Thresh  75%/ 25%

Last Command: dspfrport 3.1


Next Command:
```

Note that the Frame Relay port at the other end (the other VNS) will also have to be configured. The Frame Relay connection between these two VNSs will be built through the VNS Configuration Interface which is described in Chapters 7 and 8. The connection will default to a Frame Relay Class of Service 1. The *Cisco WAN Switching Command Reference* contains detailed information about Frame Relay classes.

Modifying the Default Range of VNS DLCIs

The VNS's Frame Relay Port comes from the factory with DLCIs 101 to 113 configured for use. These DLCIs are used for establishing Frame Relay PVCs between VNSs in different VNS areas. If you need to use a DLCI other than 101 to 113, you will have to add it to the fr_conv file. This applies to both the local and remote ends of the Frame Relay PVC between the VNSs.

These DLCIs are used by the VNS Configuration Interface and are described in Chapter 7 in the section, Local Adjacency Information.

Note You should not modify fr_conv unless you are sure you need to use a DLCI which is not in the default range.

To modify the default range of DLCIs used for PVCs between VNSs in different VNS areas, follow these steps:

Step 1 Log in to the VNS on which you need to add a DLCI. This could be either the local or the remote VNS.

Step 2 If they are running, stop the VNS processes using the VNS CLI as described in Chapter 5 in the section Shutting Down the VNS.

Step 3 Change directory (cd) to /usr/net/fr.

Step 4 Execute ./frstop

Step 5 Edit (vi) *fr_conv.* A typical fr_conv file is shown below:

```
Sample fr_conv File
# ADAX Frame Relay IP address to DLCI (0, . . . , 1023) to port mapping
#
# Note: ports 0-7 are physical, upper ports 8-15 are for protocol layers
#   connected to the Frame Relay Multiplexer package (i.e. TCP/IP).
#
# IP Address    Frame Relay DLCI        Port
# 189.0.0.1     123                     0
# 189.0.0.2     234                     0
# 189.0.0.3     0x345                   2       # Hex-coded DLCI is OK
# 189.0.0.4     0x345                   2       # Same DLCI
# 1             456                     3       # SNA encapsulation
# 2             567                     3       # X.25 encapsulation
# 189.0.0.6     678                     8       # Local TCP/IP home port
#
# The following examples would only be used if Frame Relay were operating as
# network and performing Frame Relay switching.  This is a rarely used option.
#
# Lines that begin with a dash (-) indicate a port-to-port DLCI and port number
# mapping.  Each entry consists of five fields, including the dash.  The second
# through fifth fields are the source DLCI and port, and the destination DLCI
# and port.
#
#                 Source      Destination
#              DLCI   Port     DLCI   Port
# -             25      0       22      1       # software <-> hardware
# -             30      0       39      2       # demo <-> software
# -             30      1       40      2       # demo <-> hardware
# -             31      3       41      2       # bacchus <-> hardware
# -             33      3       43      0       # bacchus <-> eng_lab
# -             134     0       144     7       # software <-> Dial-up
# -             135     1       45      7       # hardware <-> Dial-up
# -             136     3       46      7       # bacchus <-> Dial-up
# -             137     5       47      7       # silenus <-> Dial-up
# -             38      5       48      3       # silenus <-> bacchus
-               100     0       100     9       # silenus <-> bacchus
-               101     0       101     9       # silenus <-> bacchus
-               102     0       102     9       # silenus <-> bacchus
-               103     0       103     9       # silenus <-> bacchus
-               104     0       104     9       # silenus <-> bacchus
-               105     0       105     9       # silenus <-> bacchus
-               106     0       106     9       # silenus <-> bacchus
-               107     0       107     9       # silenus <-> bacchus
-               108     0       108     9       # silenus <-> bacchus
-               109     0       109     9       # silenus <-> bacchus
-               110     0       110     9       # silenus <-> bacchus
-               111     0       111     9       # silenus <-> bacchus
-               112     0       112     9       # silenus <-> bacchus
-               113     0       113     9       # silenus <-> bacchus
```

The lines at the end of the file that began with a dash (-) indicate a port-to-port DLCI and port number mapping. These are the DLCIs reserved for the Frame Relay connections to the VNS’s Frame Relay Port. Each entry consists of five fields, including the dash. The second through fifth fields are the source DLCI and port and the destination DLCI and port.

Step 6 To add another DLCI for use at this VNS’s Frame Relay Port, add it at the end of the file. For instance to add DLCI to the range of DLCIs available, you would enter:

```
-               114    0        114     9        # additional DLCI 114
```

Step 7 Add all the DLCIs that you need to the end of this file.

Step 8 Save the modified *fr_conv* file (:ZZ).

Step 9 Execute ./frstart.

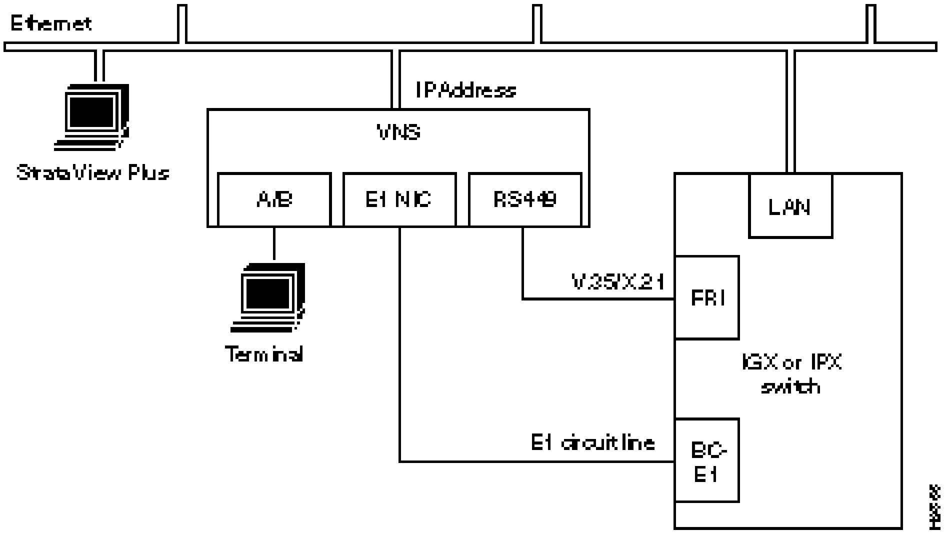
Step 10 Execute ./frroute.

Step 11 Restart the VNS processes.

Connecting to an Ethernet Segment

The VNS connects to an ethernet to communicate both with the node, the IPX Nodal Processor Card (NPC), or the IGX Nodal (i.e., Network) Processor Module (NPM), and with an SV+ Workstation. Figure 6-6 illustrates the ethernet connections.

Figure 6-6 Ethernet Connection



Normally the VNS is connected from its 10Base-T connector (see Figure 6-1) to an Ethernet Hub. (The 10Base-T ethernet hub is not supplied by Cisco.) The node's LAN port and the SV+ Workstation are also connected to this same ethernet segment.

Note If the SV+ Workstation is collecting statistics, it is recommended that it *not* be connected to the same ethernet segment as the VNS and the node. The heavy statistics traffic can affect the operation of VNS.

Local LAN Environment

You may have to modify some of the VNS's UNIX operating system (i.e., Solaris 2.4) files for your local LAN environment. To do this, you will need to use a text editor such as *vi* to modify files and a few simple Sun operating system (SunOS) commands.

Using vi

vi is a UNIX-based screen editor which can be used to make some minor modifications to the UNIX-based files. You can find out more about vi, by typing *man vi* at the VNS's UNIX prompt and pressing Enter. In vi there is a command mode and an editing (i.e., insertion) mode. Most commands are entered from the command mode; while the file is actually modified in the editing mode. You quit the editing mode with ESC. Since only minor changes need to be made to VNS UNIX files, you should only need to know a few commands:

- *vi "file name"* opens the file you are about to edit.
- *i* enters the insertion mode. You can start editing the file at the cursor. You end the insertion mode with *ESC*.
- *o* opens a line in the file below the position of the cursor. Enter data on this line until you hit *ESC*.
- *D* deletes the rest of a line.
- *dd* deletes a line.
- *R* enters the overwrite mode, where you will type over existing lines.
- *:* opens up the one line command mode at the bottom of the screen.
- *h, j, k, l* move the cursor around the file in the command mode.
- *ESC* takes you out of the editing mode and returns you to the command code.
- *:q!* quits the file without saving changes.
- *:w* saves the file while your editing it.
- *ZZ* saves the file and quits.

When you are logged in to the VNS, you can find out the use and syntax of operating system commands with the **man page** command; for instance, enter *man login* to find out about the login command.

A quick procedure for editing any of the files:

Step 1 cd to where the file is located.

Step 2 vi **filename**.

Step 3 Position cursor where you want to add or change text (use the arrow keys or h, j, k, l).

Step 4 Enter o to add a new line, i to edit a line, or R to enter overwrite mode.

Step 5 Enter your text.

Step 6 Hit ESC when you are done adding text. You are now back in the command mode.

Step 7 Enter ZZ to save the file. (You can use *more* **filename** to check that file has been modified).

Note If you are uncomfortable with vi, you might copy the (cp) the original file to another name before editing it; for example, *cp* **filename newfilename.**

Modifying LAN (Ethernet) Parameters

Note The local LAN parameters can be very involved, particularly if NIS+ is running on your WAN switching network. These UNIX-based files should only be modified by an experienced system administrator who is familiar with the Solaris 2.4 operating system.

After checking with your system administrator, set the IP address, hostname, and other parameters necessary for operating the VNS in your local area network environment, as follows:

Step 1 Connect a terminal to the VNS.

Step 2 Log in to VNS as superuser.

Note Once you start changing host names and IP addresses, you must make sure you complete all the files. Do not turn off power or reboot in the middle of this process or you could disable your VNS.

Step 3 Use vi to screen edit the file */etc/hosts* and add the IP address for VNS and the IP address for the SV+ Workstation.

For direct Ethernet connection where, for example, you have an SV+ Workstation with a hostname of *nms* and an IP address of *200.1.2.3* and a VNS with a hostname of *ins1* and an IP address of *200.1.2.4*, you would add the two lines, shown in bold type, to the *hosts* file:

```
Contents of /etc/hosts
#
127.0.0.1     localhost
#
200.1.2.4     ins1       loghost    # INS1 (VNS 1 local Ethernet port)
200.1.2.3     nms                   # SV+ Workstation
#192..x.x.x   fr-ins1     frhost    # INS1 (Frame-Relay)
# End of hosts
```

Note that the frhost (frame-relay host) IP address is used for remote SV+ Workstation connectivity and can be commented out by adding a # sign to beginning of line. This feature is not used with the VNS.

Step 4 If required for your local network, use vi to screen edit the file */etc/networks*, which will appear similar to the following:

```
Contents of /etc/networks file:
#
# The loopback network is used only for intra-machine communication
#
loopback      127
#
# Internet networks
#
arpanet       10         arpa       # Historical
nms-net       200.1.2               # SV+ network
# End of networks
```

For our example, the line in bold text, **nms-net** . . ., is added to the networks file.

Step 5 If required for your local network, use vi to screen edit the file */etc/netmasks* to add the appropriate subnet mask for your LAN segment.

Step 6 If required for your local network, use vi to screen edit the file */etc/hostname.le0* to name the VNS's ethernet port.

Step 7 If required for your local network, use vi to screen edit the file */etc/nodename* to name the VNS node, and verify that this name is the same name as /etc/hostname.le0.

Step 8 Use the *date* SunOS command to set the local date and time.

Step 9 Set the VNS's local timezone by editing */ect/TIMEZONE* file. Table 6-1 lists the supported time zones. Open the file (with vi) and look for the line:

```
TZ=US/Pacific
```

Change this line to the required TimeZone;
for example:

```
TZ=Etc/GMT
```

Save the /etc/TIMEZONE file .

Step 10 Execute the *reboot* command to restart the VNS.

Note For VNS operation, the /etc/defaultrouter file should be empty.

Note Note that the UNIX ifconfig command could be used to configure the VNS's Ethernet port IP address. So for our example:

```
ifconfig le0 200.1.2.4
```

This should not be necessary if the IP address has been added to /etc/hosts.

Table 6-1 Supported Time Zones

Australia/	Brazil/	CET	CST6CDT	Canada/
Chile/	Cuba	EET	EST	EST5EDT
Egypt	Erie	Etc/	Factory	GB
GB-Eire	GMT	GMT+0	GMT+1	GMT+10
GMT+11	GMT+12	GMT+13	GMT+2	GMT+3
GMT+4	GMT+5	GMT+6	GMT+7	GMT+8
GMT+9	GMT-0	GMT-1	GMT-10	GMT-11
GMT-12	GMT-2	GMT-3	GMT-4	GMT-5
GMT-6	GMT-7	GMT-8	GMT-9	Greenwich
HST	Hongkong	Iceland	Iran	Israel
Jamaica	Japan	Kwajalein	Libya	MET
MST	MST7&MDT	Mexico/	Mideast	NZ
NZ-CHAT	Navajo	PRC	PST8PDT	Poland
ROC	ROK	Singapore	Turkey	UCT
US/	UTC	Universal	W-SU	WET
Zulu	posixrules			

For the following you need to enter both country/area (for example, US/Eastern)

For Australia:

ACT	Broken_Hill	LHI	NSW	North
Queensland	South	Tasmania	Victoria	West
Yancowinna				

For Brazil:

Acre	DeNoronha	East	West	

For Canada:

Atlantic	Central	East-Saskatchewan	Eastern	Mountain
Newfoundland	Pacific	Yukon		

For Chile:

Continental	EasterIsland			

For Etc:

GMT	GMT+0	GMT+10	GMT+11	GMT+12
GMT+2	GMT+3	GMT+4	GMT+5	GMT+6
GMT+7	GMT+8	GMT+9	GMT-0	GMT-1
GMT-10	GMT-11	GMT-12	GMT-13	GMT-2
GMT-3	GMT-4	GMT-5	GMT-6	GMT-7

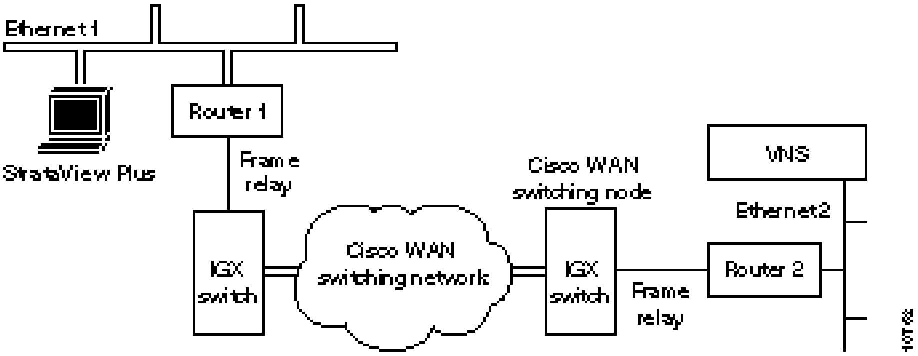
Table 6-1 Supported Time Zones (Continued)

GMT-8	GMT-9			
For Mexico:				
BajaNorte	BajaSur	General		
For Mideast:				
Riyadh87	Riyadh88	Riyadh89		
For US:				
Alaska	Aleutian	Arizona	Central	East-Indiana
Eastern	Hawaii	Michigan	Mountain	Pacific
Pacific-New	Samoa			

Remote StrataView Plus Workstation

Where the VNS and the StrataView Plus Workstation are not on the same Ethernet, they must communicate over a frame-relay connection. In this case, the SV+ Workstation and the VNS are connected to separate Ethernet segments, as shown in Figure 6-7.

Figure 6-7 Connectivity Using Two Ethernet Segments

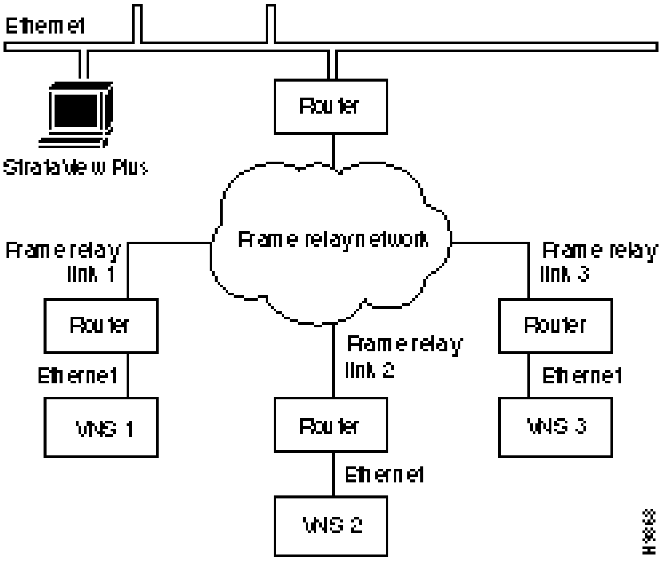


In the situation shown in Figure 6-7, the messages from the VNS to the SV+ (i.e., SNMP Traps) are routed over Ethernet 2 to Router 2 to the Cisco WAN switching network to Router 1 to Ethernet 1 to the SV+ Workstation. The only configuration that needs to be done is to provide the route from the VNS to the SV+ Workstation on the IP network. Consult your network administrator for help in setting up this route over the routers.

Multiple Remote VNSs

When there are multiple VNSs in the WAN switching network, a separate ethernet connection will have to be made between each VNS and the SV+ Workstation as shown in Figure 6-8. Your network administrator should assist you in setting up these connections over the additional routers.

Figure 6-8 Multiple VNSs



Connecting the Redundant VNS

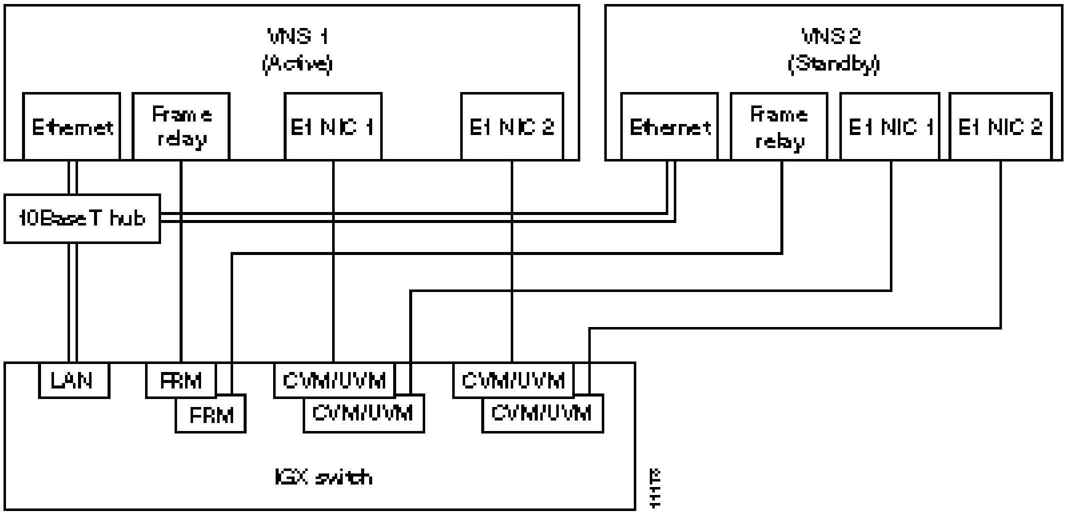
When configuring redundancy, do not switch on the redundant VNS until the active unit is fully configured. You connect the redundant VNS, or second VNS in a redundant pair, in exactly the same way as you did with the first VNS. As shown in Figure 6-9, the second VNS uses identical physical interfaces:

- Terminal
- Frame Relay Card
- E1 NICs
- Ethernet

The Frame Relay Card and E1 NICs physical connections will be to different physical ports on the IGX/IPX switch. The connections can be made to two ports on the same card, however.

The second VNS will also have to have its local LAN environment set up, and it will use a different IP address and host name than the first VNS.

Figure 6-9 Redundant VNS



Note The Frame Relay Card connection is only used when there are multiple VNS areas in your WAN switching network.

Configuring the Node

When adding Voice Network Switching (VNS) to a Cisco WAN switching network, the node connected to the VNS will require some high-level adjustments to its operating parameters. These parameters are adjusted with:

- **cnfnodeparm** (Configure Node Parameters)
- **cnfcmparm** (Configure Connection Management Parameters)
- **cnftrk** (Configure Trunk)
- **cnffunc** (Configure Function)

Table 6-2 lists these commands and the parameters that can have an effect on the operation of a VNS network. During an initial installation of a VNS, these parameters have to be changed as indicated in the table.

Caution The **cnfnodeparm** and **cnfcmparm** are **superuser-level** commands and should be used carefully. And, although the **cnftrk** command is not superuser-level command, it should also be used carefully. Note that these parameter changes can adversely affect your network’s operation. They should be adjusted only after your network has been carefully modeled.

Table 6-2 Configuring the Node Commands

Command	Parameter	Adjustment
cnfnodeparm	**Nw Pkt Tx Rate (pps)** Network Packet Transmit Rate	The default of **500** packets per second should be changed to **1000** packets per second.
cnfcmparm	**17 Max SVC Retry**[1]	Should be set to 5.
	18 Send SVC urgent msg[1]	Should be set to **Yes.**
cnftrk	**Statistical Reserve**	The **Statistical Reserve** for trunks connecting to the VNS node should be doubled from the default value.
cnffunc	**Index 10**	Enable index 10 for the registration of D channel failures on StrataView Plus.

The **cnfnodeparm** and **cnfcmparm** commands are described in detail in the *Cisco WAN Switching SuperUser Command Reference*. The **cnftrk** and **cnffunc** commands are described in detail in the *Cisco WAN Switching Command Reference*.

[1] In switched software release 8.5, Max SVC Retry and Send SVC urgent msg parameters apply only to IPX nodes.

SNMP Community Names

Each of the nodes (i.e., Cisco wide-area switches) in the network need to have their SNMP community names set up before Voice Network Switching will work. You should ensure that the Cisco wide-area switch and network have seen set up for proper IP connectivity. If necessary, refer to the Release 8.4 *Cisco WAN Switching Command Reference* or *Cisco WAN Switching SuperUser Command Reference* and use the following commands:

- **cnflan** to configure each node’s communication parameters so the node can communicate with the SV+ Workstation over an ethernet LAN using TCP/IP protocol. This command configures the IP address for the node’s LAN (physical) port.
- **cnfnwip** to configure the node’s IP address and subnet mask.
- **cnfsnmp** to configure the node’s SNMP GET and SET community strings. The SNMP community strings should be set as follows:

  Get Community String = Public

  Set Community String = Private

  Trap Community String = Public

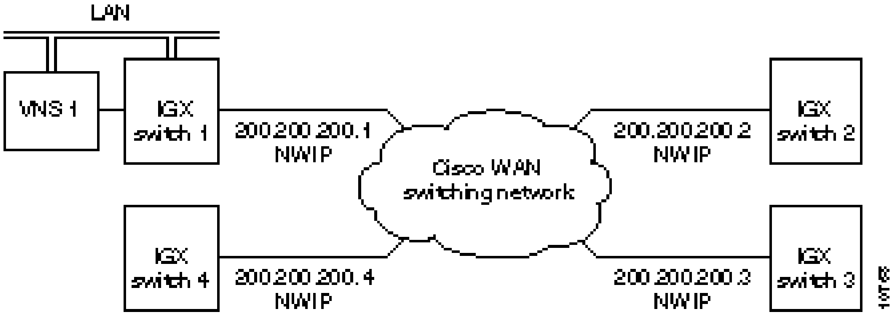
  The Set Queued Request Timeout should also be set to maximum.

Adding Network IP Routes

The VNS must be able to communicate with each node in the network. If there is not an Ethernet connection to each node, the VNS can communicate with the nodes through IP Relay. This involves setting up the Network IP addresses (**cnfnwip**), creating a Network IP (NWIP) subnet, and adding the gateway to that subnet with the route add net command on the VNS. (The **route add net** command can be stored in a file at /etc/rc3.d that executes at system startup time.)

For instance in Figure 6-10, IGX switch 1 is connected to the same Ethernet segment as VNS 1. IGX switch 1 has a LAN IP address of 200.1.2.5. The other three IGX switches (IGX switch 2, 3, and 4) will communicate with VNS 1 using IP Relay. This IP Relay network will have become a subnet with address 200.200.200.0. Traffic from VNS 1 to IGX switch 2, 3, or 4 has to be directed out the Network IP (NWIP) subnet (200.200.200.0) through IGX switch 1. In effect IGX switch 1 serves as a gateway to the NWIP subnet.

Figure 6-10 Network IPs



To configure this sample NWIP subnet, you would follow these steps:

Step 1 The Network IPs (NWIP) for each of the four nodes will have to be configured with each node’s **cnnwip** command. (They are all be put on the same subnet with the subnet mask argument, 255.255.255.0.)

Step 2 Next you would log into the VNS and create a file containing the UNIX-level **route add net** command. The command is:

route add net 200.200.200.0 200.1.2.5 1

Where 200.200.200.0 is the network address of the NWIP subnet, and 200.1.2.5 is the LAN address of IGX switch 1. Note that there is a space between the two IP addresses and a space between the second IP address and the 1. The 1 after the second IP address is a hop metric and must be non-zero if the destination is not directly connected to the VNS’s Ethernet segment.

This file with the **route add net** command should saved in /etc/rc3.d and could be named S70route, as in this example file:

```
/etc/rc3.d more s70route

#Sample S70route file
#route add default xxx.xxx.xxx.xxx #if applicable, add the address of the default
router
route add net 200.200.200.0 200.1.2.5 1
#
# End
```

This file executes at system startup.

Migrating Voice Connections to a VNS Network

Often Voice Network Switching is added to a Cisco WAN switching network which has previously been configured for voice connections. When migrating voice connections to a VNS network, you should consider the following commands which may have to be adjusted:

cnfchgn (Configure Channel Gain)

cnfchadv (Configure Channel Adaptive Voice)

cnfecparm (Configure Integrated Echo Cancellor Parameters)

The **cnfchgn** and **cnfchadv** commands are described in the *Cisco WAN Switching Command Reference* in the Chapter on Voice Connections. The **cnfecparm** command is a superuser-level command and is described in the *Cisco WAN Switching SuperUser Command Reference*. Note that the **cnfecparm** command is used to set the **Voice Template** parameter, which selects either normal level (USA) or high-level (UK) voice.

Note Circuit line connections to PBXs or to VNSs should be set to CCS signaling.

Synchronizing Time

To ensure time synchronization between VNS systems in the VNS network (for either single or multiple domains), the **rdate** UNIX command should be used in a cron job so that all clocks are synchronized from a single point on the network. This is network relative and does not have to be synchronized from an absolute clock source.

The rdate command sets the VNS time from a specified remote host (that is, another VNS) and takes the form:

```
rdate <hostname or ipaddress>
```

Where hostname or ipaddress is the VNS from which you want to get the time to synchronize another VNS.

For instance, if you had 4 VNSs in your network (vns1, vns2, vns3, and vns4) and you want vns1 to be the master for the time for all the VNS systems. You could create a script named vns_set_time on each of the other VNSs (vns2, vns3, and vns4.) The script could look like:

```
#!/etc/csh
/usr/bin/rdate vns1
```

Make the scripts executable; as root user, issue the command:

```
chmod 700 vns_set_time
```

This assumes that the /etc/host file is updated with the IP address to host names for all the VNSs in the system. You run this file as a cron job, a UNIX system feature which uses the cron daemon to execute processes at specified times.

You create the cron job by editing the root crontab file on vns2, vns3, and vns4. Use crontab -e root and add the following line to the file:

```
30 1 * * * /usr/local/bin/vns_set_time > /dev/null 2>&1
```

This schedules the script vns_set_time to run at 1:30 am. /dev/null 2>&1directs the error messages to a null file.

A crontab file consists of lines of six fields each. The fields are separated by spaces or tabs. The first five are integer patterns that specify the following:

- Minute (0-59)
- Hour (0-23)
- Day of the month (1-31)
- Month of the year (1-12)
- Day of the week (0-6 with 0=Sunday)

The example runs vns_set_time everyday at 1:30 am. The vns_set_time file has to be run as a cron job on every VNS that needs to synchronize its date and time from vns1.

Note You can find out more about cron and crontab using the UNIX man command.

Ping the VNS

After you have connected and configured the VNS(s), you should log in (or have someone log in) to the SV+ Workstation and Ping the VNS to ensure that they are communicating. You should also be able to ping all the remote nodes.

The rest of the configuration of a VNS network is done with the VNS Configuration Interface, described in Chapter 7. Chapter 8, VNS Network Operation, describes using the VNS Configuration Interface to provision the VNS network.

Adding a VNS Object to the SV+ Topology Maps

After you determine that StrataView Plus and the VNS are communicating (as a result of Ping), you need to install a network map icon, which represents either the VNS or its redundant VNS, on the topology maps of the SV+ Workstation. A VNS icon is added, modified, or deleted only through HP OpenView. This icon shows only the existence of the VNS; StrataView Plus does not manage the VNS object. StrataView Plus does receive SNMP Traps from the VNS, however, and will display the status of the VNS with different colors:

Green	Normal
Yellow	Minor alarm
Red	Major alarm
Brown	VNS unreachable

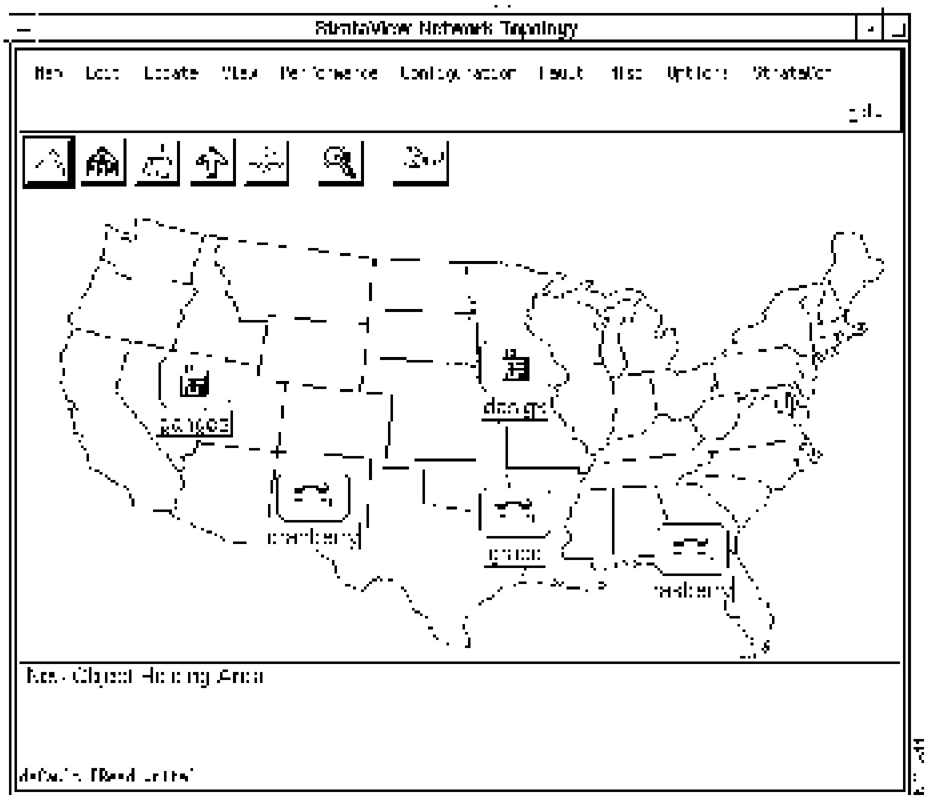
The VNS icon is only visible on the SV+ Workstation where it was added.

To add a VNS icon, which requires access to the HP OpenView network topology main menu on the SV+ Workstation, follow these steps:

Step 1 At the SV+ Workstation open an HP OpenView window (at the UNIX prompt, change to the OV directory, then enter `ovw`).

Step 2 Double-click your network icon to open a Network Topology window and map, shown in Figure 6-11.

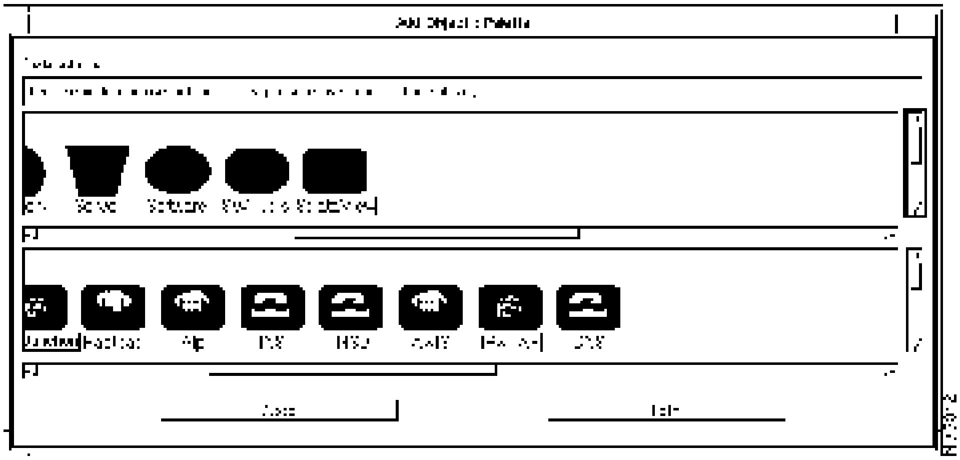
Figure 6-11 HP OpenView Network Topology Map



Step 3 Select the `Edit - Add Object...` menu.
The Add Object: Palette window appears.

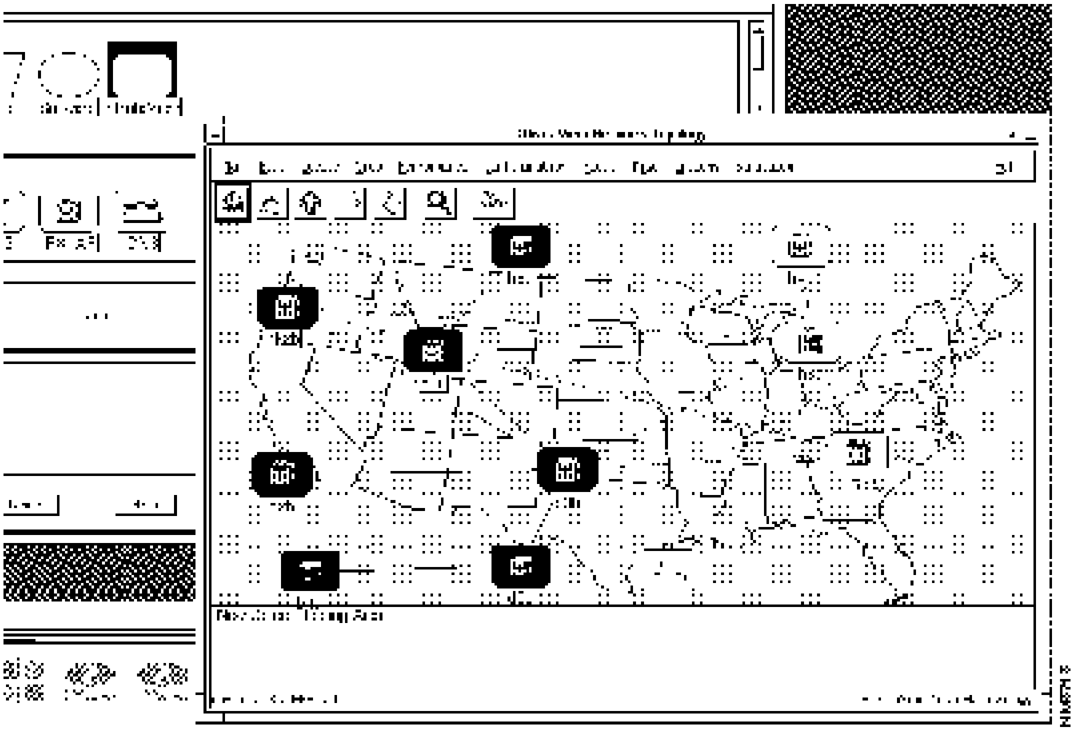
Step 4 Click on the StrataView icon on the Add Object: Palette to open the Symbol Subclasses window where you will find the VNS icon as shown in Figure 6-12.

Figure 6-12 Add Object: Palette and VNS (DNS) icon



Step 5 Using the middle mouse button, drag and drop the VNS symbol from the Palette to the map as shown in Figure 6-13. The `Add Object` window appears.

Figure 6-13 VNS Icon on HP OpenView Topology Map



Step 6 In the `Add Object` window, shown in Figure 6-14, you name the VNS object and call up another window to set its object attributes by identifying the Cisco wide-area switch to which it is attached. To name the VNS object:

- Click in the `Label:` box and enter the host name of the VNS. (This name will be displayed with the symbol on the map if you select Yes at the `Display Label` field.)
- Select one of the `Display Label:` radio buttons:

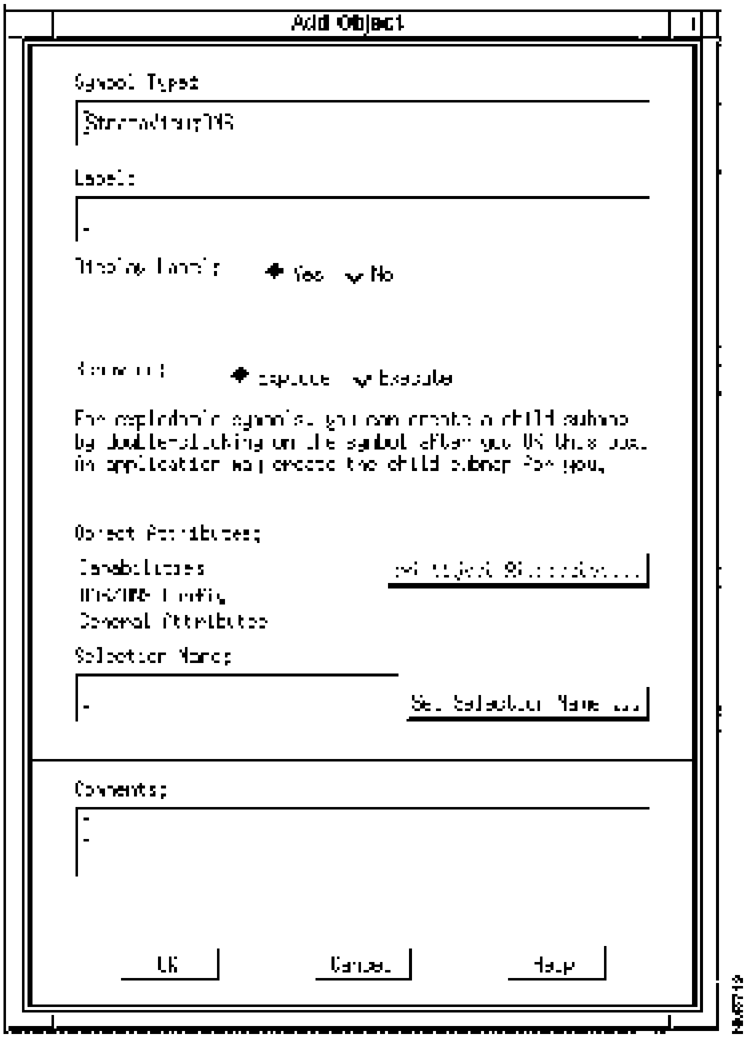
  Set to *Yes* to display the name of the symbol.

  Set to *No* if you do not want to see an object label on the map.
- Select one of the `Behavior:` radio buttons:

  Selecting `Explode` causes the submap to display when the symbol is double-clicked.

  Selecting `Execute` permits the symbol to execute an application which performs an action on a set of objects when it is double-clicked.

Figure 6-14 Add Object Menu



Add Object

Symbol Type:

StrataView:VNS

Label:

Display Label: ● Yes ○ No

Behavior: ● Explode ○ Execute

For explodable symbols, you can create a child submap by double-clicking on the symbol after you OK this box. An application may create the child submap for you.

Object Attributes:

Capabilities

DAS/DNS Config

General Attributes

Selection Name:

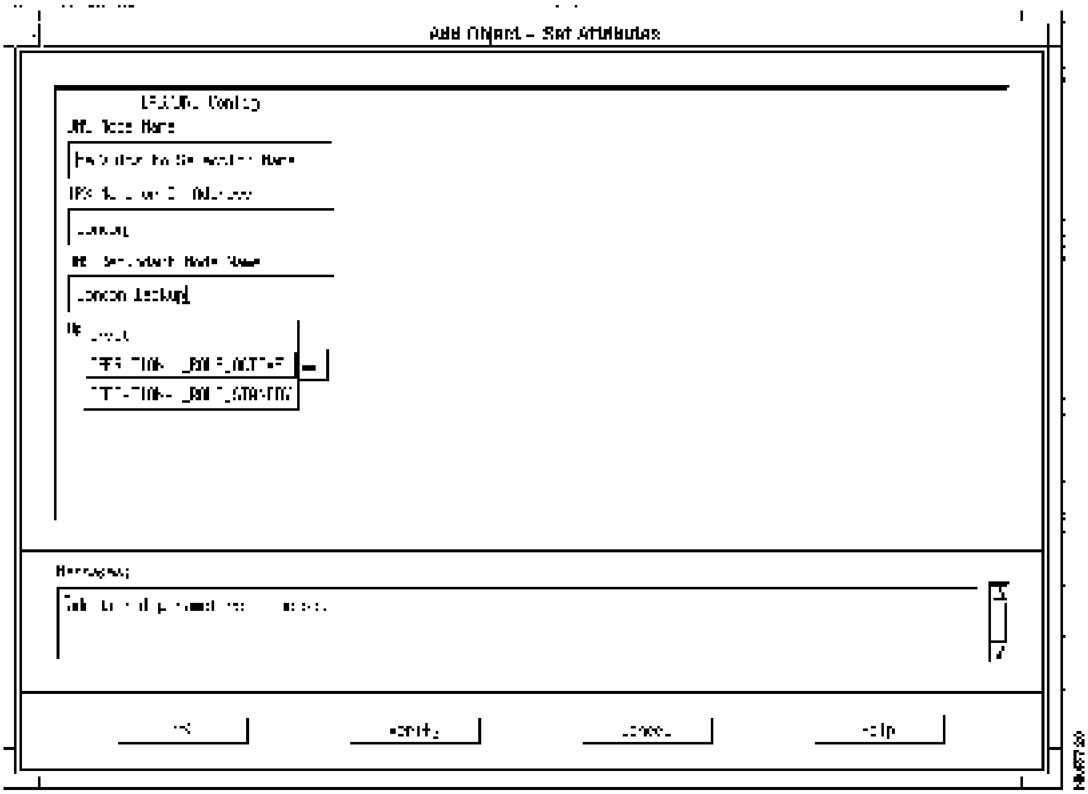
Comments:

Note HP OpenView on-line help explains the difference between explodable and executable symbols.

Step 7 Next Select `DAS/DNS Config` in the Object Attributes: box. This will activate the `Set Object Attributes...` button.

Step 8 Click the `Set Object Attributes...` to present the `Add Object - Set Attributes` window, shown in Figure 6-15, for DAS/DNS Config. The host name of the VNS that you entered in the previous window will appear in the VNS Node Name box.

Figure 6-15 Add Object - Set Attributes Window



Step 9 In the next three boxes, you enter information about the Cisco wide-area switch to which the VNS is attached:

- In the `IPX Name or IP Address` box, enter the node name of the Cisco wide-area switch (IGX/IPX switch) to which the VNS is attached.

Note Although these boxes are labeled with IPX, they refer to any Cisco wide-area switch to which the VNS attaches.

- In the `VNS Redundant Node Name` box, enter the name number of this VNS's peer VNS.
- In the `Operational Role` box, enter the active or standby role of this VNS.
- Operational Role is an informational field only. There is no indication on the topology map whether this VNS has the active or standby role in a redundant pair.

Step 10 If you have entered your information correctly, press the `Verify` button. The OK button will activate.

Step 11 Press the OK button, you will return to the Add Object window. Press the OK button on the Add Object window and you will return to the HP OpenView network topology map.

Removing the VNS Object From the Topology Map

You must use the StrataCom pull-down menu to remove an INS icon (that is, VNS) from a network topology map. Using any of the other HP OpenView tools, such as Edit--Delete, will cause an error.

To remove the INS icon from you network topology map, follow these steps:

Step 1 With your network topology map displayed, select the VNS icon on the map.

Step 2 Pull down the `StrataCom` menu from the top menu bar.

Step 3 Select `Remove DNS Station` from the StrataCom pull down menu.

Note DNS and INS were previous names for the VNS.

Adding VNS Users

With this release, user-access verification has been added to the VNS Configuration Interface (i.e., vnscli). In other words, the use of the VNS Command Line Interface is password controlled. The password control has been added through a UNIX-Level vns_passwd file.

Adding a user with specific privileges takes two steps:

1. Add a UNIX User
2. Add the VNS User

Adding UNIX users and controlling the vns_passwd file should typically be done by your system administrator.

Add a UNIX User

The system administrator generally adds UNIX users with the Solaris **admintool**. With its graphical user interface, the admintool simplifies adding users to UNIX operating systems, a task which previously had to be done with the adduser command and by editing the /etc/group file.

To add a UNIX user, the system administrator would follow these steps:

Step 1 From the StrataView Plus Workstation, rlogin or telnet to the VNS.

Step 2 Log in to the VNS as root.

Step 3 At the root prompt, type **admintool**. The Administration Tool opening screen will appear.

Step 4 Click on the **User Account Manager** button. The User Account Manager window appears.

Step 5 Press the Edit button and select the Add User option. This will bring up the User Information window.

Step 6 Fill in the username, userid, and the various options. There is a Help button on the menu that provides information about the various options.

Step 7 Press the Add button. The UNIX user now has been added to the VNS.

Add the VNS User

VNS users can be added only after they are UNIX users. The VNS user is added by editing the file /etc/vns_passwd and adding an entry for the VNS user. The entry in the vns_passwd file has the following format:

```
VnsUserName:Permissions
```

VnsUserName is the username of the VNS user and must be the same as the one used for the UNIX user which was just added. Permission is the string which specifies the various VNS CLI operations which the user will be permitted to perform. The valid permission options are each specified by a single letter, that is ‘a’ or ‘d’ or ‘m’ or ‘b’ or ‘g’ and provide the following permissions:

- 'a' - gives add object permission
- 'd' - gives delete object permission
- 'm' - gives modify object permission
- 'b' - gives browse object permission
- 'g' - gives debug level setting permission
- ‘v’ - gives validate database permission

The two fields must be separated by ':' , the field separator.

A sample factory-default VNS password (vns_passwd) file is shown below:

```
vns_passwd File
#################################################################
#This is the passwd file which determines user access to the VNS
#database which should exist in /etc.
#
#The sample format given below has to be adhered to for adding
#new users.
#
#format:user_login_id:permissions
#
#“permissions” can be a string of any of the letters ‘a’, ‘d’, ‘m’,
#‘b’, ‘g’, ‘v’ which stand for add, delete, modify, browse, debug and validate
#respectively. These can be specified in any order.
#
#The user will be allowed to perform only the operations specified
#by the permission string, on the VNS database using the vnscli.
#
#The entry for root has been added by default. This line may be
#yanked and the required number of users and their permissions
#may be added. A user not listed in this file is not allowed to
#run vnscli. vnscli also does not run if this file is not present.
#
#A ‘#’ in the first column of a line turns the line into a comment.
#Users may be deleted by commenting out the corresponding line also.
#
##################################################################
root:amdbgv:
```

This vns_passwd file shows the root as having all available vnscli privileges (amdbg) as described in the dns_passwd file's comments. To add other users and privilege levels, you edit the file /etc/vns_passwd and add users as shown below:

```
########################
root:amdbg:
njones:admb:
bsmith:b:
pnirmel:admbv:
```

Each user is added as a line in the file with the associated privilege levels. In the example above, njones has add, delete, modify, and browse privileges and nsmith has browse (read only) privileges. Save the vns_passwd file after you have added additional VNS users. If the file /etc/vns_passwd does not exist, the VNS Command Line Interface (vnscli) will only operate in the browse mode.

Note The debug privilege 'g' should be reserved for Product Support.

Understanding the VNS Configuration Interface

This chapter provides a description of VNS Configuration Interface, which is used to view, configure, and provision the Voice Network Switching application through a series of inter-linked menus. This chapter concentrates on providing a description of these menus and their respective fields, including the parameters that are entered in them. Chapter 8 provides instructions for using the VNS Configuration Interface to configure a VNS and VNS WAN switching network.

This chapter contains the following sections:

- Accessing the VNS Configuration Interface
- VNS Records
- Configuring the Domain
- Configuring UNI or PBX Addressing
- Configuring Multiple Domains
- Configuring Preferred D Channel Routes
- Cause Code Mapping
- Delete an Entry
- Modify an Entry
- Browse Data Base
- Validate Data Base
- Debug Mode
- Exit the Program
- VNS Parameter Ranges and Defaults

Accessing the VNS Configuration Interface

To access the VNS Configuration Interface, follow these steps:

Step 1 Log in to the VNS through either a telnet session or from a terminal directly connected to the VNS. (Chapter 6 provides instructions for connecting a terminal. You can also telnet from StrataView Plus Workstation.)

Step 2 Log in as `root` and enter the password (if applicable) that you normally use in your UNIX environment.

Step 3 Type *vnscli* (lower case) at the prompt and press Enter. The VNS Configuration Interface main menu, shown in the following example, appears:

```
VNS Configuration Interface Example Main Menu
################################################################################
#                                                                              #
#                   ciscoSystems/StrataCom   V N S                             #
#                 Configuration Interface, Release 3.0.00                      #
#                                                                              #
#     1. Add an entry                                                          #
#                                                                              #
#     2. Delete an entry                                                       #
#                                                                              #
#     3. Modify an entry                                                       #
#                                                                              #
#     4. Browse Data Base                                                      #
#                                                                              #
#     5. Debug Mode                                                            #
#                                                                              #
#     6. Validate Data Base                                                    #
#                                                                              #
#     7. Exit the program                                                      #
#                                                                              #
#     Enter your selection:                                                    #
#                                                                              #
#                                                                              #
#                                                                              #
?###############################################################################
```

Using the VNS Configuration Interface

As shown, the VNS Configuration Interface main menu presents 7 options. Each option is indexed by a number. You select one of the options by typing its number and pressing Enter. For instance, to Add an entry, you would type 1 and press Enter. (Throughout the rest of this book, the VNS Configuration Interface main menu will be referred to simply as the VNS main menu.)

The six options are:

1 Add an entry

2 Delete an entry

3 Modify an entry

4 Browse Data Base

5 Debug Mode

6 Validate Data Base

7 Exit the program

Each option (except no. 7) leads to subsequent menus and screens. These screens normally have a name and a list of fields. Each field is followed by a pair of square brackets, [ ], separated by some blank space. The cursor is positioned between the square brackets which is active for entering information. Many fields accept an index number for the various parameters that can be configured. You move the cursor to the next field by pressing Return. The cursor will skip over read-only fields. The following information line appears at the bottom of most field lists:

```
Enter ‘c’ to commit changes or ’q’ to quit [   ]
```

When using these screens to configure an option, type in the value and press Enter to move the cursor to the next field, the square brackets. When you reach the “**Enter ‘c’ to commit...**”, square brackets, make sure you have entered the desired values in each field, then type c and press Enter to save your changes. When you save your changes, the completed menu becomes a record in the VNS data base. If you do not want to save the values you entered, type q and press Enter. You can re-access the configuration menu from the VNS main menu.

In the Browse Data Base mode, the line at the bottom will read:

```
Enter ‘s’ to skip record or ’q’ to quit [   ]
```

Entering ‘s’ in the square brackets will bring up the next record of the same type.

Some configuration screens will have additional information fields (i.e., a help line at the bottom of the screen) describing a field’s parameters. This information line will change as the cursor is moved from field to field.

To reach any of these screens or menus, follow these steps:

Step 1 From the VNS main menu, enter the index number of desired option.

Step 2 Press Enter, the desired screen or menu will appear.

VNS Configuration Interface Responses

The VNS Configuration Interface communicates with VNS processes using the Simple Network Management Protocol. The responses and error status conform to SNMP standards. The VNS Configuration Interface typically responds to your inputs in three ways:

- With an Operation Successful message when the operation is successfully executed.
- With a Request timed out message when a requested operation has not completed within 30 seconds. Timeout indicates that an SNMP request timed out. This could be because either a port is not responding to an SNMP request or an internal process on the VNS has not responded.
- With an Error Message, similar to the following:

  Response Error: ErrorCode (5), Error Index (1)

Error Messages

Nineteen possible ErrorCodes that could be returned are listed in Table 7-1:

Table 7-1 VNS Configuration Interface Error Codes

Error Code	Description
1	Too Big
2	No Such Value
3	Bad Value
4	Read Only
5	General Error

When using the VNS Configuration Interface, the most common error response is:

Response Error: ErrorCode (3), ErrorIndex (3)

This message typically indicates that you entered an unacceptable value in one of the fields of the menu. The ErrorIndex number points to the first field of the menu containing a bad value. For instance Error Index (1) is the first field on the menu. (Hitting the enter or tab key will step you through the various fields of a menu in their indexed sequence.) When you see this message, you should closely look over all the fields for which you entered values because there could be more than one mistake.

The other common error response is:

Response Error: ErrorCode (5), ErrorIndex (1)

ErrorCode 5 (General Error) indicates there was a logical error while trying to execute the command. In general, it implies that the operation is not allowed to be performed. The ErrorIndex does not have any meaning in this case.

Table 7-2 at the end of this chapter lists the configuration parameters of each menu, along with the index number associated with that field that is returned with VNS Configuration Interface error messages.

VNS Records

Options 1 through 4 of the VNS main menu will access the VNS Records menu. The VNS Records menu is accessed in four ways:

- Choose option 1, **Add an entry**, from the VNS main menu; the VNS Records menu will open blank menus which can be completed and saved. When you save a completed menu, it becomes a record in the VNS database. If a record already exists for a menu that can only have a single record, a message will inform you that you can not add another record.
- Choose option 2, **Delete an entry**, from the VNS main menu; the VNS Records menu will lead to the database of completed menus, that is the individual records. These records appear as completed menus and can be individually deleted.
- Choose option 3, **Modify an entry**, from the VNS main menu; the VNS Records menu will open the completed records in the data base. These menus (records) can be modified and resaved as records.
- Choose option 4, **Browse Data Base**, from the VNS main menu; the VNS Records menu will open the VNS record data base. You can step through these records, which are completed menus, without the danger of changing any fields or deleting any records. Note that when you browse the data base some additional fields appear on a couple records. These additional fields are typically status fields, which are not user-configurable; thus, they do not appear when you are Adding an entry, that is creating a record, in the database.

Note It is good practice to use Browse Data Base after you complete a VNS Configuration Interface menu to recall the record and see if it contains the entered parameters.

Deleting or Modifying Records

When modifying or deleting a VNS record from a batch of records, the VNS Configuration Interface will provide an intermediate menu that will allow you to select the individual record. For instance, it is possible to have a great number of Address records configured in your system. Rather than have to scroll through them to find the record you are seeking, the VNS will provide a menu that allows you to specify the exact record you are seeking. If you selected Delete or Modify and Address record, the following menu will appear:

```
Delete or Modify Menu Example
+##############################################################################+
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   Address            [                                        ]              #
#   Port Descriptor    [                ]                                      #
#                                                                              #
#   Enter the Address and Port Descriptor and press 'd' to                     #
#   delete record, 'b' to browse before deleting or 'q' to quit [   ]          #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
+###############################################################################
```

If you knew the Address and Port Descriptor for the record you wanted to delete or modify, you could enter them directly. If you do not know the specific record information, enter ‘b’ at the prompt and you will enter the Browse mode. The Browse mode allows you to step through the configured records sequentially.

VNS Record Menu Options

The VNS Records menu, shown in the following example, has 16 options. With the exception of option 16, each option leads to a menu or record.

```
VNS Records Menu
################################################################################
#                   ciscoSystems/StrataCom   V N S                             #
#                 Configuration Interface, Release 3.0.00                      #
#                                                                              #
#     1.  VNS Information                                                      #
#     2.  Local Adjacency Information                                          #
#     3.  Network Adjacency Information                                        #
#     4.  Interface Card Information                                           #
#     5.  Address Information                                                  #
#     6.  Network Prefixes Information                                         #
#     7.  Address Screening Information                                        #
#     8.  Transformation Rules Information                                     #
#     9.  Nodes Information                                                    #
#     10. Cards Information                                                    #
#     11. Ports Information                                                    #
#     12. More VNS Info and Redundancy Information                             #
#     13. Multihome port configurations                                        #
#     14. Multihome policy configurations                                      #
#     15. Preferred Route configurations                                       #
#     16. Cause Code Configuration                                             #
#     17. Return to Previous Menu                                              #
#                                                                              #
#     Enter your selection:                                                    #
?###############################################################################
```

Options 1 through 16 of the VNS Records menu lead to the following menus or records:

1 **VNS Information** menu provides configuration information about a specific VNS.

2 **Local Adjacency Information** menu provides information about VNSs that are connected by a frame relay signaling PVC.

3 **Network Adjacency Information** menu provides information about the link (frame relay PVC signaling connection) between two VNS's in the WAN switching network when there is more than one path between them. (This menu is not used in VNS Release 2.1.)

4 **Interface Card Information. (Not supported in this release.)**

Note The Interface Card Information menu is not supported in this software release. When you select this option, you will see an OPTION NOT SUPPORTED, ENTER ANY KEY TO CONTINUE message. Press any key to return to the VNS Records menu.

5 **Address Information** menu describes the addresses, the telephone number in E.164 format, assigned to a UNI port in a VNS's area.

6 **Network Prefixes Information** menu is used assign addresses to VNS areas in the network. These VNS prefixes (or addresses) help to organize the numbering plan for the VNS network.

7 **Address Screening Information** menu specifies the type of source and destination screening applied to each UNI port. Address Screening lists destination addresses that are allowed or not allowed for a specific port.

8 **Transformation Rules Information** menu specifies a list of transformation rules to be applied to a particular UNI port. Each rule consists of a control string that will specify the way in which digits in a telephone number are to be manipulated.

9 **Nodes Information** menu contains information about a node, an IPX or IGX switch, in a VNS's area.

10 **Cards Information** menu contains information about a specific voice card (e.g., a CDP in an IPX switch, or an CVM in an IGX switch) in the VNS's area.

11 **Ports Information** submenu leads to other menus that provide information about the voice ports in a VNS's area. These other menus provide **Port Information** about a specific UNI port in a VNS's area, and **Screening Type Information** for that port.

12 **More VNS Info and Redundancy Information** menu contains information about the VNS and its redundant peer.

13 **Multihome port configurations** menu is used to multihome a pair of E1 UNI ports and select the policy the VNS will use for choosing between those ports.

14 **Multihome policy configurations** menu is used to provide a weight for the Select policy when more than one Select Policy is specified for a multihomed port pair.

15 **Preferred Route Configurations** menu leads to the menus for configuring Preferred Routes for Local Adjacency and UNI Port D-channel connections.

16 **Cause Code Information** menu is used map cause codes for a specific type of PBX. This allows you to specify which cause codes the VNS will send back to a PBX for disconnect, release, or release complete messages.

17 **Return to Previous Menu.**

Menu Order

VNS menus are **not** completed in the numerical sequence (that is their option number) in which they appear on the VNS Records menu. During an initial installation of a Voice Network Switching system, the menus must be completed in a logical sequence. This logical sequence groups the menus into four sequential operations:

- Configuring the Domain
- Configuring the UNI or PBX Addressing
- Configuring Multiple Domains
- Configuring Preferred Routes

Each of the four operations has its own group of menus that must be configured in a particular order. Certain fields of one menu must be completed before subsequent menus can be completed. These fields are linked between menus. Where it is applicable, this chapter will point out the links between the menus. The following sections describe each of the menus in these three logical groups. For each menu, all the fields are listed along with the parameters or options that the field contains. Where a parameter is listed with an index number, such as, **1 = DPNSS**, the default, you only need to enter the index number in that field when completing a menu before moving on to the next field. Other fields will accept text or numerical data from the keyboard; for those fields, we list the range of acceptable values or the length of the character string to be entered. Where applicable the default value of the field is also listed.

Menu Illustrations

In the following sections, the illustration of VNS Configuration Interface menus are taken from both VNS Records **Add an entry** and **Browse Data Base** options. **Add an entry** leads to menus with blank fields that a user must complete. **Browse Data Base** leads to completed records, and are identified by the `Enter ‘s’ to skip record...` line at the bottom. The Browse Data Base records have been used to indicate typical values that are entered in some fields. Although the Browse Data Base records and Add an entry menus are nearly identical, a couple Browse Data Base records have an extra field for status. These status fields are typically not user-configurable and thus do not appear on Add an entry menus. The descriptions of the menus in the following pages will point out the differences between Add an entry menus and Browse Data Base records.

Configuring the Domain

The domain configuration menus must be completed in the following order:

- Nodes Information (option 9 on the VNS Records menu)
- Cards Information (option 10 on the VNS Records menu)
- VNS Information (option 1 on the VNS Records menu)
- More VNS Information (option 12 on the VNS Records menu)

Nodes Information

The Nodes Information menu, shown in the following example, creates records of the node's (IGX or IPX switch) in a VNS's area. It includes the node's IP address through which the VNS will communicate with the node. For the node which is directly attached to the VNS, this IP address is the LAN address of the IGX or IPX switch. For nodes which are not directly attached to the VNS, however, this IP address is typically the Network IP (NWIP) address of remote IGX or IPX switch.

You must create separate Nodes Information records for each node in the VNS's area or domain. (The example menu is actually a Browse Data Base record; the Add an entry Nodes Information Menu will not have the **State of Node** field shown here.) This menu must be completed first because the Node Name field is linked to other menus.

```
Nodes Information Menu
###############################################################################
#                                                                               #
#                                                                               #
#                                                                               #
#                                                                               #
#   Node Name         [ ganges        ]                                         #
#   IP Address        [ 192.168.200.200  ] State of Node     [ 2              ] #
#                                                                               #
#   Enter 's' to skip record   or 'q' to quit  [   ]                            #
#                                                                               #
#                                                                               #
#                                                                               #
#                                                                               #
#                                                                               #
#                                                                               #
#                                                                               #
#                                                                               #
#                                                                               #
#                                                                               #
#                                                                               #
#                                                                               #
?###############################################################################
```

The Nodes Information menu contains the following fields:

- **Node Name**—The unique 10-character IGX/IPX's node name. This must be the configured name of the node as it appears on the node's command line interface.
- **State of Node**—The current state of the node. The possible values are:
  - **0 = unknown**
  - **1 = inService** indicates that the node is fully operational
  - **2 = outOfService** indicates that the node is not operational
  - **3 = NodeReset** indicates that the node has reset and that it will soon appear as inService or outOfService. This value appears only temporarily.

Note The **State of Node** field is a read-only field that only shows up when you **Browse Data Base** and are viewing a completed Nodes Information record.

- **IP Address**—The nodes's IP address in dotted decimal notation. This is typically the LAN address of the node to which the VNS is directly attached and the NWIP address of remote nodes. (Chapter 6 contains information about configuring Network IPs for remote nodes in the section Adding Network IP Routes.)

Cards Information

The Cards Information menu, shown in the following example, contains information about a specific voice or frame relay card (e.g., a CVM in an IGX switch or a CDP in an IPX switch) in the VNS's area. The Nodes Information menu must have been completed before you can complete this menu. You will not be able to delete a Cards Information record if it is being used for redundancy. Also there can not be any ports configured on that card (see Ports Information Submenu) if you want to delete a Cards Information record.

```
Cards Information Example Menu
##############################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   Card Descriptor   [ ganges.8      ]                                        #
#   Card State        [ 1             ]    Card Type         [ 1             ] #
#                                                                              #
#   Enter 's' to skip record   or 'q' to quit  [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?##############################################################################
```

The Cards Information menu contains the following fields:

- **Card Descriptor**—The node.slot. notation that identifies the CDP or CVM in the node.
- **Card State**—The read-only current state of the card. Since this is not a user-configurable field, the cursor will skip over this field. The possible values that will appear in a Cards Information record are:
  - **0 = unknown**
  - **1 = outOfService** indicates that the card is not operational
  - **2 = inService** indicates the card is fully operational and can be used by the VNS
- **Card Type**—Specifies the type of card. It can be:
  - **0 = unknown**
  - **1 = CDP or CVM (or for FRP or FRM for frame relay cards used for SPNNI connections)**

VNS Information

The VNS Information menu, shown in the following example, provides configuration information about a specific VNS. There will be a separate VNS Information screen for each VNS in the VNS WAN switching network. When completing this menu, press Return for fields that do not have to be changed. The Nodes Information and Cards Information menus must have been completed before you complete this menu.

```
VNS Information Example Menu
##############################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   VNS Name          [ vnslab8       ]                                        #
#   Node Name         [ dasipx1       ]                                        #
#   Node IP Address   [ 192.168.200.111  ]                                     #
#   Shut Down Timer   [ 3             ]    Statistics        [ 2             ] #
#   CDR File Count    [ 10            ]    CDR File Interval [ 1             ] #
#   SPNNI Type        [ 1             ]    Compression Type  [ 6             ] #
#   Read Comm String  [ public                           ]                     #
#   Write Comm String [ private                          ]                     #
#   Keep Alive Timer  [ 2             ]    State Change Timer[ 30            ] #
#   RRP_UDP Port      [ 5134          ]    RRP Retry Count   [ 10            ] #
#   Config Redundancy?[ 1             ]    Enable MultiDomain[ 2             ] #
#   Operational Status[ 2             ]    Operational Role  [ 1             ] #
#   VNS IP Address    [ 192.168.4.68  ]    CVM Redundancy    [ 2             ] #
#   Enter 's' to skip record    or 'q' to quit [   ]                           #
#                                                                              #
#                                                                              #
?##############################################################################
```

The VNS Information menu contains the following fields:

- **VNS Name**—A unique 8-character name for this VNS.
- **Node Name**—The name, up to 10 characters, of the IGX/IPX node to which this VNS is directly attached.
- **Node IP Address**—The dotted decimal IP address of the IGX/IPX's LAN port.
- **Shut Down Timer**—Specifies the grace period in seconds allowed for calls to terminate when the VNS is being shut down. The range is 0 to 65535, with a default of 0. Set this to 0 to cause an immediate shutdown.
- **Statistics**—This field is not used in this release. You must enter a 2 or a 3, however.
  - **2** = Statistics generation is **on**, the default.
  - **3** = Statistics generation if **off**.

Note To complete this menu, you must enter one of the options for the Statistic's field. This choice does not affect the operation of the VNS, however.

- **CDR File Count**—Specifies the number of CDR files that the VNS will generate before starting to reuse files, over-writing their content. The range is 1 to 65535, with no default.
- **CDR File Interval**—Specifies the interval in minutes for which a CDR file will be generated. After this interval expires, the VNS will close the currently open file and start writing to the next one. The range is 1 to 65535, with no default.

- **SPNNI Type**—Identifies whether either DPNSS, QSIG, ETS, or AT&T 4ESS ISDN signaling variant is being used. This field is informational only; you fill it in only to help identify your network:
  - — **1 = DPNSS**
  - — **2 = QSIG**
  - — **3 = JISDN (Q931A)**
  - — **4 = Reserved for future use**
  - — **5 = EISDN (European ISDN, also referred to as ETSI)**
  - — **13 = AT&T 4ESS ISDN**

Note If you are using the QSIG protocol package, you must make sure that the SPNNI Type is set to QSIG and that the Port Information submenu's **Stack Type** Field is also set to QSIG.

- **Compression Type**—Specifies the type of voice connection. One type of compression is selected for the entire VNS network. Compression will not be used during data calls. The options are:
  - — **1 = a32** for ADPCM with 32 kbps compression.
  - — **2 = a24** for ADPCM with 24 kbps compression.
  - — **3 = a16** for ADPCM with 16 kbps compression.

    Compressed code avoids all zeros and can be used on lines with no other zero code suppression techniques. Modified 16 kbps technique.
  - — **4 = a16z** for standard 16 kbps ADPCM only. This compressed code can have strings of zeros and must be used only on lines that do not use ZCS (for example, that use B8ZS).
  - — **5 = a32d** used for Enhanced Instafax, which supports high speed circuits but stays at 32 kbps when a high-speed modem is detected. This permits ADPCM compression that would otherwise be unavailable for a modem/FAX circuit.
  - — **6 = c32** for both ADPCM and Voice Activity Detection (VAD) with 32 kbps compression.
  - — **7 = c24** for both ADPCM and Voice Activity Detection (VAD) with 24 kbps compression.
  - — **8 = c16** for both ADPCM and Voice Activity Detection (VAD) with 16 kbps compression.

    Compressed codes avoid all zeros and can be used on lines with no other zero code suppression techniques. 16 kbps compression is non-standard.
  - — **9 = c16z** for standard ADPCM 16 kbps compression and Voice Activity Detection (VAD). This compression can have long strings of zeros and should be used only on trunks that do not use ZCS (for example, that use B8ZS).
  - — **10 = c32d** used for Enhanced Instafax, which supports high speed circuits but stays at 32 kbps when a high-speed modem is detected. This permits ADPCM compression with VAD that would otherwise be unavailable for a modem/FAX circuit.
  - — **11 = p** for a 64 kbps connection with no compression and supports A-law or mu-law encoding and conversion, level adjustment (gain/loss).
  - — **12 = t** for a clean 64 kbps connection with no compression, i.e., clear channel data traffic. Transparent connections treat all bits, including signaling bits, as data bits and disables any gain adjustment conversion that may be specified.

- — **13 = v** for PCM with VAD but no other compression.

Note The VNS provides support for 16k LDCELP connections only between IGX UVM cards. Therefore, once this compression type is specified, it is assumed that all SVCs are being made from UVM to UVM cards. If there are a mixture of CVM/CDP and UVM cards in the WAN switching network, the VNS will automatically fall back to a type of ADPCM compression supported by all card types in the network.

Note Voice connection parameters are described in greater detail in the *Cisco WAN Switching System Overview*, in the Voice Connections chapter of the *Cisco WAN Switching Command Reference*, and in the reference document for the Cisco wide-area switch. For instance, the *Cisco IPX Reference* describes voice connection parameters within the description of the Channelized Data Pad (CDP) card.

- **Read Comm String**—Specifies the Read Community String that has to be used by an SNMP manager sending GET or GETNEXT requests to the VNS. The range is 1 to 32 characters.
- **Write Comm String**—Specifies the Write Community String that has to be used by an SNMP manager sending SET requests to the VNS. The range is 1 to 32 characters.
- **Keep Alive Timer**—Specifies the frequency in seconds that the Role Resolution protocol messages are exchanged between the pair of redundant VNSs. It has a range of 1 to 60, with a default of 5.
- **State Change Timer**—Specifies the period in seconds used by the Role Resolution protocol to change states. It has a range of 10 to 120, with a default of 30. This field is typically not changed from its default.
- **RRP_UDP Port**—Specifies the UDP port number for the Role Resolution protocol to run between the two VNSs. It has a range of 3000 to 65535, with a default UDP port of 5134.

Note When completing the VNS Information menu, typically you do not change the RRP_UDP Port field from its default (5134). Simply press Return when the cursor reaches that field.

- **RRP Retry Count**—Specifies the number of retries before the Role Resolution protocol declares the peer VNS as unreachable. It has a range of 10 to a 100, with a default of 10. Typically the RRP Retry Count should be set to 10 or greater.
- **Config Redundancy?**—Helps configures redundancy for this VNS, by starting the Role Resolution protocol:
  - — **0 = No**, the default.
  - — **1 = Yes**.

  To complete the redundancy configuration, you have to complete the More VNS Info and Redundancy Information menu for both VNSs in the redundant pair. (Chapter 8 contains a procedure for configuring redundancy in the section, Configure Redundancy.)

- **Enable MultiDomain**--This field is used to re-enable multidomain service, when there are two pairs of redundant VNS's controlling different VNS areas, and multidomain service becomes disabled. Multi-domain service could have become disabled when one of the VNS's in a redundant pair went Out of Service and there was a problem bringing the VNS's Frame Relay Port back In Service.

  This Enable MultiDomain field has the following options:

  — **1 = Disabled** (This is a read-only value, it means that Multi-Domain service is enabled but not working. This could mean that the Frame Relay port on the node could not be Uped or that you could not Down the standby VNS Frame Relay port.)

  — **2 = Enable**d. Enter 2 to enable multidomain service if it has become disabled as described above.

  During an initial installation, if you are not using multidomain service, leave this field alone.

- **CVM Redundancy**—Specifies whether or not CVM Redundancy is activated.

  — **1 = Disabled**

  — **2 = Enabled**

Note The CVM Redundancy field (and feature) also applies to UVM cards.

- **Operational Status**—A read-only indicator of the current Operational Status of this VNS. The options are:

  — **0 = Unknown**, the default.

  — **1= outOfService** indicates that the VNS is not operational either due to an error condition or that the VNS had previously been taken out of service

  — **2 = In service** indicates that the VNS is operation but not necessarily processing calls. It could be in standby mode.

- **Operational Role**—A read-only indication of the current Operational Role of the VNS. The values can be:

  — **0 = unknown**, the default.

  — **1 = active** indicates that this VNS is the active VNS of a redundant pair. The active VNS performs all the call processing and configuration updates.

  — **2 = standby** indicates that this VNS is the standby VNS of a redundant pair. The standby VNS waits for the active VNS to fail and will then take over the call processing once the previously active VNS assumes the standby role.

- **VNS IP Address** –A read-only field indicates the IP address in dotted decimal format of this VNS. This field is automatically completed by the VNS.

More VNS Info and Redundancy Information

The More VNS Info and Redundancy Information menu, shown in the following example, provides information for the VNS and its redundant peer. (The Nodes Information and Cards Information must be completed before you complete this menu.) This menu has to be completed for both VNSs in a redundant pair. Make sure the redundant VNS is turned off while configuring the active VNS. When completing the More VNS Info and Redundancy Information menu, make sure to enter the Peer IP Address correctly. Also make sure to set the Admin Role to 1 (active). Save the record.

Open and complete another More VNS Info and Redundancy Information record that corresponds to the peer VNS. Enter the Peer IP Address so that it points back to the Active VNS. Set the Admin Role to 2 (standby). Save the record.

When these records have been completed, you can turn on the redundant (peer) VNS.

An active redundancy record for the active VNS must exist, you can not delete it. Also you cannot delete a standby redundancy record when the standby VNS is In Service.

```
More VNS Information and Redundancy Information Example Menu
##############################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   VNS Name          [ vnslab8       ]                                        #
#   Voice Port#1      [ dasipx1.4.1      ]                                     #
#   Voice Port#2      [                  ]                                     #
#   Frame Relay Port  [ dasipx1.5.1      ]                                     #
#   Operational Status[ 2             ]    Operational Role  [ 1             ] #
#   Admin Status      [ 1             ]    Admin Role        [ 1             ] #
#   Peer IP Address   [ 0.0.0.0          ]                                     #
#   VNS FR-IP Address [ 0.0.0.0          ]                                     #
#   Peer FR-IP Address[ 0.0.0.0          ]                                     #
#                                                                              #
#   Enter 's' to skip record   or 'q' to quit  [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?##############################################################################
```

The More VNS Info and Redundancy Information menu contains the following fields:

- **VNS Name**—A unique 8-character name for this VNS.
- **Voice Port #1**—The ID (node.slot.port) of the voice card (e.g., CVM on an IGX switch or CDP on an IPX switch) which is directly attached to the E1 NIC card. This field is linked to the Nodes Information and the Cards Information menus.
- **Voice Port #2**—The ID (node.slot.port) of the voice card (e.g., CVM on IGX switch or CDP on the IPX switch) which is directly attached to a second E1 NIC card in this VNS.
- **Frame Relay Port**—The ID (node.slot.port) of the Frame Relay Port (e.g., FRP card on the IPX switch) to which the Frame Relay (RS422 to V.35) card is directly attached.

- **Operational Status**—A read-only indicator of the current Operational Status of this VNS. Since this is not a user-configurable field, the cursor will skip over it. The possible values in a More VNS Info and Redundancy Information record are:
  - **0 = unknown**.
  - **1= outOfService** indicates that the VNS is not operational either due to an error condition or that the VNS had previously been taken out of service.
  - **2 = In service** indicates that the VNS is in operation but not necessarily processing calls. It could be in standby mode.
- **Operational Role**—A read-only indication of the current Operational Role of the VNS. Since this is not a user-configurable field, the cursor will skip over it. The possible values in a More VNS Info and Redundancy Information record are:
  - **0 = unknown**.
  - **1 = active** indicates that this VNS is the active VNS of a redundant pair. The active VNS performs all the call processing and configuration updates.
  - **2 = standby** indicates that this Voice is the standby VNS of a redundant pair. The standby VNS waits for the active VNS to fail and will take over the call processing once the previously active VNS assumes the standby role.
- **Admin Status**—Used to change the Operational Status of the VNS. The options are:
  - **1 = outOfService** brings the VNS to an off-line state where the configuration can be updated.
  - **2 = inService** indicates that the VNS is to be brought into an operational state. Its role being indicated by Operational Role.
  - **3 = resetConfig** will cause the VNS to read a new configuration from disk.
  - **4 = shutdown** shut downs the VNS after the grace period indicated by Shut Down Timer.
- **Admin Role**—Used to change the Operational Role of a VNS in a redundant pair. The options are:
  - **1 = active** to cause a change from standby to active which causes the standby VNS to take over all call processing once the previously active VNS assumes the standby role.
  - **2 = standby** to cause a change from active to standby which causes all the calls on the active VNS to become terminated and the standby VNS to become active.
- **Peer IP Address**—Specifies the IP address in dotted decimal format of the other (the peer) VNS in a redundant pair.
- **VNS FR-IP Address**—This field is not used. Skip over this field. It has an address of 0.0.0.0 in the VNS records.
- **Peer FR-IP Address**—This field is not used. Skip over this field. It has an address of 0.0.0.0 in the VNS records.

Configuring UNI or PBX Addressing

The UNI (User Network Interface) or PBX addressing configuration menus must be completed in the following order:

- Ports Information (option 11 on VNS Records menu)
- Address Information (option 5 on the VNS Records menu)
- Address Screening Rules (option 7 on the VNS Records menu)
- Transformation Rules (option 8 on the VNS Records menu)
- Multihome Port Configurations (option 13 on the VNS Records menu)
- Multihome Policy Configurations (option 14 on the VNS Records menu)

Ports Information Submenu

The Ports Information submenu, shown in the following example, leads to other menus that provide information about the UNI ports in a VNS's area.

```
Ports Information Menu
################################################################################
#                                                                              #
#                   ciscoSystems/StrataCom   V N S                             #
#                 Configuration Interface, Release 3.0.00                      #
#                                                                              #
#     1. Port Information                                                      #
#                                                                              #
#     2. Screening Type Information                                            #
#                                                                              #
#     3. Return to Main Menu                                                   #
#                                                                              #
#     Enter your selection:                                                    #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?###############################################################################
```

The Ports Information menu contains the following options:

1 **Port Information**

2 **Screening Type Information**

3 **Return to Previous menu**

To access one of the options, enter the selection index number and press Enter.

Port Information

The Port Information menu, shown in the following example, creates a record information about a UNI port in a VNS’s area. You must create one of these records for each UNI port in the VNS’s service area. The Nodes Information and Cards Information menus must have already been completed before you can complete this menu.

```
Port Information Example Menu
################################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   Port Descriptor   [ vnsigx11.9.1  ]                                        #
#   Port Type         [ 1             ]    Port State        [ 2             ] #
#   UNI Channel       [ 16            ]    VNS Channel       [ 1             ] #
#   First Channel     [ 1             ]    Last Channel      [ 31            ] #
#   Channel Alloc Role[ 3             ]    Channel Allocation[ 3             ] #
#   Interface ID      [ 1             ]                                        #
#   Statistics        [ 2             ]    Stats Interval    [ 60            ] #
#   Stack Type        [ 13            ]    Record Oper State [ 0             ] #
#   PBX Type          [ seimenspbx    ]                                        #
#                                                                              #
#   Enter 's' to skip record   or 'q' to quit  [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?###############################################################################
```

The Port Information menu contains the following fields:

- **Port Descriptor**—The node.slot.port notation that identifies the specific UNI port.
- **Port Type**—The type of UNI port. The options are:

  — **1 = UNI** (User Network Interface)

  Other values are reserved for future use.
- **Port State**—The read-only current state of the port. The values can be:

  — **0 = unknown**.

  — **1 = outOfService** indicates that the port is not operational, which is the default.

  — **2 = inService** indicates that the port is fully operational and can be used by the VNS.
- **UNI Channel**—The logical channel (1 -31) of the signaling channel on the UNI. This logical channel corresponds to the E1 timeslot (TS), typically TS16, carrying signaling information between the PBX and the VNS WAN switching network. (For CAS to QSIG conversion, the UNI Channel is 25 as described in Appendix I, Channel Associated Signaling Voice Switching.)
- **VNS Channel**—The logical channel (1-31) on the E1 NIC in the VNS carrying the signaling information from the node to the VNS. Since all 30 of the E1 NIC’s logical channels (timeslots) are used to carry signaling information from a UNI port (i.e., a PBX) to the VNS, any of these logical channels can be assigned. (The user should keep track of which signaling channel is assigned to which voice port.)
- **First Channel**—The first channel in the range of channels on this UNI port available for user data. This is similar to the first channel in a hunt group. The range is 1 to 31.

- **Last Channel**—The last channel in the range of channels on this voice port available for user signaling. This is similar to the last channel in a hunt group. The range is 1 to 31.
- **Channel Alloc Role**—This field is incorrectly named. It should be renamed LAP role A/B. For all protocols, a side A can only be established with a side B. The options are:
  - — **1 = unknown**
  - — **2 = side B (slave or user)**
  - — **3 = side A (master or network)**

Note DPNSS X - Y is not configurable. Side A is always side x and side B is always side y.

Note With CAS signaling, as described in Appendix I, Channel Associated Signaling Voice Switching, the protocol is operating between the IGX's UVM card and the VNS. The UVM always performs the master role, so the VNS must be set to slave.

- **Channel Allocation**—This field is incorrectly named. It should be thought of as channel assignment. It specifies the direction (from low-to-high or from high-to-low) which the VNS will assign channels for calls from a PBX. Low end specifies that channels are assigned from the First Channel to the Last Channel; high end specifies that channels are assigned from the Last Channel to the First Channel. (First and Last Channels were specified in previous fields of this menu.) The options are:
  - — **1 = unknown**
  - — **2 = low end** (from low to high channels, such as from 1 to 31, or from whatever channel was specified as First Channel to the Last Channel)
  - — **3 = high end** (from high to low channels, such as from 31 to 1, or from whatever channel was specified as Last Channel to the First Channel)

Note For ISDN preferred/exclusive is not configurable. For incoming requests both preferred and exclusive will be processed. All outgoing calls are exclusive.

- **Interface ID**—The ID of the E1 NIC voice port connected to this UNI port.
  - — **1 = Voice Port 1 (**E1 NIC 1, whose location is shown in Figure 6-2**)**
  - — **2 = Voice Port 2** (E1 NIC 2, whose location is shown in Figure 6-2**)**
- **Statistics**—This field is not used in this release. The options are:
  - — **2 = on**
  - — **3 = off**

Note To complete this menu, you must enter one of the options for the Statistic's field. This choice does not affect the operation of the VNS, however.

- **Statistics Interval**—Specifies the interval, in minutes, at which statistics for this port are written to file, when statistics generation is turned on. The range is 1 to 65535. (Note that statistics are not collected in this release.
- **Stack Type**—This field specifies the signaling stack (i.e., protocol variant) that this UNI port will use. When Break-Out/Break-In is not used, this field must be set to match the protocol type your VNS WAN switching network is running. If this port is going to be used as the Break-Out/Break-In port, you select 5, ETSI. The options are:
  - **1 = DPNSS**
  - **2 = QSIG**
  - **3 = JISDN (Q931A)**
  - **4 = Reserved for future use**
  - **5 = EISDN (European ISDN, also referred to as ETSI).** This is the option when the port is used as the Break-Out/Break-In port.
  - **13 = AT&T 4ESS ISDN**
- **Record Operational State—**This field is used to monitor the operation being performed on the port record. Currently only the delete operation is monitored. When a port is being deleted, all the addresses configured for that port have to be deleted before the port can be deleted. This can take several minutes. This field indicates the progress of the deletion. You have to exit and re-enter the menu to see the updated status of this field. On success of a delete operation, the value is set to on unsuccessful it is set to 4. The possible values are:
  - 0 = successful
  - 1 = adding
  - 2 = deleting
  - 3 = modifying
  - 4 = unsuccessful

  You can delete a record only when it is in the 0 or 4 state. Once a port has been deleted the port record will no longer be accessible.
- **PBX Type**—This field creates a cause code file associated with this port. To create a file, you enter a 1 to 16 character text string, such as “seimenspbx” in the field. The cause code file can be used to map cause codes to a particular cause code for your PBX type. Once the cause code file has been created, you use option 16, Cause Code Information, on the VNS Record menu to modify the default cause code mapping for your particular PBX. For information on modifying, the default cause code file, see the Cause Code Mapping.

  A typical use of the PBX Type field is to create a cause code file for a specific type of PBX, then reference that file, by entering the appropriate PBX Type, for each PBX of the same type in your network.

Screening Type Information

Screening allows you to screen addresses, that is, filter calling party and called party numbers. In other words, you can create lists of numbers from which or to which you will allow calls, or lists of numbers from which or to which you will not allow calls. Using the Screening Type Information menu, shown in the example, you can select the type of screening you are going to do for calling parties (that is, source) or the called parties (that is, destination) for a UNI port. (The Address Screening Information menu is used to specify the actual addresses that are going to be screened.) Typically, you use this menu to select the type of screening which will allow you to create the shorter screening list. For example, if you have a small number of addresses (called party numbers) to which you do not want to allow calls, you would select Destination Screen Type disallowed; then use the Address Screening Information menu to specify these addresses.

```
Screening Type Information Example Menu
##############################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   Port Descriptor    [dasigx1.7.1    ]                                       #
#   Source Screen Type [2              ]   Destination Screen [2              ]#
#                                                                              #
#   Enter 'c' to commit changes or 'q' to quit [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?###############################################################################
```

The Screening Type Information menu contains the following fields:

- **Port Descriptor**—The UNI port ID (node.slot.port) of the port for which you are going to screen addresses (that is, calling and called party numbers).
- **Source Screen Type**—The type of source (calling party) screening configured. Screening types, which are configured with the Address Screening Information menu, can be either:
  - **1 = allowed** to indicate that the screening identifies addresses, which will be specified with the Address Screening Information menu, that are permitted from this port.
  - **2 = disallowed** indicates that the screening identifies addresses, which will be specified with the Address Screening Information menu, that are not permitted from this port.
- **Destination Screen**—The type of destination (called party) screening configured for this port. The screening types are:
  - **1 = allowed** to indicate that the screening identifies addresses, which will be specified with the Address Screening Information menu, that are permitted to this port.
  - **2 = disallowed** to indicate that the screening identifies addresses, which will be specified with the Address Screening Information menu, that are not permitted on this port.

Address Information

The Address Information menu, shown in the following example, describes the addresses, the telephone number format, assigned to a UNI port in a VNS's area. When you browse the Address Information records, they will be displayed in a sorted, descending order. For example, Address 8000 will be displayed before Address 7999, which will be displayed before Address 900, and so on.

The Nodes Information, Cards Information, and Ports Information menus must be completed before you can complete this menu.

```
Address Information Example Menu
##############################################################################
#                                                                              #
#                                                                              #
#   Address            [069******                               ]              #
#   Port Descriptor    [dasigx1.7.1     ]                                      #
#                                                                              #
#   Enter 'c' to commit changes or 'q' to quit [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   KEY: The address configured on the local VNS.                              #
#                                                                              #
#                                                                              #
?##############################################################################
```

The Address Information menu contains the following fields:

- **Address**—An address, i.e.a telephone number, for a UNI port in this VNS's area. An address can be a string of 1 to 40 digits or characters.

  When the QSIG protocol is used, to avoid having to enter very complex numbering plans and to speed up the call routing process, the VNS allows the use of wildcards (that is, the * symbol) in an address. For instance, you could enter Address 069***** to route all calls beginning with 069 to the PBX attached to UNI port dasigx1.7.1.

  For exceptions you add another Address Information record, specifying the complete address and port. For instance, you could add Address 069-123456 and Port Descriptor dasigx1.6.1 and Address 069124*** and Port Descriptor dasigx1.5.1 to route those calls to different PBX's.

  When using wildcards, you must observe the following rules:

  — All addresses must start with a digit.

  — The exception digits cannot exceed the length of the default string. That is, if the default entry is 069*** (7 digits), any specific entries have to be 7 digits or less. If the specific entry is less than 7 digits, use the wildcard symbol (*) to fill out the string, such as 069124***. In other words, the default string must be as long or longer than the largest exception.

  — One wildcard symbol needs to be entered for every digit that needs to be processed. For example, **** indicates four digits.

  — The wildcard symbols must be entered as consecutive digits. Thus, 069****** is allowed, but 069**5*** is not allowed.

- **Port Descriptor**—The port ID (node.slot.port) on the node (IGX/IPX switch) of the UNI port for which the specified address/telephone number is configured.

Address Screening Information

The Address Screening Information menu, shown in the following example, is used together with the Screening Type Information menu to create the lists of called party (that is, source) and calling party (that is, destination) addresses that you are going to filter (allow or disallow) for the specified UNI port. The Screening Type Information must have been completed before you can complete this menu. This menu specifies the address (that is, the called or calling party number) that is allowed or not allowed for a specific port, while the Screening Type Information menu specifies the type of screening that will be performed. This menu creates one record for your screening list. You must complete one record for each number you want to screen.

```
Address Screening Information Example Menu
##############################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#              Address Screening Rule                                          #
#   [5551234                                    ]                              #
#   Port Descriptor    [dasigx1.7.1     ]                                      #
#   Screening Type     [2              ]                                       #
#                                                                              #
#   Enter 'c' to commit changes or 'q' to quit [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   KEY: The address screening rule.                                           #
#                                                                              #
#                                                                              #
?###############################################################################
```

The Address Screening Information menu contains the following fields:

- **Address Screening Rule**—The full 20-byte address, a prefix, or a partial address that will be screened (that is, filtered) at the specified UNI port. The rule is entered as a string of 1 to 30 digits or characters.
- **Port Descriptor**—The UNI port ID (node.slot.port) notation on the node (IGX/IPX switch) to which the screening rule will be applied.
- **Screening Type**—Specifies the type of address screening implemented for this port. Screening can be applied as a source (calling party) screen, a destination (called party) screen, or both a source and destination screen. The indexed options are:
  - — **0 = unknown**
  - — **1 = source screening** (calling party filtering)
  - — **2 = destination screening** (called party filtering)
  - — **3 = both source and destination screening** (both calling party and called party filtering)

Transformation Rules Information

The VNS provides address (that is, number) translation to route public network telephone numbers over a VNS private networks. This translation feature can be used to translate a public number to a private number for Break-In and a private number to a public number for Break-Out. (The Break-Out/Break-In feature is described in Chapter 1 in the section, Break-Out/Break-In Feature.)

The Transformation Rules Information menu, shown in the following example menu, specifies the way a number is transformed, that is converted from one number to another. Transformation rules applied to a particular UNI port and can be applied to calling party or called party numbers. The Nodes Information, Cards Information, and Ports Information menus must be completed before you can complete this menu.

Transformation rules can not be applied between VNS domains.

```
Transformation Rules Information Example Menu
##############################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   Port Descriptor    [dasigx1.7.1     ]                                      #
#   Priority           [1              ]                                       #
#                                                                              #
#             Pattern to Locate                                                #
#   [^123                                       ]                              #
#             Pattern to be Replaced                                           #
#   [$0                                         ]                              #
#             Replacement Digits                                               #
#   [1234                                       ]                              #
#   Direction          [4              ]   Application        [3              ]#
#                                                                              #
#   Enter 'c' to commit changes or 'q' to quit [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#   KEY: The port descriptor to which transformation rule is to be applied     #
#                                                                              #
#                                                                              #
?##############################################################################
```

The Transformation Rules Information menu contains the following fields:

- **Port Descriptor**—The UNI port ID (node.slot.port) of the port to which the transformation is to be applied.
- **Priority**—A unique number that identifies this transformation rule record. There can be multiple Transformation Rules associated with a single UNI port. You must assign a unique Priority number for each record that you complete for a specified port. (This field does not determine the priority with rules are applied.) The range is 1 to 65535.
- **Pattern to Locate**—The pattern of digits that are to be located in an address before the Transformation Rule can be applied. It also specifies where in the Address these strings can be located. For instance, the character “^” included in the pattern indicates that the remaining digits are to be located at the start of the address. The character “$” indicates that the remaining digits are to be located at the end of the address. For example, if you wanted to transform numbers beginning with the digits “123”, you would enter “^123” in this field. The range is 0 to 40 digits or characters.

- **Pattern to be Replaced**—The pattern of digits that are to be replaced in an address and the location of these digits in the address. For instance, the character “^” in the pattern indicates that the remaining digits are to be located at the start of the address. The character “$” indicates that the remaining digits are to be located at the end of the address. For example, if you wanted to replace the digit “0” at the end of a string, you would enter “$0” in this field. The range is 0 to 40 digits or characters.
- **Replacement Digits**—Specifies the digits that are to replace the digits listed in the Pattern to be Replaced field. For instance, if you want to replace the “0” in the Pattern to be Replaced field with the digits “1234”, you would enter “1234” in this field. The range is 0 to 40 digits.
- **Direction**—Species the direction of the calls to which the Transformation Rules are to be applied. The options are:
  - **2 = inComing** specifies calls that originate on the specified UNI port.
  - **3 = outGoing** specifies calls that terminate on the specified UNI port.
  - **4 = both directions**.
- **Application**—Specifies the different addresses in a call request that the transformation Rule is to be applied to. It is a bit mask with each bit indicating the following:
  - bit 0—called party number (the decimal equivalent is 1; thus enter 1 for called party).
  - bit 1—calling party number (the decimal equivalent is 2; thus enter 2 for calling party).

Note There are not other types of addresses supported by the Application field.

If any bit is set then the Transformation Rule will be applied to that number. Although the Application field is implemented as a bit mask, it is entered as a decimal number, with a range of 0 to 65535. Therefore to select “called party number,” you would enter 1, and to select “calling party number,” you would enter 2. To select both “calling party number” and “called party number”, you would enter 3, the sum of the decimal equivalent of the two set bits.

Wildcard Translations

The wildcard ‘*’ character is supported in translation patterns. To use wildcard translations, follow these guidelines:

- There can be one contiguous stream of wildcard characters in a given pattern. For instance 55****55 is ok, but 55**3**55 is not ok.
- A pattern must not start with a wildcard character.
- When a wildcard stream is embedded between to digit streams, a wildcard character matches only one digit (between 0 and 9) at a time. For example, in 77888***001, each * represents one digit that needs to be translated.
- A trailing wildcard string when present also matches one digit to one wildcard character that follows the digits the wildcard string the is translating. For example. in 77888*, the trailing * matches one digit beyond 77888.
- The translated to number may or may not have the same number of digits as the translated from number.
- Each wildcard * in the number that is being translated can only represent one single digit that needs translation.

The use of wildcards greatly simplifies the use of transformation rules. For instance, if you wanted to translate all the numbers between 200 and 299 to the same address, without wildcards you would have to create 100 Transformation Rule records, one for 200, another for 201, another for 202....until you reached 299. With wildcards, a single record can use 2** to translate all the numbers between 200 and 299.

Translation Limitations

The number of digits in a translation rule should not exceed the number of digits in a local or network address or the call will be routed before the number is translated. Also if the number coming in to be translated does not match a route address, the call will be rejected when the first number that does not match is found. Thus a call which needs to be translated, could be rejected before the translation has been performed.

To avoid these limitations, careful planning of network addressing and transformation rules is necessary.

Multihome Port Configurations

The Multihome Port Configurations menu, option 13 on the VNS Records menu, shown in the following example, is used when configuring Multihomed E1 UNI port pairs. Multihoming E1 Ports is described in Chapter 1 in section Multihomed E1 Links. Multihomed ports typically have the same address configured for them and are used to increase the hit ration of successful calls to a specific address, load-sharing, or backup for a particular link.

You must create one of these records for each of ports in a multihomed pair. For instance, to multihome dasigx2.7 to dasigx2.8, after committing the record shown below, you would create a record for dasigx2.8 with dasigx2.7 as the multihomed port, also with a select policy of 8. If you were going to multihome 3 UNI ports, A, B, and C, you would complete 6 Multihome Port Configuration records. Two for A & B, two for B & C, and two for A & C.

The Nodes Information, Cards Information, and Ports Information menus must already have been configured before you can complete this menu.

```
Multihome Port Configurations Example Menu
##############################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#         CPE Port                                                             #
#   [dasigx2.7        ]                                                        #
#   Multihomed Port   [dasigx2.81     ]                                        #
#   Select Policy     [8      ]                                                #
#                                                                              #
#   Enter 'c' to commit changes or 'q' to quit [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?##############################################################################
```

This menu includes the following fields:

- **CPE** Port specifies in Cisco Node.Slot.Port notation the first port in the multihomed pair. This port is considered the primary port of multihomed pair.
- **Multihomed Port** specifies in Cisco Node.Slot.Port notation the port being multihomed to the primary port.
- **Select Policy** specifies the type of selection criteria the VNS will use to determine which of these ports to route a specific call to. The Select Policy is entered as an index number indicating:
  - — **1**= A round-robin alternation between each port
  - — **2** = Port with most bandwidth available
  - — **4**= Port with the least amount of transients (that is the fewest amount of calls to it)
  - — **8**= Or port with least errors

Multihome Policy Configurations

The Multihome Policy Configurations menu, option 14 on the VNS Records menu, shown in the following example, is used to provide a weight for a Select Policy when more than one Select Policy is specified for a multihomed port pair. Multihoming E1 Ports is described in Chapter 1 in section Multihomed E1 Links.

The Nodes Information, Cards Information, and Ports Information menus must already have been configured before you can complete this menu.

```
Multihome Policy Configurations Example Menu
##############################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#      Port Description                                                        #
#   [dasigx1.7.1       ]                                                       #
#   Policy            [8       ]                                               #
#   Weightage         [100     ]                                               #
#                                                                              #
#   Enter 'c' to commit changes or 'q' to quit [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   KEY: The port descriptor where the policy is linked.                       #
#                                                                              #
#                                                                              #
?##############################################################################
```

This menu includes the following fields:

- **Port Description** specifies which port in Cisco Node.Slot.Port notation to which you want to weight a specific Selection Policy for the VNS’s port selection process.
- **Policy** indicates the index number (1, 2, 4, or 8 as described in the previous section Multihome Port Configurations) selected for the specified port.
- **Weightage** indicates the amount of weight (between 0 and 100) that the VNS should apply to the specific Select Policy. 0 (zero) indicates no weight and will never be taken into account; 100 is full weight and will always be the first consideration.

  On a specific port, each of the Select Policies could be assigned a different weight. When there are more than one pair of multihomed ports configured for the same primary port, the VNS will consider all the selection policies and all of their weights before routing a call to a specific port.

Configuring Multiple Domains

The multiple domain configuration menus must be completed in the following order:

- Local Adjacency Information (Option 2)
- Network Prefix Information (Option 6)
- Network Adjacency Information (Option 3) (not used in VNS Release 2.1)

Naturally if there were only a single VNS domain in your VNS WAN switching network, these menus would not have to be completed.

Local Adjacency Information

The Local Adjacency Information menu, shown in the following example, provides information about locally adjacent VNS's, that is VNS's controlling separate VNS domains and connected to one another through a Frame Relay PVC (that is, a SPNNI connection). After committing this record, the VNS instructs the node (IGX or IPX switch) to build the Frame Relay connection to the remote VNS. (The example is actually a Local Adjacency Information record; the VNS State field will not appear on the Local Adjacency Information menu.) Local Adjacency menus have to completed at both ends of the SPNNI connection. (Chapter 8 contains an example of counterpart Local Adjacency records in the section Local Adjacency Example.)

Note In this release, the VNS signaling is done over a full-mesh network. Every VNS has a frame relay PVC to every other VNS controlling a separate domain in the network. Thus every VNS is considered "locally adjacent" to every other VNS.

```
Local Adjacency Information Example Menu
##############################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   VNS Name          [ boysen        ]    Standby VNS Name  [               ] #
#   Local Port Type   [ 3             ]    Local DLCI        [ 100           ] #
#   Remote Port Desc  [ dasigx1.4.1   ]    Remote DLCI       [ 200           ] #
#   Link Weight       [ 1             ]    VNS State         [ 0             ] #
#   Rmt Stby Port Desc[               ]                                        #
#                                                                              #
#   Enter 's' to skip record   or 'q' to quit  [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?###############################################################################
```

This menu contains the following fields:

- **VNS Name**—The unique 8-character name of the adjacent VNS.
- **Standby VNS Name**—The unique 8-character name of the adjacent VNS's peer unit. This field has to be completed when the adjacent VNS is part of a redundant pair.
- **Local Port Type**—The type of frame relay port. It can be configured as either network or user Cisco Proprietary Network-to-Network Interface (SPNNI, N-SPNNI or U-SPNNI). The two ends of a frame relay signaling PVC must be configured differently for a connection to be established, i.e., one end must be u-spnni and the other must be n-spnni. To select the Local Port type, enter one of the following index numbers:
  - **2 = U-SPNNI.**
  - **3 = N-SPNNI.**
- **Local DLCI**—The DLCI at the local VNS of the frame relay PVC to the locally adjacent VNS. The factory default range of DLCIs reserved for the Local DLCI is 101 to 113. If you need to use a DLCI which is not in this default range, you will have to add the DLCI to the fr_conv file as is described in Chapter 6 in the section, Modifying the Default Range of VNS DLCIs.
- **Remote Port Desc**—Port ID (node.slot.port) on the node (IGX/IPX switch) connected to the remote VNS used to establish the frame relay PVC with the local VNS. In other words, this is the remote Node's port ID which is connected to the remote VNS's Frame Relay Card.
- **Remote DLCI**—The DLCI at the remote VNS of the frame relay PVC between locally adjacent VNS's. The factory default range of DLCIs reserved for the Local DLCI is 101 to 113. If you need to use a DLCI which is not in this default range, you will have to add the DLCI to the fr_conv file in the remote VNS as is described in Chapter 6 in the section, Modifying the Default Range of VNS DLCIs.
- **VNS State**—The read-only Operational Status of the adjacent VNS. This status field appears on Local Adjacency Information record, but does not appear on the Local Adjacency Information menu. This field can be:
  - **0 = unknown**, the default.
  - **1 = outOfService** indicates that the VNS has lost connection to the adjacent VNS. This may or may not be because the VNS has gone out of service.
  - **2 = inService** indicates that the VNS is fully operational.
- **Link Weight**—This field is reserved for future use and has no effect. The range is 1 to 65535, with a default of 1. It will accept any value, but should be left at its default.
- **Rmt Stby Port Desc**--Port ID (node.slot.port) on the node (IGX/IPX switch) connected to the remote VNS's peer unit's Frame Relay Port. In other words, this is the remote nodes Port ID which is connected to the remote VNS's peer's Frame Relay Port. This field has to be completed only when the adjacent VNS is part of a redundant pair.

Note Since the VNS frame relay signaling network is full mesh, every link (i.e., frame relay PVC between VNSs) will have the same weight or preference.

Network Prefixes Information

The Network Prefixes menu, shown in the following example, is used to organize addresses in VNS areas in the network. These VNS prefixes (or addresses) help to organize the numbering plan for the VNS WAN switching network. Unique prefixes are typically assigned to each VNS area, much like an area code in plain old telephone service (POTS).

```
Network Prefixes Information Example Menu
###############################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   Network Address   [ 30                                       ]             #
#   VNS Name          [ boysen        ]                                        #
#                                                                              #
#   Enter 's' to skip record   or 'q' to quit  [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?###############################################################################
```

The Network Prefixes Information menu contains the following fields:

- **Network Address**—The address prefix for a specific VNS area. A prefix can be a string of 1 to 30 characters or digits.
- **VNS Name**—The unique 8-character name of the VNS area to which the address prefix is assigned.

Network Adjacency Information

This menu is reserved for use when the VNS supports alternate signaling links between VNS areas. It can not be used in VNS Release 2.1.

The Network Adjacency Information menu, shown in the following example, provides information about the link (frame relay PVC signaling connection) between two VNSs in the network.

Note In this release, where a full-mesh signaling network is required, this menu has no use. Do not complete it.

```
Network Adjacency Information Example Menu
##############################################################################

#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   First VNS Name     [dasigx1        ]   Second VNS Name    [dasigx2        ]#
#   Link Weight        [1              ]                                       #
#                                                                              #
#   Enter 'c' to commit changes or 'q' to quit [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   KEY: Unique name of the first VNS, up to 8 chars long                      #
#                                                                              #
#                                                                              #
?##############################################################################
```

This menu contains the following fields:

- **First VNS Name**—The unique 8-character name of the first VNS of an adjacent pair.
- **Second VNS Name**—-The unique 8-character name of the remote VNS of an adjacent pair.
- **Link Weight**—The weight/preference assigned to the link (i.e., frame relay PVC) between the adjacent VNSs. The range is 1 to 65535, with a default of 1. (This field is not used in this release.)

Configuring Preferred D Channel Routes

The Preferred Route Configurations menu leads to menus that let you specify a preferred route for the signaling channel between a UNI port and the VNS, or between two locally adjacent VNS's. The VNS system adds these preferred routes as signaling PVCs in the network. Preferred routing of these signaling channels provides the flexibility needed to avoid network congestion, and to provide load balancing and resiliency across network trunks.

Note Preferred routes will fail if a trunk they are traversing fails, such as when the trunk is deleted or upped but not added.

From the Preferred Route Configurations menu, shown in the following example menu, you can select either:

1 Local Adjacency Preferred Route Information

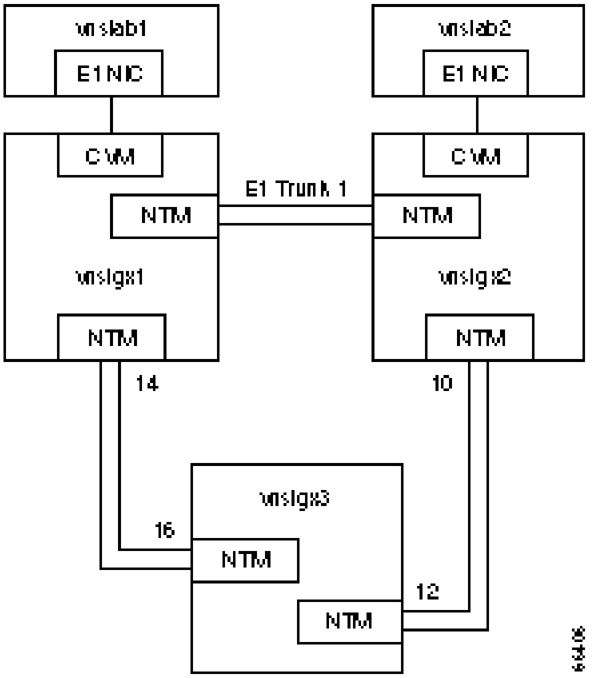
2 Port Preferred Route Information

```
Preferred Route Configurations Example Menu
################################################################################
#                                                                              #
#                   ciscoSystems/StrataCom   V N S                             #
#                 Configuration Interface, Release 3.0.00                      #
#                                                                              #
#     1. Local Adjacency Preferred Route Information                           #
#                                                                              #
#     2. Port Preferred Route Information                                      #
#                                                                              #
#     3. Return to Main Menu                                                   #
#                                                                              #
#     Enter your selection:                                                    #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?###############################################################################
```

Local Adjacency Preferred Route Information

The Local Adjacency Preferred Route option allows you to specify a preferred route for a SPNNI connection between two locally adjacent VNS's. Local Adjacency must be configured with the Local Adjacency Information menu before you can configure a preferred route. Figure 7-1 provides a simple example where the Local Adjacency Preferred Route option could be used. In this example, rather than use E1 Trunk 1, you want to route the SPNNI channel between vnslab1 and vnslab2 (that is, the locally adjacent VNS's) through vnsigx3. The numbers in the example indicate the IGX slot number of the NTMs, that is, the trunk cards. For instance, the 14 below vnsigx1 indicates that the NTM (that is, the trunk card is in slot 14.

Figure 7-1 Local Adjacency Preferred Route Example



You use the Local Adjacency Preferred Route Information menu, shown in the following example menu, to configure a preferred local adjacency route. The Local Adjacency Preferred Route record must be configured on both of the locally adjacent VNS's.

```
Local Adjacency Preferred Route Information Example Menu
##############################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   Remote VNS Name  [ vnslab2       ]                                         #
#   Local VNS Name   [ vnslab1       ]                                         #
#   Local node       [ vnsigx1.14    ]    Remote node      [ vnsigx2       ]   #
#   1st Hop          [ vnsigx3.12    ]    2nd Hop          [               ]   #
#   3rd Hop          [               ]    4th Hop          [               ]   #
#   5th Hop          [               ]    6th Hop          [               ]   #
#   7th Hop          [               ]    8th Hop          [               ]   #
#   9th Hop          [               ]                                         #
#   Enter 's' to skip record  or 'q' to quit   [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?###############################################################################
```

The Local Adjacency Preferred Route Information menu contains the following fields:

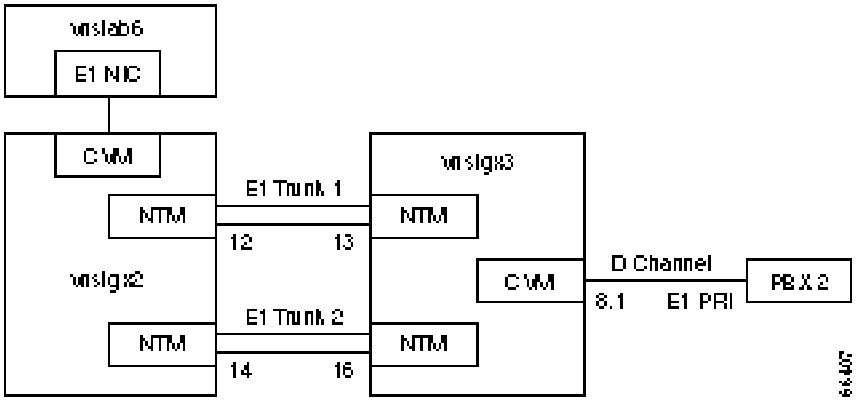
- Remote VNS Name is the configured name of the remote VNS, such as, vnslab2 from the example.
- Local VNS Name is the configured name of this VNS, such as vnslab1 from the example.
- Local Node is the node (IGX or IPX switch) to which this VNS is connected. This is entered in node.slot notation, such as vnsigx1.14 from the example.
- Remote Node is the node (IGX or IPX switch) to which the remote VNS is connected, such as vnsigx2 from the example.
- 1st Hop through 9th Hop fields in node.slot notation, such as vnsigx3.12 in the 1st Hop field from the example. If the preferred route is routed through other intermediate routing nodes, you specify the node.slot of the trunk card on which the preferred route leaves the node, for the 2nd Hop, 3rd Hop, and so on.

The preferred route for the Local Adjacency PVC then becomes the concatenation of Local Node, all non-empty hop fields (1st Hop, etc.), and the Remote Node. When the Local Adjacency PVC is built either at boot time or at configuration time, the VNS will send the node (IGX or IPX switch) SNMP commands to build the connection over the preferred route. If the node fails to set up the preferred route signaling PVC, it will try to build a PVC through another route. Also if the preferred route fails after it has been built, the node will build another route.

Port Preferred Route Information

The Port Preferred Route option allows you to specify a preferred route for the signaling channel from a port (that is, a UNI attached to a PBX) to a VNS. The port must be configured with the Ports Information Submenu before you can configure a preferred route for it. Figure 7-2 illustrates a simple example where Port Preferred Routing could be used. In this example, there are a couple ways that the signaling channel (that is, the D channel) could be routed from PBX 2 to vnslab6. Depending on your traffic loading and network requirements, you could specify either E1 Trunk 1 or E1 Trunk 2 to be the preferred route. In the example, the numbers at either end of the E1 trunk indicate the slot numbers of the NTM, that is, the trunk cards.

Figure 7-2 Port Preferred Route Example



In this case, you would use the Port Preferred Routing menu to specify the preferred route. The Port Preferred Route Information menu is shown in the following example menu.

```
Port Preferred Route Information Example Menu
###############################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   Port descriptor  [ vnsigx3.8.1          ]                                  #
#   Local VNS Name   [ vnslab6       ]                                         #
#   Local node       [ vnsigx2.14    ]    Remote node      [ vnsigx3       ]   #
#   1st Hop          [               ]    2nd Hop          [               ]   #
#   3rd Hop          [               ]    4th Hop          [               ]   #
#   5th Hop          [               ]    6th Hop          [               ]   #
#   7th Hop          [               ]    8th Hop          [               ]   #
#   9th Hop          [               ]                                         #
#   Enter 's' to skip record  or 'q' to quit   [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?###############################################################################
```

The Port Preferred Route Information menu has the following fields:

- Port Description is the port in node.slot.port notation of the UNI port for which you are configuring a preferred route, such as vnsigx3.8.1 in the example.
- Local VNS Name is the configured name of this VNS, such as vnslab6 in the example.
- Local Node is the node (IGX or IPX switch) to which this VNS is connected. This is entered in node.slot notation, such as vnsigx2.14 in the example.
- Remote Node is the node (IGX or IPX switch) which contains the remote port, such as vnsigx3 in the example.
- 1st Hop through 9th Hop fields in node.slot notation. If you are routing this signaling channel through intermediate routing nodes, this field contains the configured node name and the slot (.slot) of the trunk card on which the signaling channel leaves the node.

The preferred route for the UNI port PVC (that is, the D-channel from the UNI port to the VNS) then becomes the concatenation of Local Node, all non-empty Hop fields (1st Hop, etc.), and the Remote Node. When the port PVC is built either at boot time or at configuration time, the VNS will send the node (IGX or IPX switch) SNMP commands to build the connection over the preferred route. If the node fails to set up the preferred route signaling PVC, it will try to build a PVC through another route. Also if the preferred route fails after it has been built, the node will build another route.

Cause Code Mapping

When a call is terminated abnormally, some PBXs can re-route the call on a different trunk based on the cause code that is contained in the disconnection message. Often, the re-route has to be done for different disconnection causes, but PBXs can be configured to re-route on a limited set of cause codes. The VNS allows you to configure specific cause codes to be returned to specific PBX types. This configuration is done on a per-port basis (see the PBX Type field of the Port Information menu). Cause codes form the far-end PBX as will as cause codes generated by the VNS will be translated as configured before being delivered to the near-end PBX.

Configuring cause codes requires the following items:

- Each port will be associated with a PBX type. When a port is added to the VNS database, a corresponding cause code file will be created. The number of cause code files will correspond to the number of PBX types in the VNS WAN switching network.
- The cause code files can be modified by option 16, Cause Code Information, on the VNS Confutation Interface Record Menu.

Cause Code Information Menu

Option 16, Cause Code Information, on the VNS Record Menu allows you to edit or view the cause code mapping file for a specific PBX type or port. (Note that this process is taking a default file which has cause codes 2, 3, 38, 41, 42, 111 translated to 34 and allows you to modify it for your application.) Here you enter the exact PBX type, which is a text string that is identical to a PBX Type field already configured on a Port Information menu. This string forms the file name of the cause code mapping file for the specified PBX type.

In the Cause Code Information Example Menu, seimenspbx is the PBX Type. This PBX Type must have been previously configured on a Port Information menu.

```
Cause Code Information Example Menu
################################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   Enter PBX Type :seimenspbx                                                 #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?###############################################################################
```

After entering the PBX Type (such as, seimenspbx), when you press Enter, you are prompted to enter a cause code to translate from as shown in the Translate From/Translate To Example Menu. Next you are prompted to enter the cause code to translate to. In this example, cause code 112 will be translated to cause code 34 when returned to a port configured with “seimenspbx” PBX Type. Finally, as shown in the example, you are prompted to enter more cause codes to translate. You commit each cause code mapping pair individually. Repeat the process for every cause code you want translated, then press any other key to quit and save the file.

```
Translate From/Translate To Example Menu
+##############################################################################+
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   Enter PBX Type : seimenspbx                                                #
#                                                                              #
#   Enter Cause Code to Translate From : 112                                   #
#                                                                              #
#   Enter Cause Code to Translate To : 34                                      #
#                                                                              #
#                                                                              #
#                                                                              #
#   Enter 'm' for More, any other key to Quit                                  #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
+##############################################################################+
```

You can use the Browse Data Base option from the Main Menu to see the entire list of cause codes that are mapped for a particular PBX Type file. As shown in the Browse Cause Code Example file, the translated-from cause codes and the translated-to cause codes are shown in two columns. This example shows the default list of translated cause codes (2, 3, 38, 41, 42, 111 translated to 34), as well as the 112 being translated to 34.

```
Browse Cause Code Example File
+###############################################################################+
#                                                                               #
#                                                                               #
#                                                                               #
#                                                                               #
#   Enter PBX Type : seimenspbx                                                 #
#                                                                               #
#   Translate From       Translate To                                           #
#                                                                               #
#        2                   34                                                 #
#        3                   34                                                 #
#        38                  34                                                 #
#        41                  34                                                 #
#        42                  34                                                 #
#        111                 34                                                 #
#        112                 34                                                 #
#                                                                               #
#   Type any key to Exit..                                                      #
#                                                                               #
#                                                                               #
#                                                                               #
#                                                                               #
#                                                                               #
+###############################################################################+
```

Delete an Entry

The Delete an Entry option of the VNS main menu allows you to delete completed entries in the VNS database.

When you choose this option, you get the same list of menus that you get when you select Add and entry. However choosing an item, such as VNS Information, pulls up a completed menu. You can then delete that entry to remove it from the data base.

Modify an Entry

The Modify an Entry option of the VNS main menu allows you to modify completed entries in the VNS database.

When you choose this option, you get the same list of menus that you get when you select Add and entry. However choosing an item, such as VNS Information, pulls up a completed menu. You can then modify that entry and save the modifications in the data base.

Browse Data Base

The Browse the Data Base option of the VNS main menu allows you to view the entries in the VNS database.

When you choose this option, you get the same list of menus that you get when you select Add and entry. However choosing an item, such as VNS Information, pulls up a completed menu. You can then look at it without modifying the data base.

Note There are a couple of read-only status fields that appear on Browse Data Base menus that do not appear on Add an Entry menus.

Validate Data Base

The Validate Data Base option of the VNS main menu allows you check the integrity of the VNS database. This command will return either a DATA BASE IS VALID or DATA BASE IS INVALID, PLEASE RESTORE FROM BACKUP message. When the database is invalid, you will have to restore it from a backup or recreate it. The following example shows the DATA BASE IS VALID message.

```
Validate Data Base Response
##############################################################################
#                                                                              #
#                                                                              #
#         DATABASE IS VALID...
#                                                                              #
#         Hit any key to continue                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?##############################################################################
```

Debug Mode

Note The Debug Mode menu is reserved for use by Support Personnel. Misuse of this menu could seriously degrade the performance of your VNS and WAN switching network.

```
Debug Mode Example Menu
##############################################################################
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#   VNS Name          [ vnslab8       ]                                        #
#   Debug Level       [ 0             ]                                        #
#   Log Information   [ 0             ]                                        #
#   Dump Sys Table    [ 0             ]                                        #
#                                                                              #
#   Type 'c' to commit,'s' to skip,'q' to quit [   ]                           #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
#                                                                              #
?##############################################################################
```

Exit the Program

Select this option from the VNS main menu to close the VNS Configuration Interface and return to the VNS’s UNIX prompt.

VNS Parameter Ranges and Defaults

Table 7-2 lists all the parameters (including their menu index number) in the VNS Configuration Interface, along with their ranges and defaults. The table lists each relevant menu in the left column. the menus are listed in the same order in which they are described in this chapter; this is the order in which they are completed and not the numerical sequence in which they appear on the Main Menu. The right column lists the parameter with its index number in parenthesis (that is, the index number returned in VNS Configuration Interface error messages identifying the field), the applicable range, and the default in bold text. Only those menus that have user-changeable fields are listed. Fields which are described as read-only display information but are not user-configurable.

Table 7-2 VNS Configuration Parameters

Menu	Field (and index number), Range, and Default
Nodes Information	Node Name (1): 10-character text string IP Address (2): State of Node: read-only field
Cards Information	Card Descriptor (1): node.slot notation Card State: read-only field Card Type (2):
VNS Information	VNS Name (1): 8-character VNS name Node Name (2): 10 character IGX/IPX name Node IP Address(3): IGX/IPX's LAN port IP address in dotted decimal notation Shut Down Timer (4): **0** - 65535 Statistics (5): **On** CDR File Count (6): CDR File Interval (7): SPNNI Type (8): Compression Type (9): Read Comm String (10): 1 - 32 characters Write Comm String (11): 1 - 32 characters Keep Alive Timer (12): 1 -60 seconds, **5** State Change Timer (13): 10 - 120 seconds, **30** RRP_UDP Port (14): 3000 to 65535, **5134** RRP Retry Count (15): 1 -100, **5** Config Redundancy (16): **0 = No**, 1 = Yes Enable MultiDomain (17): 1 = Disabled, 2 = Enabled CVM Redundancy: 1 = Disabled, 2 = Enabled Operational Status: **0 = Unknown**, 1 = outOfService, 2 = InService Operational Role: **0 = Unknown**, 1 = active, 2 = standby VNS IP Address (18): read-only field
More VNS and Redundancy Information	VNS Name (1): 8-character for VNS Voice Port #1 (2): node.slot.port of Voice Card on IGX/IPX switch Voice Port #2 (3): node.slot.port of Voice Card on IGX/IPX switch Frame Relay Port (4): node.slot.port of Frame Relay Port on IGX/IPX switch Operational Status: read-only field Operational Role: read-only field Admin Role (5): 1 = active, 2 = standby Admin Status (6): 1 = outOfService, 2 = inService, 3 = resetconfig, 4 = shutdown Peer IP Address (7): dotted decimal format VNS FR-IP Address (8): Not used Peer FR-IP Address (9): Not used

Table 7-2 VNS Configuration Parameters (Continued)

Menu	Field (and index number), Range, and Default
Port Information	Port Descriptor (1): node.slot.port notation Port Type (2): 0 = unknown, 1 = UNI Port State: 0 = unknown, 1 = outOfService, 2 = inService UNI Channel (3): 1 - 31 VNS Channel (4): 1 -31 First Channel (5): 1 -31 Last Channel (6): 1 - 31 Channel Alloc Role (7): 1 = unknown, 2 = side B (slave or user), 3 = side A (master or network) Channel Allocation (8): 1 = unknown, 2 = low end, 3 = high end Interface ID (9): 1 = Voice Port 1, 2 = Voice Port 2 Statistics (10) 2 = on, 3 = off Statistics Interval (11): 1 to 65535 minutes Stack Type (12): 1 = DPNSS, 2 = QSIG, 3 = JISDN (Q931A), 4 = Reserved, 5 = EISDN, 13 = AT&T 4ESS ISDN PBX Type (13):
Screening Type Information	Port Descriptor (1): node.slot.port of the port Source Screen Type (2): 1 = allowed, 2 = disallowed Destination Screen (3): 1 = allowed, 2 = allowed
Address Information	Address (1): 1 - 40 digit E.164 number Port Descriptor (2): Node.slot.port of the UNI port
Address Screening Information	Address Screening rule (1): 1 = 30 digits or characters Port Descriptor (2): node.slot.port of UNI port Screening Type (3): 0 = unknown, 1 = source screening, 2 = destination screening, 3 = both source and destination screening
Transformation Rules Information	Port Descriptor (1): node.slot.port of UNI port Priority (2): 1 - 65535 Patter to Locate (3): 0- 30 digits or characters Pattern to be Replaced (4): 0 - 30 digits or characters Replacement Digits (5): 0 - 30 digits Direction (6): 2 = inComing, 3 = outGoing, 4 = both directions Application (7): 0 - 65535 decimal number for bit pattern
Multihome Port Configurations	CPE Port (1): node.slot.port Multihomed Port (2): node.slot.port Select Policy (3): 1 = round robin alternation between ports, 2 = port with most available bandwidth, 4 = port with least amount of calls to it, 8 = port with least errors
Multihome Policy Configurations	Port Descriptor (1): node.slot.port notation Policy (2):1 = round robin alternation between ports, 2 = port with most available bandwidth, 4 = port with least amount of calls to it, 8 = port with least errors Weightage (3): 0 - 100
Local Adjacency Information	VNS Name (1): 8-character name of adjacent VNS Standby VNS Name (2): 8-character name of adjacent VNS’s peer unit Local Port Type (3): 2 = U-SPNNI, 3 = N-SPNNI Local DLCI (4): Remote Port Desc (5): Remote DLCI (6) VNS State: 0 = unknown, 1 = outOfService, 2 = inService Link Weight (7): 1 - 65535 Rmt Stby Port Desc (8): node.slot.port
Network Prefixes Information	Network Address (1): 1 - 30 character or digit prefix VNS Name (2):

Table 7-2 VNS Configuration Parameters (Continued)

Menu	Field (and index number), Range, and Default
Network Adjacency Information	Not used in this release.
Local Adjacency Preferred Route Information	Remote VNS Name (1): configured VNS name of remote VNS Local VNS Name (2): configured name of this VNS Local Node (3): node.slot of local node Remote Node (4): 1st Hop through 9th Hop (5 - 13): node.slot of the preferred trunks
Port Preferred Route Information	Port descriptor (1): node.slot.port notation of the UNI port Local VNS Name (2): Local Node (3): node.slot of local node Remote Node (4): 1st Hop through 9th Hop (5 - 13): node.slot of the preferred trunks
Cause Code Information	Enter PBX Type (1): Match a PBX Type previously configured with the Ports Information menu.

VNS Network Operation

This chapter provides procedures for performing the common tasks encountered during the initial provisioning and operation of a VNS network. It includes the following sections:

- VNS Network Planning
- VNS Network Provisioning
- VNS Network Operation

VNS Network Planning

To properly configure and provision a VNS network, you must do a good deal of planning before hand. For a typical VNS network installation, you will probably:

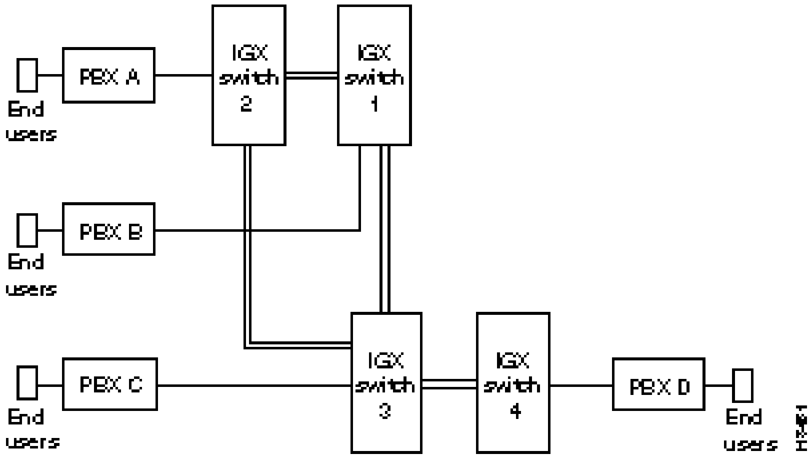
- Draw a Topology Map
- Identify VNS Areas and Interfaces
- Identify Adjacent VNS's for Multiple Service Area Networks (not necessary for a single VNS area)
- Identify each UNI Port
- Identify each Voice Port and signaling Channel
- Setup a numbering plan including VNS area prefixes and determine which UNI ports will be multihomed

The rest of this planning section will use a simple VNS network to illustrate the process.

Draw a Topology Map

Figure 8-1 illustrates a simple network consisting of four IGX switches. Each IGX switch has one PBX attached to it. In reality, there would typically be more than one PBX attached to each node.

Figure 8-1 Network Topology



Identify VNS Areas and Interfaces

Only a single VNS will be added to the topology of Figure 8-1. The VNS has been connected to IGX switch 1-1 as shown in Figure 8-2. (Sometimes the node, IGX or IPX switch, to which the VNS is directly attached is referred to as the "master node". The single VNS is responsible for the nodes (IGX switch 1-1, 1-2, 2-1, and 2-2) in its area. (When there is only a single VNS area, the configuration is much simpler. There do not have to be frame-relay connections between VNS's.) Figure 8-2 also points out the UNI (user-to-network interfaces) and Voice Ports that will have to be configured for this VNS network.

Figure 8-2 VNS Interfaces

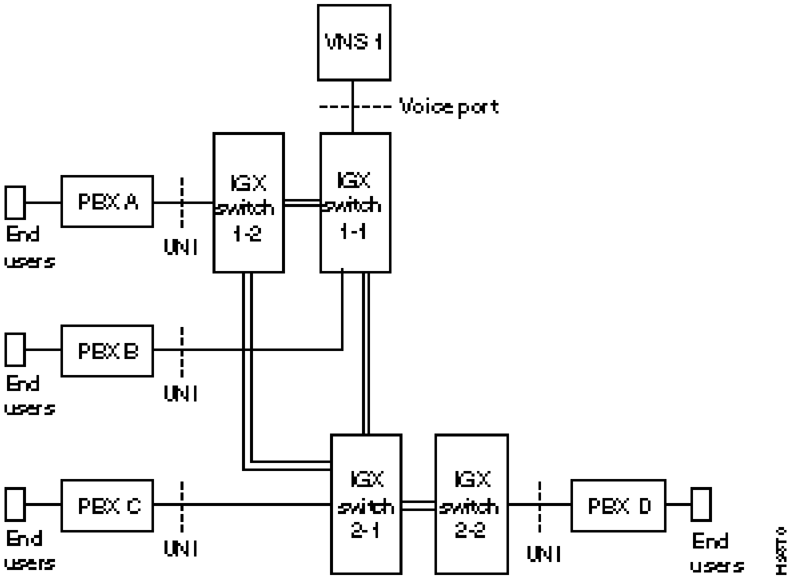


Table 8-1 lists some of the information that you should note about the VNS. The VNS information will be used in the provisioning, especially in the VNS Information, More VNS Info and Redundancy Information, and Nodes Information menus.

Table 8-1 VNS Information

VNS Name	VNS IP Address	Node Name	Node IP Address	Peer IP Address
VNS 1	200.1.2.3	IGX1-1	200.1.2.4	Not used here
Note 1: The VNS and Node IP addresses are only used for example. Your IP addresses should be consistent with the IP addresses of your network and must be assigned by your network administrator. **Note 2:** The peer IP address, not used in this example, is the IP address of the redundant (standby) VNS in a redundant pair.				

Identify Adjacent VNS's for Multiple Service Area Networks

Identify all the adjacent pairs of VNS's in the network. In this release, all the VNS's are connected through a full-mesh network. For each pair of VNS's, you should note the VNS hostname, the Voice Port Id (node.slot.port notation) of the Node's Frame Relay Port to which it is attached. Remember for each pair of VNS's, one side of this connection will be configured as U-SPNNI and the other will be N-SPNNI. You should also note the local and remote DLCIs for this connection which you configure with the Local Adjacency Information menu.

Identify each UNI and Voice Port

There is a user-to-network interface (UNI) for each PBX in the VNS network. A UNI port is identified by standard Cisco node.slot.port notation for the CVM or UVM (or CDP for the IPX switch) on the node to which the PBX is connected. Figure 8-3 illustrates this notation for the UNI port between PBX B and IGX switch 1-1 in the sample VNS network shown in Figure 8-3. Table 8-2 lists the UNI notation for the other UNI ports in our sample VNS network. Table 8-3 lists the IDs for the Voice Ports, i.e., the interface between the VNS's E1 NIC cards and the node.

This information will be used in the Cards Information, Ports Information, and More VNS and Redundancy Information menus.

Figure 8-3 VNS Areas

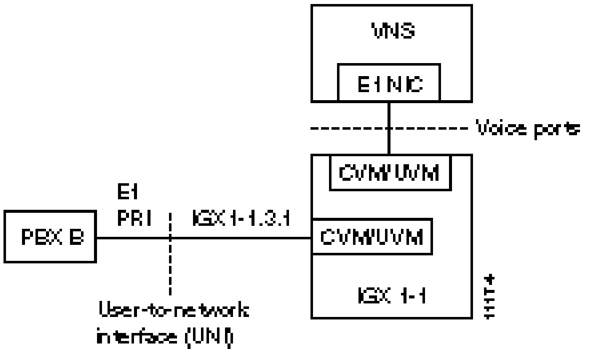


Table 8-2 UNI Ports

UNI Ports	Node ID.
PBX A	IGX 1-2.4.1
PBX B	IGX 1-1.3.1
PBX C	IGX 2-1.4.1
PBX D	IGX 2-2.4.1

Table 8-3 Voice Port IDs

Voice Port	Node ID.
Voice Port 1	IGX 1-1.4.1
Voice Port 2	Not used in this example

Note: There are two E1 NICs in each VNS. Each E1 NIC will be connected to a different CVM or UVM (or CDP in an IPX switch) port. When only one E1 NIC is needed, you should connect Voice Port 1.

Identify each Signaling Channel

There will be a signaling channel from each PBX (i.e., UNI port) to the VNS which is responsible for it. Figure 8-4 illustrates this UNI to VNS signaling channel for PBX 2 in the sample VNS network shown in Figure 8-2. The PBX to IGX switch connection is a channelized E1 connection, and timeslot (TS) 16 is typically used as the signaling channel at the UNI interface. (For CAS signaling as described in Appendix I, the signaling channel is DS0 25.) At the Voice Port interface, i.e., the connection between the node and VNS's E1 NIC, the timeslot is user assigned. Any of the E1 NIC's 30 timeslots can be assigned for this side of the signaling channel. Each timeslot of the channelized E1 connection (i.e., E1 NIC to node's CVM or CDP) can only be used for one PBX, i.e., PRI interface.

Table 8-4 lists the UNI signaling channel information for each of the PBX's (i.e., UNI ports) in the sample VNS network of Figure 8-2. This information is used primarily in the Ports Information menu.

Figure 8-4 UNI-to-VNS Signaling Channel

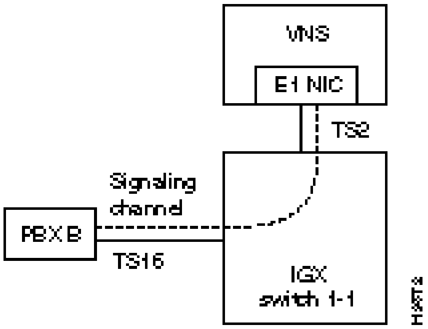


Table 8-4 UNI Signaling Channel Information

UNI Ports	UNI Channel	VNS Channel	First Channel for User Signaling	Last Channel for User Signaling	Channel Allocation
PBX A	16	1	1	30	QSIG or DPNSS side 1 or side 2
PBX B	16	2	1	30	QSIG or DPNSS side 1 or side 2
PBX C	16	3	1	30	QSIG or DPNSS side 1 or side 2
PBX D	16	4	1	30	QSIG or DPNSS side 1 or side 2

Setup a Numbering Plan Including VNS Area Prefixes

To set up a numbering plan, you have to assign addresses (i.e., E.164 telephone numbers) to every UNI port in the VNS network. Table 8-5 lists the addresses for the UNI ports in our sample VNS network shown in Figure 8-2. This information is used primarily to complete the Address Information menu. Each UNI port address can be up to 40 digits long.

Table 8-5 Voice Port Addressing

UNI Ports	Port ID	Address (E.164 number)
PBX A	IGX 1-2.4.1	xxxxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxxxxx
PBX B	IGX 1-1.3.1	xxxxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxxxx
PBX C	IGX 2-1.4.1	xxxxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxxxx
PBX D	IGX 2-2.4.1	xxxxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxxxxx xxxxxxxxxxxxx

You can assign network prefixes to a VNS area to help organize the numbering plan for the VNS network. Table 8-6 provides address prefix information for our sample VNS network shown in Figure 8-2. This information is used primarily in the Network Prefixes Information menu. Address Prefixes, which can be up to 30 digits long, are typically used to identify a VNS area.

Table 8-6 VNS Prefixes

VNS Area	Address Prefix
VNS 1	xxxxxxxxxxxxxxxx

Finally for each voice port you can specifying the Address Screening and Transformation Information that would go in Table 8-7. This information is used in the Address Screening Information and Transformation Rules Information menus.

Table 8-7 Voice Port Screening and Transformation

UNI Port ID	Address Screening	Address Transformation
Node.slot.port	xxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxx
Node.slot.port	xxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxx
Node.slot.port	xxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxx

VNS Network Provisioning

After you have planned your VNS network, installed the necessary nodes (IGX/IPX switches), and installed and connected the VNS's, you are almost ready to use the VNS Configuration Interface to provision the network. First, however, you must "Up" the ports, lines, and trunks that comprise the VNS network. "Up-ing" ports, lines, and trunks is done through the Cisco wide-area switch's command line interface with the same commands that are used in all Cisco WAN switching networks. Details about these commands and procedures are described in the *Cisco IPX Reference,* the *Cisco IGX 8400 Series Reference* and the *Cisco WAN Switching Command Reference* publications. In addition, the *Cisco WAN Switching System Overview* provides detailed information about the way various Cisco WAN switching networks are interconnected and operated.

In a VNS network, provisioning consists of:

- Configuring the VNS
- Creating VNS areas
- Configuring the UNI, PBX to node interface
- Configuring the signaling channel between the PBX and the VNS
- Configuring the signaling channel between VNS's in the network
- Configuring the VNS to node ethernet path
- Assigning prefixes to VNS areas
- Assigning addresses (E.164 telephone numbers) to end users
- Multihoming selected UNI ports

The VNS Configuration Interface is used to provision the VNS network. During provisioning, the VNS Configuration Interface menus must be completed in four sequential operations:

1. Configure the domain
2. Configure UNI or PBX addressing
3. Configure multiple domains
4. Configure Preferred D-Channel Routes

You should have read Chapter 7, Understanding the VNS Configuration Interface, before you use the menus to configure and provision the VNS and VNS network. As described in Chapter 7, certain fields of one menu must be completed before subsequent menus can be completed. These fields are linked between menus. In other words, the VNS Configuration Interface menus must be completed in the described order.

Configure the Domain

To configure the domain, complete these menus in the following order:

1. Nodes Information--Complete this menu for each node in the VNS's area. (See Nodes Information on page 7-9 .)
2. Cards Information--Complete this menu for each CDP/CVM card in the Cisco IGX/IPX wide-area switch. (See Cards Information on page 7-10 .)
3. VNS Information--Complete this menu for each VNS in your network. (See VNS Information on page 7-11 .)
4. More DNS Info and Redundancy Information--Complete this menu for each redundant pair of VNS's in your network. The menu has to be completed for both the first and second VNS's. (See More VNS Info and Redundancy Information on page 7-15 .)

Configure Redundancy

When you install redundant pair of VNSs, you first configure the domain for the active VNS, then restart the standby VNS to trigger a bulk database update. To configure redundant VNSs, follow these steps:

Step 1 Configure the domain for the active VNS:

- Complete a Nodes Information menu for each node in the active VNS's service area.
- Complete a Cards Information menu for each card (CVM, CDP, FRM, or FRP) in use on the nodes in the active VNS's service area.
- Complete the VNS Information menu making sure that the Config Redundancy field is set to 1 (1 = Yes).
- Configure a More VNS Info and Redundancy Information menu for both the active and standby VNSs. As described in Chapter 7 in the section, More VNS Info and Redundancy Information, this menu has to be completed for both VNSs in a redundant pair.

Step 2 Bring up the standby VNS to initiate a bulk update of the database.

Configure UNI or PBX Addressing

To configure UNI or PBX addressing, complete these menus in the following order:

1. Ports Information--Complete this menu for each UNI Port (i.e., PBX interface) in the VNS's area. (See Port Information on page 18.)
2. Screening Type Information--Complete this menu for each UNI Port in your VNS network. (See Screening Type Information on page 21.)
3. Address Information--Complete this menu for each UNI Port in the VNS's area. (See Address Information on page 22.)
4. Address Screening Information--Complete this menu for each UNI Port in your VNS network. (See Address Screening Information on page 23.)
5. Transformation Rules Information--Complete this menu for each UNI Port in your VNS network. (See Transformation Rules Information on page 24.)
6. Multihome Port Configurations--Complete this menu for each pair of UNI Ports which you want to multihome. (See Multihome Port Configurations on page 27.)

7 Multihome Policy Configurations--Complete this menu for each UNI Port which has multiple multihoming policies configured for it. (See Multihome Policy Configurations on page 28.)

Configure Multiple Domains

To configure multiple domains, complete these menus in the following order.

1 Local Adjacency Information--Complete this menu for each SPNNI frame-relay PVC between the VNSs in your network. (See Local Adjacency Information on page 29.)

2 Network Prefixes Information--Complete this menu for each VNS in your network. (See Network Prefixes Information on page 31.)

3 Network Adjacency Information--This menu is not used. (See Network Adjacency Information on page 32.)

These menus, Local Adjacency Information, Network Prefixes Information, and Network Adjacency Information do not have to be completed if there is only a single VNS area in your network.

You must complete these menus for each VNS (or VNS area) in your network. Within a VNS area, you must complete a menu for each node and each UNI port.

Local Adjacency Example

In a multidomain VNS network, there must a SPNNI connection between each VNS domain. This connection must be built from both ends of the connection. For instance, in a two domain network, the connection must be built from domain 1 and domain 2. In other words, the Local Adjacency Information menu must be completed at domain 1 and at domain 2.

For example, if vnslab1 was connected vnsigx1 and controlled domain 1, and vnslab2 was connected to vnsigx2 and controlled domain 2, you will have to create Local Adjacency records at both vnslab1 and vnslab2. Some of the fields on these coordinated records are counterparts, as shown in the following example:

At vnslab1 (domain 1), you complete a Local Adjacency menu making sure the following fields have been completed correctly and point to vnslab2:

- VNS Name contains vnslab2 (this is, the configured VNS Name from the VNS Information menu at vnslab2; vnslab2 controls domain 2).
- Local Port Type will be 3 (N-SPNNI). (One end of the SPNNI connection must be N-SPNNI, the other end must be U-SPNNI.)
- Remote Port Desc contains vnsigx2.3.1 (describing the port on vnsigx2 which is connected to the Frame Relay card on vnslab2).
- Local DLCI = 101.
- Remote DLCI = 102.
- Link Weight = 1.

At vnslab2 (domain 2), you complete a Local Adjacency menu making sure the following fields have been completed correctly and point to vnslab1:

- VNS Name contains vnslab1 (that is, the configured VNS Name from the VNS Information menu at vnslab1; vnslab1 controls domain 1).
- Local Port Type will be 2 (U-SPNNI). (One end of the SPNNI connection must be U-SPNNI, the other end must be N-SPNNI.)

- Remote Port Desc contains vnsigx1.3.2 (describing the port on vnsigx1 which is connected to the Frame Relay card on vnslab1.)
- Local DLCI = 102.
- Remote DLCI = 101.
- Link Weight = 1.

Note VNS Local Adjacency Information is validated only at VNS start up. You must ensure the Remote Port Desc on the node is the Frame Relay Port configured on the More VNS Info and Redundancy menu.

If this example, a type of global addressing scheme is used to used to identify the VNS domains. Each VNS controlling a domain (or service area) will be assigned a DLCI. Thus, vnslab1 (domain 1) is assigned DLCI 101 and vnslab2 (domain 2) is assigned DLCI 102. If a 3rd domain is added, it would be assigned DLCI 102. (DCLIs 101 to 113 are reserved on the VNS's Frame Relay card as described in Chapter 6 in the section Modifying the Default Range of VNS DLCIs.) Since there can be as many as 14 domains in a network, this makes it easier to keep track of the SPNNI connections between domains.

Configure Preferred D-Channel Routes

To configure preferred D channel routes, complete the following menus.

1. Local Adjacency Preferred Route Information--Complete this menu for each Frame Relay PVC between adjacent VNS's for which you wish to specify a particular route through the Cisco WAN switching network. (See Local Adjacency Preferred Route Information on page 7-34 .)
2. Port Preferred Route Information--Complete this menu for each UNI port for which you want to configure a preferred route through the Cisco WAN switching network to the VNS.

Saving and Restoring the VNS Database

The configuration database that is created with the VNS Configuration Interface is stored on the VNS's hard disk in a structured format. The VNS provides commands for saving this database file in a flat-file format which can be FTPed to another platform, such as a SV+ Workstation, as a backup or archive file in case the current database is corrupted. (Note that the VNS Configuration and Restore procedure is not the same as the StrataView Plus Config Save and Restore feature.) This backup database can then be restored on the VNS.

Caution Database corruption that occurs on a power failure can be corrected only by restoring the database from a backup. The database checksum feature will only detect such a failure; it can not prevent or recover from it. Therefore, you should perform database backups on a regular basis.

To save the VNS configuration data base, follow these steps:

Step 1 From the StrataView Plus Workstation (or other platform that has IP connectivity to the VNS), telnet to the VNS and log in as root or with your UNIX password.

Step 2 Execute the VNS backup command:

```
vnscli -b /server/path/backup-database-filename.a
```

or for remote host:

```
vnscli -b hostname: /path/backup-database-filename.a
```

Where /server/path/ is the path and directory where you are going to be storing the backup (or archive) file. And backup-database-filename.a is what your are naming the file. Use a dot a (.a) extension to indicate that it is an archive file. Write permissions should exist on the remote host.

To restore the VNS configuration data base from an archived file, follow these steps:

Step 1 From the StrataView Plus Workstation (or other platform that has IP connectivity to the VNS), telnet to the VNS and log in as root or with your UNIX password.

Step 2 Execute the VNS restore command:

```
vnscli -r /server/path/backup-database-filename.a
```

or for a remote host:

```
vnscli -r hostname: /path/backup-database-filename.a
```

Where /server/path/ is the path and directory from which you are restoring the backup (or archive) file. And backup-database-filename.a is the name of the file that you previously backed up and are not restoring to the VNS.

VNS Network Operation

During the operation of a VNS network, the following tasks are commonly repeated:

- Adding a PBX to the network
- Removing a PBX from the network
- Adding a VNS to the network
- Add a redundant VNS to network
- Deleting a redundant VNS from the network
- Removing a VNS from the network
- Adding an end user
- Removing an end user
- Adding an Address Prefix to a VNS
- Deleting an Address Prefix from a VNS

Adding a PBX (i.e., a Voice Port) to the Network

When adding a PBX to a VNS network, the following parameters will have to be entered on the VNS Configuration Interface menus:

- Port ID
- Card ID
- Node ID
- Signaling channel ID
- Available channel ID range

Note CAS PBX's must be connected to IGX UVM with Model B or higher firmware, which perform CAS-to-QSIG conversion. CAS switching is described in Appendix I, Channel Associated Signaling Voice Switching.

Removing a PBX from the Network

When removing a PBX (i.e., Voice Port) from a VNS network, the following parameters will have to be deleted through the VNS Configuration Interface menus:

- Port ID
- Card ID
- IGX/IPX node ID

Configuring Cause Codes for a PBX

To configure specific Cause Codes for a PBX type, refer to the section Cause Code Mapping in Chapter 7.

Adding a VNS to the Network

When adding a VNS to the network, the following parameters will have to be entered on the VNS Configuration Interface menus:

- VNS ID
- SPNNI signaling DLCI

Removing a VNS from the Network

When removing a VNS from the network, the following parameter will have to be deleted through the VNS Configuration Interface menus:

- VNS ID

Adding a Redundant VNS

When adding a redundant VNS, use the VNS configuration interface to:

- Complete Nodes Information record for all nodes in active VNS's service area.
- Complete Cards Information records for all cards (CVM, CVP, FRM, or FRP) in use in active VNS's service area.
- Complete More VNS Info and Redundancy Information menu for both active and standby VNSs.
- Turn on the standby VNS to trigger a bulk update.

Removing a Redundant VNS

Note that you can not delete a standby VNS while it is In Service.

Adding an End User

When adding an end user (i.e., an address) to a UNI port, the following parameters will have to be entered on the VNS Configuration Interface menus:

- Port ID
- Address

Removing an End User

When removing an End User (i.e., an address) from a UNI port, the following parameters will have to be deleted through the VNS Configuration Interface menus:

- Address Type
- Address

Adding an Address Prefix to a VNS

When adding an Address Prefix to a VNS, the following parameters will have to be entered through the VNS Configuration Interface menus:

- VNS Name
- Address Prefix

Deleting an Address Prefix from a VNS

When deleting an Address Prefix from a VNS, the following parameters will have to be deleted through the VNS Configuration Interface menus:

- VNS Name
- Address Prefix

Cable Information

This appendix provides information about the VNS AC power cables, Frame Relay Card cables, and includes an illustration of a sample null modem cable.

AC Power Cabling

Cable

Cisco provides a 6-foot (1.8m), 3-conductor cord with an IEC 320 C-13 appliance coupler for mating with the VNS on the system end. The other end of the power cord should be a grounding-type attachment plug as described in the paragraphs that follow.

Connector

The AC power cable can be ordered with the following connectors:

- — For North America and Japan: NEMA 5-15
- — For Continental Europe: CEE 7/7 (Schuko)
- — For Italy: CEI 23-16/VII (16 Amp plug)
- — For United Kingdom and Ireland: BS 1363
- — For Australia and New Zealand: AS 3112

For those countries not appearing in the preceding list, use a power cord with an IEC 320 C-13 appliance coupler for the system-end and an appropriate grounding-type attachment plug at the other end in accordance with local standards.

Source-end connector information is not available for all countries, so local codes must be known or obtained by either the customer or installer.

Frame Relay Card Cables

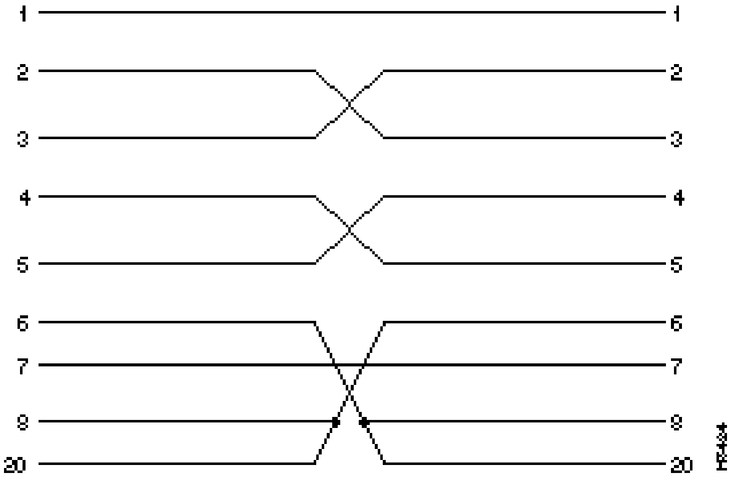
Cisco provides two cable options for connecting the VNS's Frame Relay Card to the IGX or IPX switch:

- RS449 to V.35 cable, part number 74-0850-01
- RS449 to X.21 cable, part number 72-0850-01

Sample Null Modem Cable

The figure below shows a typical null modem cable. Cisco does not supply this cable.

Figure A-1 Null Modem Cable



Troubleshooting

This Troubleshooting appendix is divided into the following sections:

- Initial Troubleshooting
- Troubleshooting SV+ to VNS Connectivity
- Troubleshooting Signaling Connections
- Troubleshooting Voice (i.e., PBX) Connections
- VNS Traps
- Cause Codes

The Initial Troubleshooting section provides some general hints, which should help to eliminate common, easily fixed problems in a VNS WAN switching network. It also provides instructions for running the VNS Status script.

The remaining sections provide suggestions for solving specific types of problems. These sections also include details on using some specific troubleshooting tools, such as the Frame-Relay Status Utility, StrataView Plus's D-Channel and SPNNI Status windows, and a list of VNS Traps.

Initial Troubleshooting

When you suspect a problem with a VNS network, you should:

Step 1 Begin troubleshooting with the SV+ Workstation:

- Make sure that the VNS has initialized and its icon on the topology maps is green.
- Use the Event Browser and monitor network events. Make sure that there has been a "Link Up" message.
- Look for event messages from the VNS.
- If you are not receiving Traps from the VNS, delete the VNS object from the HP OpenView Network Topology Maps and recreate the object. (Adding and deleting VNS objects from the HP Openview Topology Maps are covered in Chapter 6.)

Step 2 Make sure that the Clock Source is configured correctly throughout the network.

Step 3 Make sure that the signaling PVCs are built between the UNI ports (i.e., PBX's) and the VNS.

- If the signaling PVCs are not built, make sure that the SNMP parameters are set correctly on the node directly attached to the VNS:

  Read = public

  Write = private

  Trap = public

Step 4 Use the standard Cisco IGX and IPX switch command line interface and Cisco StrataView Plus troubleshooting tools (e.g., **dspnw**, **dspalarms**, **tstcon**, and **dchst**, etc.).

VNS Status

There is also a VNS Status script (*vns_status*) that provides information about the status of the VNS. This script resides in the /usr/vns directory.

To find out the VNS Status, follow these steps:

Step 1 From the UNIX prompt on the VNS, change directory to /usr/vns.

Step 2 Run vns_status.

If the VNS processes are running, the following message appears on the console:

VNS processes are active

If the VNS processes are not active, the following message appears on the console:

VNS processes are not running. Please reboot the VNS.

Troubleshooting SV+ to VNS Connectivity

When there is a problem with the SV+ Workstation to VNS communication and they are connected over ethernet, the following is a list of things that you should check:

Step 1 Check the cabling between the SV+ Workstation and a router and 10Base-T hub.

Step 2 Check the cabling between the hub or router and the VNS.

Step 3 If the VNS is on a subnet, make sure the IP Address is set correctly with respect to subnet masks.

- Make sure the subnet mask is set correctly on both the SV+ Workstation and the VNS.
- At the VNS, from the UNIX prompt use the ifconfig -a command to check the IP address and subnet mask for the VNS, as shown below. In this example, le0 is the VNS ethernet port with an IP address of 192.168.200.101 with a subnet mask of ffffff00.

```
<root@cedar>/> ifconfig -a
lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu8232
          inet 127.0.0.1 netmask ff000000
le0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
          inet 192.168.200.101 netmask ffffff00 broadcast 192.168.200.255
          ether 8:0:20:72:5e:a7
frmux0: flags=c1<UP,RUNNING,NOARP> mtu2048
          inet 201.2.3.4 netmask ffffff00
ifconfig: putmsg: Invalid argument
```

Step 4 If the ethernet connection is through routers, make sure the routers are set up correctly.

Step 5 Check with your network system administrator to see if you need to modify SV+ Workstation's */etc/defaultrouter* file to identify the router.

Step 6 Ping the SV+ Workstation from the VNS:

ping *hostname of SV+ Workstation*

then

ping *IP address of SV+ Workstation*

If you can ping with the IP address but not with the hostname, then */etc/hosts* has not been set up correctly.

Step 7 Repeat Step 6, but ping from the SV+ Workstation.

Troubleshooting Signaling Connections

There are two types of Signaling connections in a VNS WAN switching network:

- PBX to VNS
- VNS to VNS

The PBX to VNS takes an ISDN (either QSIG or DPNSS) D-channel from the PBX to the VNS. This channel is terminated on a VNS's E1 NIC. The VNS to VNS signaling connections are frame relay connections which terminate on the VNS's Frame Relay Card.

Note An ISDN protocol analyzer is helpful in troubleshooting ISDN links. It can be used to isolate layer 2 and layer 3 problems.

E1 NIC Tests

There are two series of tests available for the E1 NIC:

- E1 NIC Loopbacks
- E1 NIC Diagnostics

E1 NIC Loopbacks

The software drivers for the E1 Network Interface Cards (E1 NICs) can be tested in loopback mode. But it requires an external loopback connection.

To run the loopback tests for the E1 NICs, follow these steps:

Step 1 Connect the TX BNC connector to the RX BNC connector on one or both E1 NICs. Check that the Green LED on the back of the E1 NIC lights to indicate that the link is active and in sync. (If the Green LED does not light, the E1 NIC is bad.)

Step 2 Using a directly connected terminal (or with a Telnet connection), change your working directory with the following command:

```
cd /opt/CoE1DRV/bin
```

There are two loopback programs in this directory:
txrx used to run a loopback over a single specified channel.
thtxrx to run a loopback over multiple channels.

Step 3 To run **txrx**, Enter:

```
./txrx -s <unit number> -b <channel number> -l <packet size>
```

The number of successfully received packets will be updated on the screen periodically with sequence error indication.

Step 4 To run **thtxrx**, Enter:

```
./thtxrx -s <unit number> -b <start channel num> -n <number of channels>
```

If there is only one E1 NIC in your VNS, then it is not necessary to specify the unit number.

E1 NIC Diagnostics

The E1 NIC diagnostics (coe1diag) tests the E1 card at a specified VNS slot thoroughly. All channels are separately tested with data packets varying from 2 to 200 packets. Then all channels are tested simultaneously. The E1 NIC diagnostics program prints a summary of the test results at an attached terminal.

To run E1 NIC diagnostics (coe1diag), follow these steps:

Step 1 Using a directly connected terminal (or with a Telnet connection), change your working directory with the following command:

```
cd /opt/CoE1DRV/bin
```

Step 1 Enter:

```
./coe1diag [-s] [-e] [-l]
```

The coe1diag command has the following options:

-s <slot number> which is the VNS SBus slot number and is required only there is more than one E1 NIC card in your unit.

-e exit on error. Normally the program terminates only after carrying out the tests. With this option, the test terminates after detecting the first error on the card.

-l internal loopback mode which enables the E1 NIC to be tested without the external loopback connection. In this mode, the transmitted data is looped back to the receiver internally on the E1 NIC.

D-Channel and SPNNI Status

HP OpenView running on the Cisco StrataView Plus Workstation contains two options to check the status of VNS signaling connections:

- D-Channel Status lists the D-Signaling channels from a PBX and indicates whether their status is inService, OutofService, or unknown.
- SPNNI-Channel Status lists the SPNNI-channels between VNSes, in a multiple-area VNS network, and indicates whether they are inService, OutofService, or unknown.

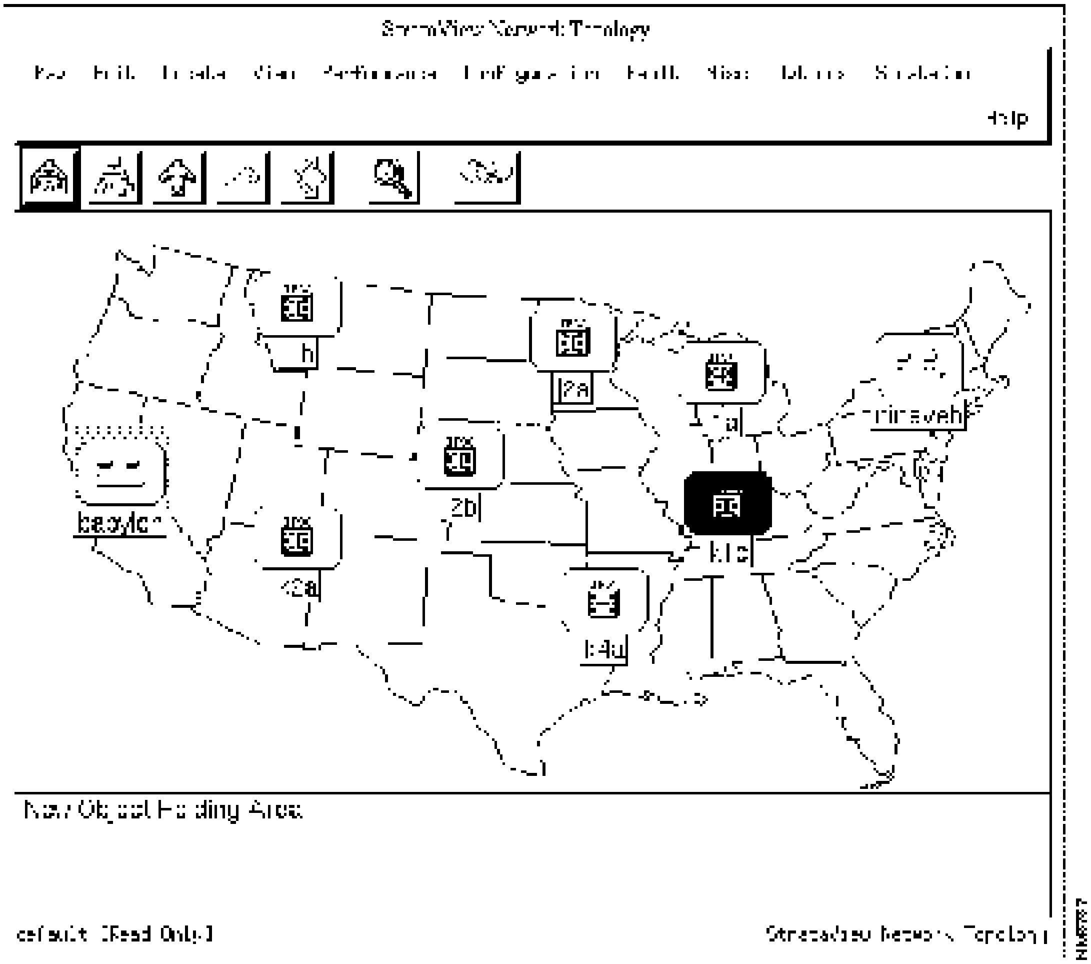
To open check the status of a VNS's signaling connections, follow these steps:

Step 1 At the SV+ Workstation, if HP Openview is not running, open an HP OpenView window:

- at the UNIX prompt, change to the OV directory.
- Enter ovw.

Step 2 Double click on your network icon to open a Network Topology window and map, as shown in Figure B-1. There are two VNS icons, babylon and nineveh, on this sample Network Topology

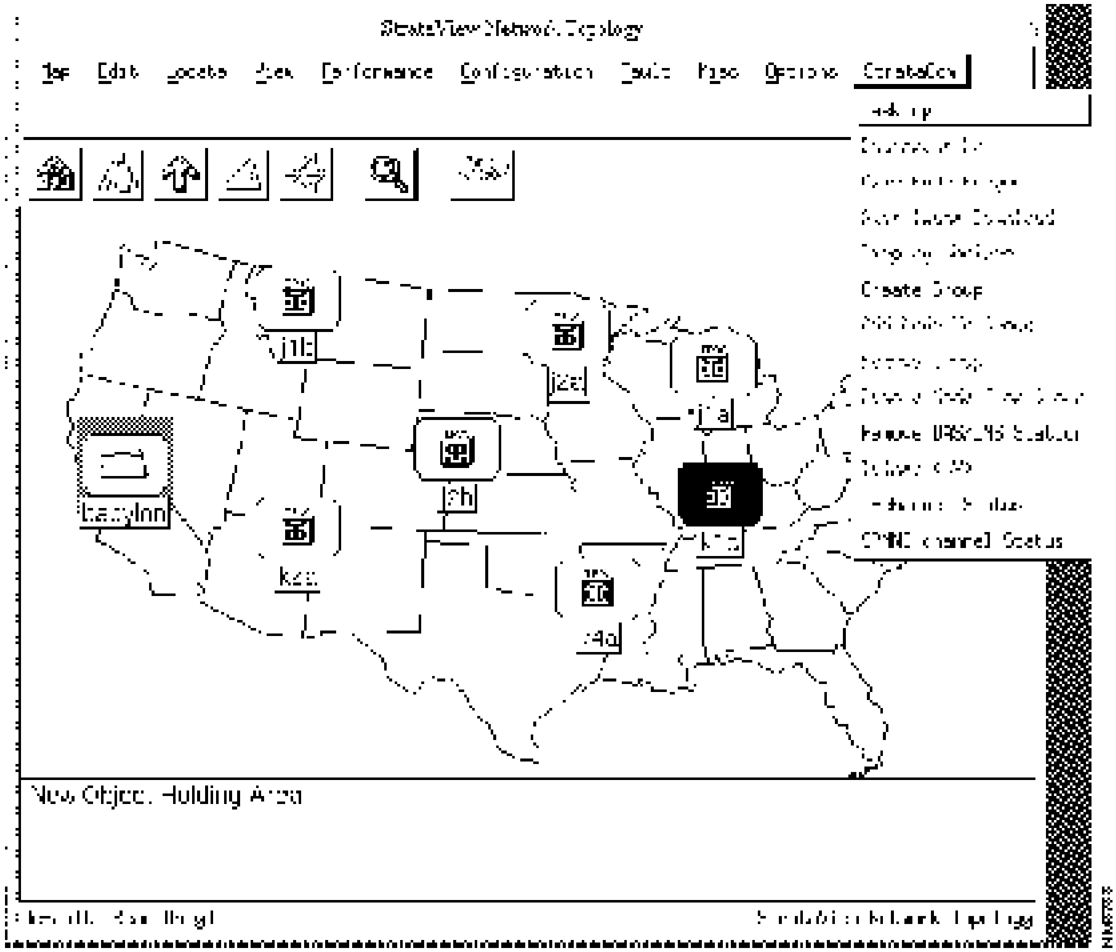
Figure B-1 HP OpenView Network Topology Window


StrataView Network Topology
Map Edit Locate View Performance Configuration Fault Misc Tools Simulation
Help
h
17a
a
nineveh
babylon
2b
12a
k1c
14u
New Object Holding Area
default [Read Only]
StrataView Network Topology

Step 3 Select the VNS icon for which you want to check the signaling connections. (In Figure B-1, babylon is highlighted as having been selected.)

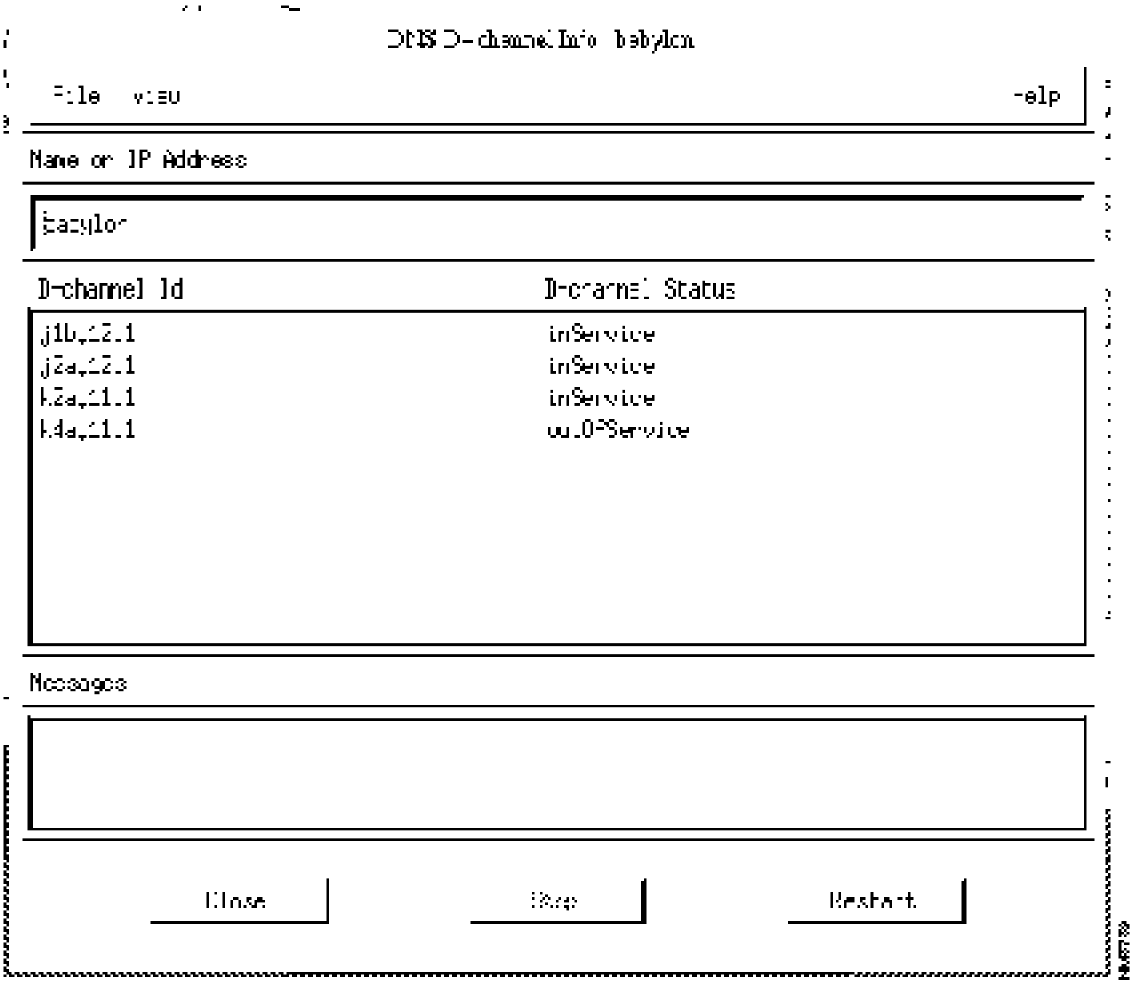
Step 4 Pull down the StrataCom menu as shown in Figure B-2.

Figure B-2 HP OpenView StrataCom Menu



Step 5 Select either D-Channel Status or SPNNI Status. If you select D-Channel Status the D-Channel Status window shown in Figure B-3 appears. If you select SPNNI-Channel Status, the SPNNI-Channel Status window shown in Figure B-4 appears.

Figure B-3 D-Channel Status Window



DMS D-channel Info babylon

Name or IP Address

babylon

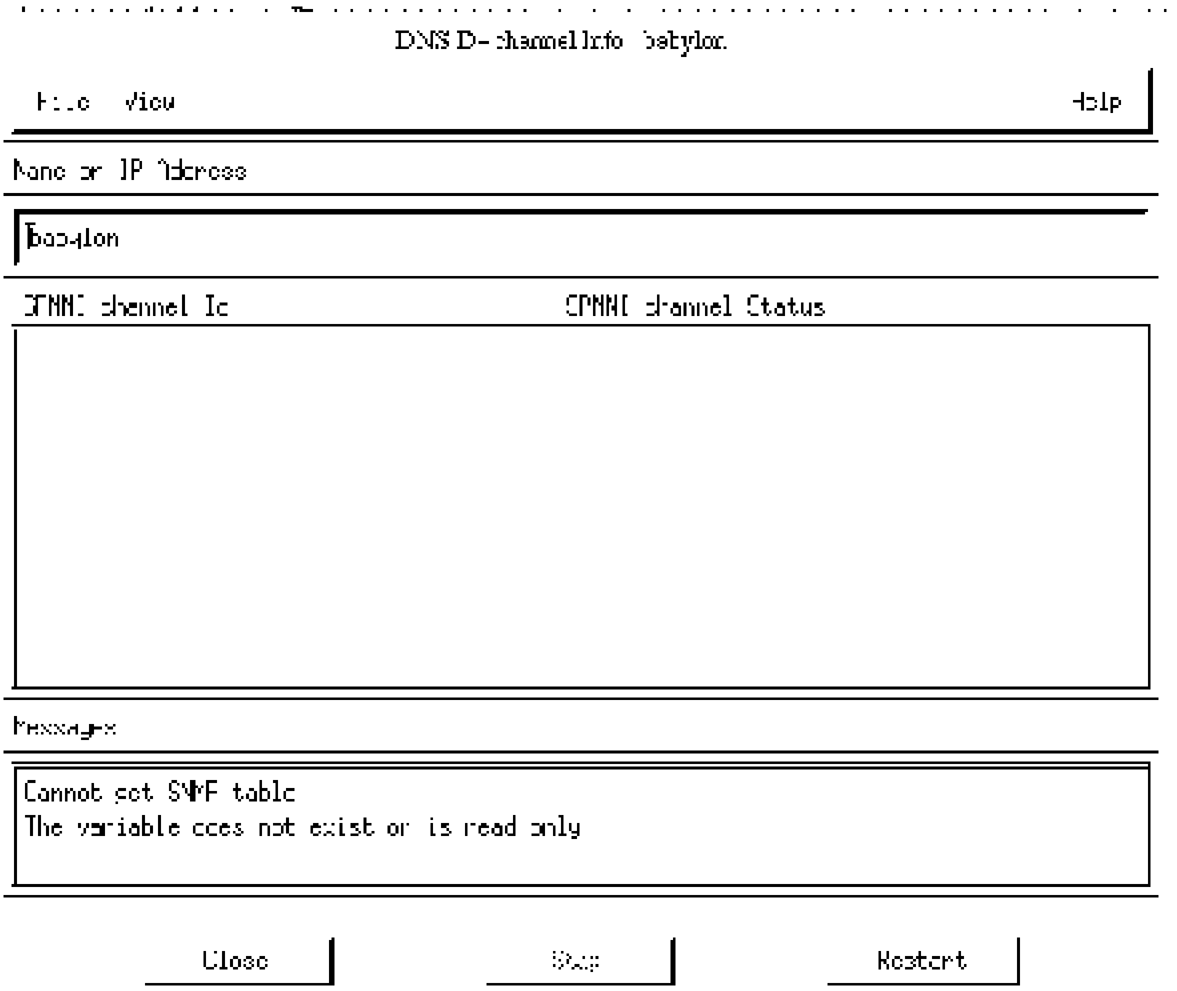
D-channel Id	D-channel Status
j1b.12.1	inService
j2a.12.1	inService
k2a.11.1	inService
k4a.11.1	outOfService

Messages

As shown, the D-Channel Status window lists the D-channel Id (node.slot.port) and its status. Note that the D-channel Id lists the physical port and not the logical port or timeslot of the D-channel.

The Restart button performs another SNMP GET request to refresh the screen. The View button allows you to sort the contents of the window by column. HP OpenView contains help menus that clearly explain these window functions.

Figure B-4 SPNNI-Channel Status Window



Name or IP Address

babylon

SPNNI channel Id SPNNI channel Status

Messages

Cannot get SNMP table
The variable does not exist or is read only

Frame Relay signaling Connections

This section contains some generic hints for troubleshooting the frame relay PVCs that the VNSes use to communicate with one another. (Note that these connections are used for multiple VNS areas, and are not required for a single domain.)

When there appears to be a problem with an existing PVC, try these things:

1. Use the **dspportstats** command to see if frames are being passed across the port. Reset the port stats counters with the **clrportstats** command. Look for frame errors. (The *Cisco WAN Switching Command Reference* publication describes this command in detail.)
2. Use the **dspchstats** command at both endpoints of the PVC. Reset the channel stats counters to the **clrchstats** command. (The *Cisco WAN Switching Command Reference* publication describes this command in detail.)
3. Use the *Frame Relay Status Utility* on the VNS to verify data on the PVC, identified by its DLCI, at the VNS. (The next section describes Using the *Frame Relay Status Utility.*)
4. Ensure that the factory-configured file */usr/net/fr/ fr_config* file appears as it is shown in Chapter 6.
5. Ensure that the */usr/net/fr/fr_conv* file contains the IP address to DLCI mapping for any IP networks accessible across the frame relay network, as shown in Chapter 6.

Using the Frame Relay Status Utility

The *Frame Relay Status Utility* runs on the VNS and monitors the frame relay connections over the serial frame-relay port (RS422/V.35).

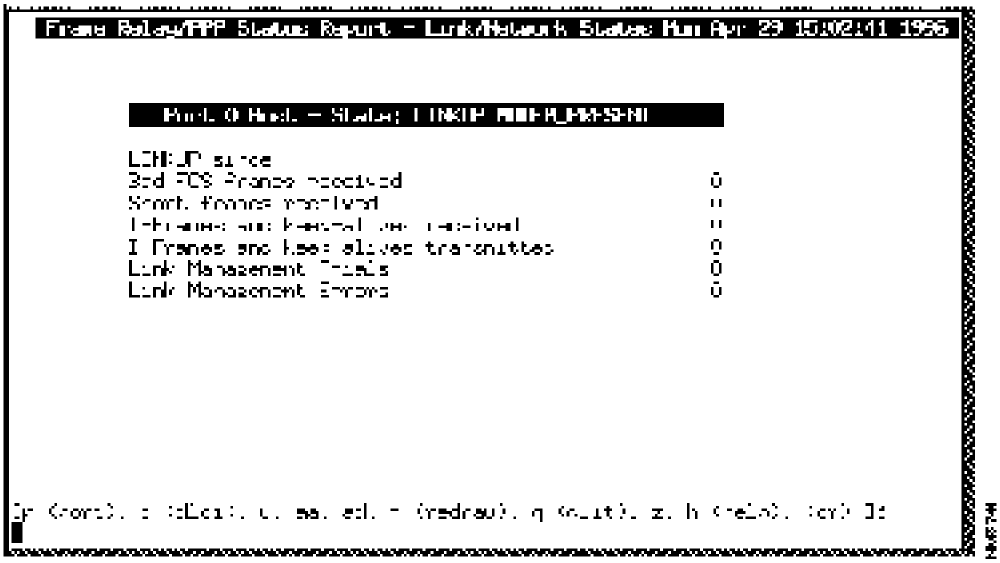
To use the Frame Relay Status Utility, follow these steps:

Step 1 Log into the VNS as root.

Step 2 Change directory to */usr/net/fr*.

Step 3 Type *frstatus* and press Enter. The Frame Relay/PPP Status Report screen appears, as shown in Figure B-5.

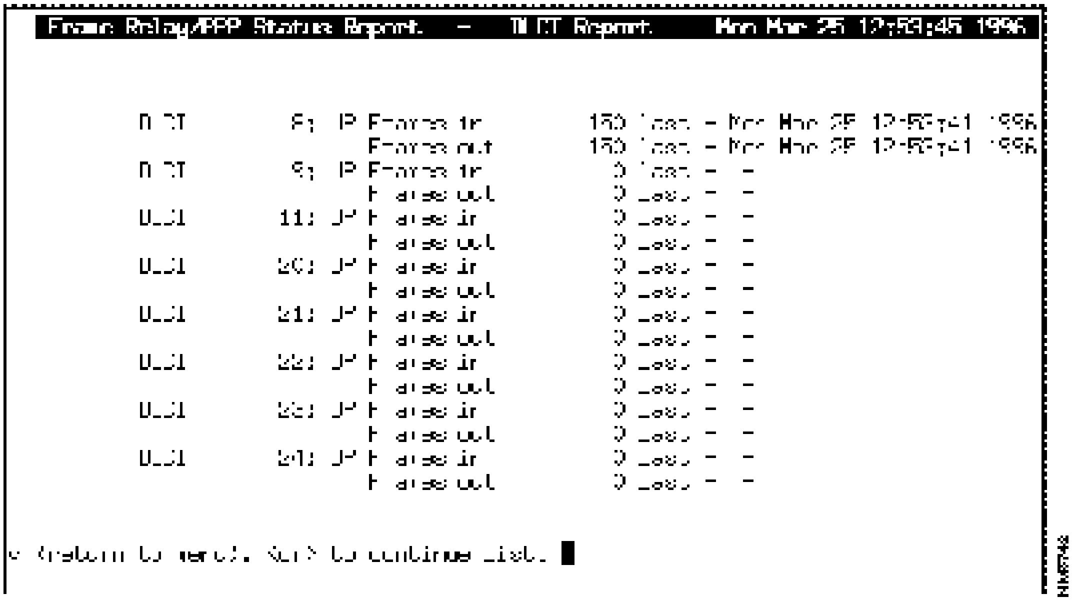
Figure B-5 Frame Relay Status Screen



```
 Frame Relay/PPP Status Report - Link/Network Status Mon Apr 29 15:02:11 1996


          Port 0 Host - State: LINKUP MODEM_ANSWERED

          LINKUP since
          Bad FCS frames received                             0
          Short frames received                               0
          I-Frames and keepalives received                    0
          I Frames and keep alives transmitted                0
          Link Management Trials                              0
          Link Management Errors                              0


p (port), d (dlci), l, as, ad, r (redraw), q (quit), z, h (help), <cr> []:
```

Step 4 Type *ad* and press enter to get a list of all the currently configured DLCIs. A DLCI Report screen, shown in Figure B-6, appears:

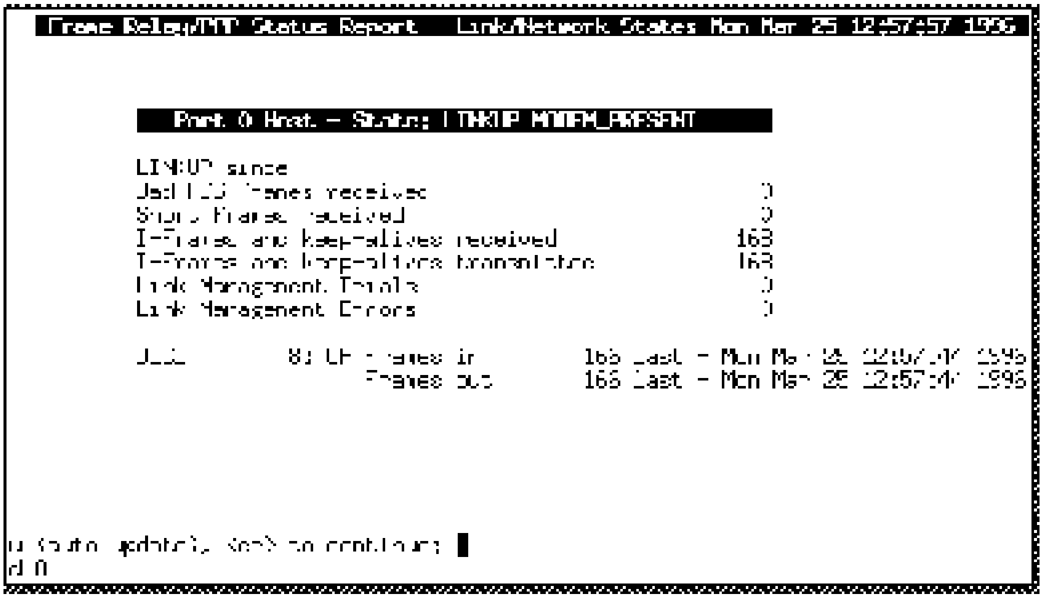
Figure B-6 DLCI Report Screen



```
 Frame Relay/PPP Status Report  -  DLCI Report     Mon Mar 25 12:53:45 1996


        DLCI        8:  IP Frames in        150 last - Mon Mar 25 12:52:41 1996
                           Frames out       150 last - Mon Mar 25 12:52:41 1996
        DLCI        9:  IP Frames in          0 last -  -
                           Frames out         0 last -  -
        DLCI       11:  IP Frames in          0 last -  -
                           Frames out         0 last -  -
        DLCI       20:  IP Frames in          0 last -  -
                           Frames out         0 last -  -
        DLCI       21:  IP Frames in          0 last -  -
                           Frames out         0 last -  -
        DLCI       22:  IP Frames in          0 last -  -
                           Frames out         0 last -  -
        DLCI       23:  IP Frames in          0 last -  -
                           Frames out         0 last -  -
        DLCI       24:  IP Frames in          0 last -  -
                           Frames out         0 last -  -

q (return to menu), <cr> to continue list.
```

Step 5 Find the DLCI you wish to monitor and press *q*. You will return to the previous screen. Type *d*, followed by a space, then the number of the DLCI, and press Enter. A Frame Relay/PPP Status Report screen, shown in Figure B-7, which includes Frames-in and Frames-out counters for the specified DLCI, will appear:

Figure B-7 Frame Relay/PPP Status Report



```
  Frame Relay/PPP Status Report    Link/Network States Mon Mar 25 12:57:57 1996



          Port 0 Host - Status: LINKUP MODEM_PRESENT

          LINKUP since
          Bad HDLC frames received                          0
          Short frames received                             0
          I-frames and keep-alives received               163
          I-frames and keep-alives transmitted            163
          Link Management Trials                            0
          Link Management Errors                            0

          DLCI        81 UP Frames in       165 Last - Mon Mar 25 12:57:47 1996
                            Frames out      166 Last - Mon Mar 25 12:57:47 1996





u (auto update), <cr> to continue: █
d 0
```

Step 6 To clear the Frames-in and Frames-out counters, press Enter, the *q*, and you will return to the VNS UNIX file directories. Type *frroute* and press Enter.

Step 7 To return to the *Frame Relay Status Utility*, type *frstatus* and press Enter. Type z and press Enter to zero the other Frame Relay Status counters.

Step 8 Type d, followed by a space, then the number of the DLCI, and press Enter. The Frame Relay Status Report screen will appear with all counters zeroed.

Step 9 Type *u 1*, to update the screen at one second intervals. Observe the seconds indicators in the current time at the top of the screen are incrementing. This screen is now being refreshed and you can observe the counters to detect what is happening on the selected DLCI.

Note You can access a Help menu from the main Frame Relay/PPP Status Report screen, by typing *h* and pressing Enter.

Troubleshooting Voice (i.e., PBX) Connections

Voice connections are the end-users connection over the VNS WAN switching network. The following is a list of common symptoms with corrective steps:

Step 1 If the handset is lifted, but there is no dial tone:

- Make sure the signaling PVCs are built.
- At the SV+ Workstation, check the Event Browser for a “link up” message.

Step 2 If you have dial tone at the handset, but can not complete a call:

- Make sure that the correct Stack Type (QSIG or DPNSS) has been configured. Using the VNS Configuration Interface, open the VNS Information menu and look at the Stack Type field. (The VNS Configuration Interface is described in Chapter 7.)
- If the Stack Type is correct, make sure that the Addresses for the VNS network are configured correctly. Reconfigure the addresses and try remaking the call.
- Make sure that the Clock Sources are configured correctly in the network.

VNS Traps

VNS Error messages are SNMP Traps sent from the VNS to the SV+ Workstation. Each trap usually has a number associated with a corresponding value in the INS Management Information Base (MIB). Traps can have a severity of either, clear, minor, or major. Table B-1 lists and describes the VNS Traps.

Table B-1 INS Traps

Trap	Description
coldStart	Standard SNMP Trap generated whenever the VNS is powered on.
insStartUpTrap	Generated whenever the VNS is started up. It indicates the current status and role of the INS.
insStatusTrap	Generated when the VNS status changes or whenever a new SNMP Manager comes in and registers for traps with the VNS. It indicates the current status of the VNS.
insRoleTrap	Generated whenever the role of the VNS in the redundant VNS pair changes. It indicates the new role of the VNS.
insNodeStateTrap	Generated when the VNS detects a change in the state of a node. The VNS determines that a node has gone out of service if it loses heartbeat with the node and it determines that a node has come back into service if it regains heartbeat with the node.
insPortDownTrap[1]	Generated when the VNS loses connection to a UNI port (i.e., a port connected to a PBX).
insSPNNIDownTrap	Generated when the SPNNI connection between two adjacent VNS nodes goes down. It indicates the name of the adjacent VNS to which the connection has been lost.
insAddrConfigFailTrap	Generated when the VNS fails to configure an address added by SV+ into operation of a port.
insNetAddrConfigFailTrap[1]	Generated when the DNÍ fails to configure a network address added by SV+ into operation on a port.
insScreenTypeConfigFailTrap[1]	Generated when the VNS fails to configure screening on a port to operate according to the specified type.
insScreenConfigFailTrap[1]	Generated when the VNS fails to configure a screen added by SV+ into operation on a port.
insTransConfigFailTrap[1]	Generated when the VNS fails to configure a transformation rule added by SV+ into operation on a port.
insSPNNIUpTrap	Generated when the SPNNI connection between two adjacent VNSes comes up. It indicates the name of the adjacent DSN to which the connection has been regained.
insDchannelDownTrap	Generated whenever the D-channel for a port goes down.
insDchannelUpTrap	Generated when the D-channel for a port comes back up.
insAlarmStatusChanged-Trap	Generated when the insAlarm Status object changes.

[1] These traps are not currently used.

Cause Codes

Cause Codes are coded messages passed from a PBX to the VNS to indicate why a switched connection cannot be made. Cause Codes are included in Call Detail Records (see Appendix C) or they can be seen with a protocol analyzer capturing the message traffic between a PBX and the VNS. The following sections describe the Cause Codes for the QSIG or DPNSS protocols:

- ISDN-Related Cause Codes
- DPNSS-Related Cause Codes

ISDN-Related Cause Codes

Table B-2 lists the set of Cause Codes that are applicable to ISDN-related calls. The ISDN-related cause codes are returned by the QSIG, JISDN (Q931A), EISDN (European ISDN, also referred to as ETSI), and AT&T 4ESS ISDN protocols. The table lists each Cause Code by number, then provides a textual description and explanation. Cause Codes are divided into the following classes within the table:

- Normal class
- Resource unavailable class
- Service or option unavailable class
- Service or option not implemented class
- Invalid message class
- Protocol error class
- Interworking class

Table B-2 ISDN-Related Cause Codes

Cause Code	Description
	Normal Class
1	**Unallocated (unassigned) number** This cause indicates that the called party cannot be reached because, although the called party number is in a valid format, it is not currently allocated (assigned).
2	**No route to specified transit network (national use)** This cause indicates that the equipment sending this cause has received a request to route the call through a particular transit network which it does not recognize. The equipment sending this cause does not recognize the transit network either because the transit network does not exist or because that particular transit network, while it does exist, does not serve the equipment which is sending this cause. This cause is supported on a network-dependent basis.
3	**No route to destination** This cause indicates that the called party cannot be reached because the network through which the call has been routed does not serve the destination desired. This cause is supported on a network-dependent basis.
4	**Send special information tone** This cause indicates that the called party cannot be reached for reasons that are of a long term nature and that the special tone should be returned to the calling party.
5	**Misdialled trunk prefix (national use)** This cause indicates the erroneous inclusion of a trunk prefix in the called party number.

Table B-2 ISDN-Related Cause Codes (Continued)

Cause Code	Description
6	**Channel unacceptable** This cause indicates that the channel most recently identified is not acceptable to the sending entity for use in this call.
7	**Call awarded and being delivered in an established channel** This cause indicates that the user has been awarded the incoming call, and that the incoming call is being connected to a channel already established to that user for similar calls (e.g., packet-mode X.25 virtual calls.
8	**Pre-emption** This cause indicates that the call is being preempted.
9	**Preemption - circuit reserved for reuse** This cause indicates that the call is being preempted and the circuit is reserved for reuse by the preempting exchange.
16	**Normal call clearing** This cause indicates that the call is being cleared because on of the users involved in the call has requested that the call be cleared. Under normal situations, the source of this cause is not the network.
17	**User busy** This cause is used to indicate that the called party is unable to accept another call because the user busy condition has been encountered. This cause value may be generated by the called user or by the network. In the case of user determine user busy, it is noted that the user equipment is compatible with the call.
18	**No user responding** This cause is used when a called party does not respond to a call establishment message with either an alerting or connection indication within the prescribed period of time allocated.
19	**No answer from user (user alerted)** This cause is used when the called party has been alerted but does not responded with a connect indication within a prescribed period of time. Note -- This cause is no necessarily generated by Q.931 procedur3es buy may be generated by internal network timers.
20	**Subscriber absent** This cause value is used when a mobile station has logged off, radio contact is not obtained with a mobile station or if a personal telecommunication user is temporarily not addressable at any user-network interface.
21	**Call rejected** This cause indicates that the equipment sending this cause does not wish to accept this call, although it could have accepted the call because the equipment sending this cause is neither busy nor incompatible. This cause may also be generated by the network, indicating that the call was cleared due to a supplementary service constraint. The diagnostic field may contain additional information about the supplementary service and reason for rejection.
22	**Number changed** This cause is returned to a calling party when the called party number indicated by the calling party is no longer assigned. The new called party number may be optionally be included in the diagnostic field. If a network does not support this cause value, cause No. 1, unallocated (unassigned) number shall be used.

Table B-2 ISDN-Related Cause Codes (Continued)

Cause Code	Description
26	**Non-selected user clearing** This cause indicates that the user has not been awarded the incoming call.
27	**Destination out of order** This cause indicates that the destination indicated by the user cannot be reached because the interface to the destination is not functioning correctly. The term “not functioning correctly” indicates that a signaling message was unable to be delivered to the remote party; e.g., a physical layer or data link layer failure at the remote party, or user equipment off-line.
28	**Invalid number format (address incomplete)** This cause indicated that the called party cannot be reached because the called party number is not in a valid format or is not complete. Note: This condition may be determined: --immediately after reception of an ST signal; or --on time-out after the last received digit.
29	**Facility rejected** This cause is returned when a supplementary service requested by the user cannot be provided to the network.
30	**Response to STATUS ENQUIRY** This cause is included in the STATUS message when the reason for generating the STATUS message was the prior receipt of a STATUS ENQUIRY message.
31	**Normal, unspecified** This cause is used to report a normal event only when no other cause in the normal class applies.
Resource unavailable class	
34	**No circuit/channel available** This cause indicates that there is no appropriate circuit/channel presently available to handle the call.
38	**Network out of order** This cause indicates that the network is not functioning correctly and that the condition is likely to last a relatively long period of time; e.g., immediately re-attempting the call is not likely to be successful.
39	**Permanent frame mode connection out-of-service** This cause is included in a STATUS message to indicate that a permanently established frame mode connection out-of-service (e.g., due to equipment section failure) (See Annex A/Q.933).
40	**Permanent frame mode connection operational** This cause is included in a STATUS message to indicate that a permanently established frame mode connection is operational and capable of carrying user information (see Annex A/Q.933).
41	**Temporary failure** This cause indicates that the network is not functioning correctly and that the condition is not likely to last a long period of time; e.g., the user may wish to try another call attempt almost immediately. This cause code may occur when the node (IGX or IPX switch) is short on resources.
42	**Switching equipment congestion** This cause indicates that the switching equipment generating this cause is experiencing a period of high traffic.

Table B-2 ISDN-Related Cause Codes (Continued)

Cause Code	Description
43	**Access information discarded** This cause indicates that the network could not deliver access information to the remote user as requested, i.e., user-to-user information, low layer compatibility, high layer compatibility, or sub-address, as indicated in the diagnostic.
44	**Requested circuit/channel not available** This cause is returned when the circuit or channel indicated by the requesting entity cannot be provided by the other side of the interface.
46	**Precedence call blocked** This cause indicates that there are no preemptable circuits or that the called user is busy with a call of equal or higher preemptable level.
47	**Resource unavailable, unspecified** This cause is used to report a resource unavailable event only when no other cause in the resource unavailable class applies.
	Service or option unavailable class
49	**Quality of Service not available** This cause is used to report that the requested Quality of Service, as defined in Recommendation X.213, cannot be provided (e.g., throughput or transit delay cannot be supported).
50	**Requested facility not subscribed** This cause indicates that the user has requested a supplementary service which is implemented by the equipment which generated this cause, but the user is not authorized to use.
53	**Outgoing calls barred within CUG** This cause indicates that although the calling party is a member of the CUG for the outgoing CUG call, outgoing calls are not allowed for this member of CUG.
55	**Incoming calls barred within CUG** This cause indicates that although the called party is a member of the CUG for the incoming CUG call, incoming calls are not allowed to this member of the CUG.
57	**Bearer capability not authorized** This cause indicates that the user has requested a bearer capability which is implemented by the equipment which generated this cause but the user is not authorized to use.
58	**Bearer capability not presently available** This cause indicates that the user has requested a bearers capability which is implemented by the equipment which generated this cause but is not available at this time.
62	**Inconsistency in designated outgoing access information and subscriber class** This cause indicates that there is an inconsistency in the designated outgoing access information and subscriber class.
63	**Service or option not available, unspecified** This cause is used to report a service or option not available when no other cause in the service or option not available class applies.
	Service or option not implemented class
65	**Bearer capability not implemented** This cause indicates that the equipment sending this cause does not support the bearer capability requested.

Table B-2 ISDN-Related Cause Codes (Continued)

Cause Code	Description
66	**Channel type not implemented** This cause indicates that the equipment sending this cause does not support the channel type requested.
69	**Requested facility not implemented** This cause indicates that the equipment sending this cause does not support the requested supplementary service.
70	**Only restricted digital information bearer capability is available (national use)** This cause indicates that the calling party has requested an unrestricted bearer service but that the equipment sending this cause only supports the restricted version of the requested bearer capability.
79	**Service or option not implemented, unspecified** This cause is used to report a service or option not implemented event only when no other cause in the service or option not implemented class applies.
	Invalid message (e.g., parameter out of range) class
81	**Invalid call reference value** This cause indicates that the equipment sending this cause has received a message with a call reference which is not currently in use on the user-network interface.
82	**Identified channel does not exist** This cause indicates that the equipment sending this cause has received a request to use a channel not activated on the interface for a call. For example, if a user has subscribed to those channels on a primary rate interface numbered from 1 to 12 and the user equipment or the network attempts to use channels 13 through 23, this cause is generated.
83	**A suspended call exists, but this call identity does not** This cause indicates that a call resume has been attempted with a call identity which differs from that in use for any presently suspended call(s).
84	**Call identity in use** This cause indicates that the network has received a call suspended request containing a call identity (including the null call identity) which is already in use for a suspended call within the domain of interfaces over which the call might be resumed.
85	**No call suspended** This cause indicates that the network has received a call resume request containing a call identity information element which presently does not indicated any suspended call within the domain of interfaces over which calls may be returned.
86	**Call having the requested call identity has been cleared** This cause indicates that the network has received a call resume request containing a call identity information element indicating a suspended call that has in the meantime been cleared while suspended (either by network timeout or by the remote user).
87	**User not member of CUG** This cause indicates that the called user for incoming CUG call is not a member of the specified CUG or that the calling user is an ordinary subscriber calling a CUG subscriber.
88	**Incompatible destination** This cause indicates that the equipment sending this cause has received a request to establish a call which has low layer compatibility, high layer compatibility, or other compatibility attributes (e.g., data rate) which cannot be accommodated.

Table B-2 ISDN-Related Cause Codes (Continued)

Cause Code	Description
90	**Non-existent CUG** This cause indicates that the specified CUG does not exist.
91	**Invalid transit network selection (national use)** This cause indicates that a transit network identification was received which is of an incorrect format as defined in Annex C/Q.931.
95	**Invalid message, unspecified** This cause is used to report an invalid message event only when no other cause in the invalid message class applies.
	Protocol error (e.g., unknown message) class
96	**Mandatory information element is missing** This cause indicates that the equipment sending this cause has received a message which is missing an information element which must be present in the message before the message can be processed.
97	**Message type non-existent or not implemented** This cause indicates that the equipment sending this cause has received a message with a message type it does not recognize either because this is a message not defined or defined by not implemented by the equipment sending this cause.
98	**Message not compatible with call state or message type non-existent or not implemented** This cause indicates that the equipment sending this cause has received a message that the procedures do not indicate this is a permissible message to receive while in the call state, or a STATUS message was received indicating an incompatible call state.
99	**Information element/parameter non-existent or not implemented** This cause indicates that the equipment sending this cause has received a message which includes information element(s)/parameter(s) not recognized because the information element identifier(s)/parameter(s) are not defined or are defined but not implemented by the equipment sending the cause. This cause indicates that the information element(s)/parameter(s) were discarded. However, the information element is not required to be present in the message in order for the equipment sending the cause to process the message.
100	**Invalid information element contents** This cause indicates that the equipment sending this cause has received an information element which it has implemented; however, one or more fields in the information element are coded in such a way which has not been implemented by the equipment sending this cause.
101	**Message not compatible with call state** This cause indicates that a message has been received which is incompatible with the call state.
102	**Recovery on timer expiry** This cause indicates that a procedure has been initiated by the expiry of a timer in association with error handling procedures.
103	**Parameter non-existent or not implemented - passed on (national use)** This cause indicates that the equipment sending this cause has received a message which includes parameters not recognized because the parameters are defined not implemented by the equipment sending the cause. The cause indicates that the parameter(s) were ignored. In addition, if the equipment sending this cause is an intermediate point, then this cause indicates that the parameter(s) were passed on unchanged.

Table B-2 ISDN-Related Cause Codes (Continued)

Cause Code	Description
110	**Message with unrecognized parameter discarded** This cause indicates that the equipment sending this cause has discarded a received message which includes a parameter that is not recognized.
111	**Protocol error, unspecified** This cause is used to report a protocol error event only when no other cause in the protocol error class applies.
	Interworking class
127	**Interworking, unspecified** This cause indicates that there has been interworking with a network which does not provide causes for actions it takes. Thus, the precise cause for a message which is being sent cannot be ascertained.

DPNSS-Related Cause Codes

Table B-3 lists the DPNSS-related cause codes. For each code, the table lists the mnemonic, the clearing or rejection cause, the meaning of the code, and the hexadecimal value associated with the code.

Table B-3 DPNSS Cause Codes

Mnemonic	Clearing/Rejection Cause	Meaning	Hex Value
AB	Access Barred	Used when a particular caller is barred access to outgoing routes.	29H
ACK	Acknowledgment	Used to inform the Requesting PBX that the Supplementary Service has been (or is being) carried out.	14H
AI	Address Incomplete	Used when insufficient address digits have been received to achieve a valid address, unless conflict dialing is permitted. Where conflict dialling is permitted, NU shall be used.	01H
BY	Busy	Used when the called party is engaged on a call.	08H
CHOS	Channel Out of Service	Used to reject a call received on a channel which is out of service or uninstalled.	23H
CNR	DTE Controlled Not Ready	Used when the called X.21 terminal is in the “controlled not ready” state.	2DH
CON	Congestion	Used when PBX equipment or suitable routes are busy.	07H
CT	Call Termination	Used when a party releases a call by clearing in the normal way.	30H
FNR	Facility Not Registered	Used when a PBX receives a request relating to a service where previous knowledge of its existence is necessary, but that knowledge does not exist (e.g., a Call Back When Free call made to a PBX with no record of original registration.	18H
ICB	Incoming Calls Barred	Used when the called party is barred to incoming calls.	OAH
INC	Service Incompatible	Used when the route available does not conform to the required SIC.	13H

Table B-3 DPNSS Cause Codes (Continued)

Mnemonic	Clearing/Rejection Cause	Meaning	Hex Value
MNU	Message Not Understood	Used when rejecting an unrecognized message on an idle channel. Note that the channel on which MNU was received may not be the one on which the unrecognized message was detected because Transit PBXes pass on Clearing Causes unchanged.	1AH
NAE-E	Network Address Extension-Error	Used to inform the Requesting PBX that a call has been rejected because of failure to process the received NAE data.	1EH
NT	Network Termination	Used when the call is released by the network for any reason (e.g., due to a timeout expiring or service interactions).	02H
NU	Number Unobtainable	Used when the Destination Address is invalid (i.e., spare).	00H
PFR	Priority Force Release	Used when an authorized intruding party forces the release of an unwanted party, e.g., an operator or a party with the required Breakdown Capability.	24H
REJ	Reject	Used when the requesting or requested party of a Supplementary Service rejects the service (e.g., Wanted party rejects a Call Offer request).	19H
ROS	Route Out of Service	Used when all suitable routes are out of service.	1CH
SI	Subscriber Incompatible	Used when the called party does not conform to the requested SIC.	04H
SNU	Signal Not Understood	Used when rejecting message contents which have not been understood. This CC is accompanied by the string SNU which either identifies a String which has not been understood or indicates another reason for not understanding the message (e.g., syntax error).	15H
SNV	Signal Not Valid	Used only when a PBX working to Issue 1 of DPNSS 1 rejects a Supplementary Information String that is invalid.	16H
SOS	Subscriber Out of Service	Used when the called party is out of service.	09H
SSI	Signaling System Incompatible	Used when the requested Supplementary Service is not supported by the route available, and there is no other suitable route.	1BH
STU	Service Temporarily Unavailable	Used when the requested Supplementary Service is available on the PBX, but cannot be provided at the moment.	17H
SU	Service Unavailable	Used when the requested Supplementary Service is supported by the PBX, but not by the called party. This Clearing Cause is accompanied by the String SU which identifies the service being rejected.	03H
TRFD	Transferred	Used (by Issue 2 and Issue 3 PBXes only) to instruct the Branching PBX of a 3-party call to connect together the two remaining parties.	1DH
UNR	DTE Uncontrolled Not Ready	Used when the called X.21 terminal is in the “Uncontrolled Not Ready” state.	2EH

Hard-Coded Cause Codes

A special file is included with the VNS software that allows five commonly used cause codes to be mapped to a single code. With the inclusion of this file, Cause Codes 2, 3, 38, 41, and 42 are all mapped to Code 34. Code 34 is then passed to PBX's attached to the VNS WAN switching network. This allows the PBX to reroute a call across a public switched network if there is a failure in the Cisco VNS WAN switching network. Call Customer Service for further information.

Configurable Cause Codes

The VNS allows you configure specific cause codes to be returned to a PBX on a per-port basis. To find out more information about this cause code mapping, refer to the section Cause Code Mapping in Chapter 7.

Call Detail Records

The VNS records information about each voice (or data) SVC call in a Call Detail Record (CDR). The CDRs are collected in files (billing.n) so that they can be uploaded by an SV+ Workstation or other billing system and used for billing. There are two CDR file parameters (CDR File Count and CDR File Interval) which are configured with the VNS Configuration Interface and are described in Chapter 7 in the section, VNS Information. These parameters specify the number of CDR files that the VNS will generate before writing over them and the interval in minutes for which a file will be generated.

This appendix describes the CDRs in the following sections:

- CDR Billing File Format
- Additional Billing Information
- Billing Example

CDR Billing File Format

The current version of the DPNSS billing file has the following format for the CDR record. The following is an example of a billing file:

```
--------------------------------------------------------------------------------
CP_BILLING_FILE,  VERSION_1,  12/06/1997 17:52:27 PDT
0.v, 600007, 900007, b4dns20-7-1, b4dns175-1,  12/06/1997 18:11:53, 0, 16, 0
1.d, 600004, 900007, b4dns20-7-1, b4dns19-5-1, 12/06/1997 18:33:24, 12, 41, 48
---------------------------------------------------------------------------------
```

The file is in ASCII format. It contains a file header that identifies the file as a billing file using the keyword CP_BILLING_FILE followed by the demarcating token “, “. Next the file identifies its version as VERSION_1 followed by “, “ this will allow for future modifications of the billing format. Next the header contains an ASCII timestamp indicating the local time that the file was created. The file header also displays the configured time zone (PDT) of the VNS. Following this header, individual CDR records will be written as ASCII strings with each record separated by a new line “\n” character.

The CDR will contain the following fields separated by the “, “ token.

1. Record number - a sequential number that identifies the individual records (0, then 1 in the first column of the example file).
2. Voice (v) or data (d) call indicator.
3. Calling number (600007 in the first record in the example file).
4. Called number (900007 in the first record in the example file).
5. Local switch node name, local CVM slot number, and local channel number separated by the “-” token (b4dns20-7-1 in the first CDR in the example file).
6. Remote switch node name, remote CVM slot number, and remote channel number separated by the “-” token (b4dns175-1 in the first CDR in the example file).
7. Record creation date and timestamp separated by a space. Date is specified in the mm/dd/yyyy format. Timestamp is specified in Universal Co-ordinated Time, hh/mm/ss (12/06/1997 18:11:53 in the first CDR in the example file).

Note All dates on the VNS are displayed in the mm/dd/yyyy format to prevent problems when the year 2000 arrives.

8. Elapsed time in seconds (defined as time difference from above timestamp to first message that released call) (0 in the first CDR in the example file).
9. Call Failure Class (VNS defined, it shall be 0 if the VNS did not force the call to be released) (16 in the first CDR in the example file).
10. Protocol specific Call Failure Class (DPNSS or QSIG defined value) (0 in the first CDR in the example file).

Additional Billing Information

Location of Billing

An environment variable VNS which is assigned during the installation of the system defines the root directory for the billing related files.

>From directory $VNS a sub-directory ‘files’ exists and this is the target directory for the billing files.

The billing process collects billing information and creates files in the directory $VNS/files with the name billing.0 billing.1 billing.2 .... billing.n where n indicates the configured number of billing files that the system wants to stored before wrapping around.

Other configured parameters are

- The size of the files
- The maximum lifetime of the files

Retrieval of Billing Files

After the VNS has written a file another entity will retrieve the file and use the stored information for billing calculation. This external entity may FTP (file transfer protocol) the desired files from the VNS.

It is expected the billing application will periodically retrieve and delete the billing files from the VNS disk at a rate adequate to avoid the VNS billing process overwriting billing files that have not been retrieved.

Billing Example

For this example, assume the following:

1. The file size has been configured for 100,000 bytes per file.
2. Each billing record is 100 bytes long => 1000 records per file.
3. The system is configured to store 20 files.
4. The system is running at 1 call per second => 3600 calls per hour.
5. Assume that the VNS environment variable is set to /usr/dns.

System Operation

The system creates the first billing file in /usr/dns/files and names it billing.0. Billing records are added to this billing file at a rate of 1 per second; thus, the billing file reaches its maximum size after 1000 seconds (approximately 20 minutes).

After 1000 seconds, the first billing file is closed and the second one is opened as billing.1. This continues until the system has cycled through all 20 files that it uses. When it attempts to open the 21 file it does not open billing.20 but instead it resets the counter to 0 and opens billing.0. If billing.0 is still on the file system its contents are deleted.

Billing File Collection

The billing application must collect the billing files from the VNS. To prevent the loss of billing information, each individual file must be transferred (FTPed) from the VNS (19*1000 seconds), approximately every six hours if the configuration as assumed above is used. The billing application may invoke the FTP operation once the file has reached its maximum size. It may also delete the file once it has been collected but this is not necessary.

The configuration parameters given above may be increased at the expense of disk space to allow a number of days records be stored prior to the overwriting of information.

Dial-In Support

Motorola V.34R VNS Dial-In Configuration

During the initial installation of the VNS, Cisco strongly recommends that a modem be attached to the serial port and configured to auto-answer calls from our Product Support. By dialing in, Product Support can access the VNS remotely and resolve potential problems. An optional Motorola V.34R Modem can be purchased from Cisco. (For initial trials, the modem is required.)

This setup prepares a modem attached to the VNS to answer a call from Cisco's Product Support. You should arrange to work with Cisco Product Support to initially set up and test the modem for dial-in operation (i.e., auto answer). Cisco must record the telephone number for dialing into the VNS.

The port on the VNS should be factory-configured for 9600 bps and VT100 mode. Table E-1 lists the modem interface requirements.

Table D-1 Modem Interface Requirements

Parameter	Requirement
VNS Port	Serial port, A/B (Terminal)
Code	Standard 8-bit ASCII, 1 stop bit, no parity
Interface	RS232 DCE
Cable	25-pin straight through cable
Phone Lines	Dedicated dial-up business telephone line for ISC-to-VNS modem connection
Data Rate	All standard asynchronous data rates from 300 to 19200 bps, independently selectable
Supported Modems	Motorola Model V.34R 9600 baud modem

There are two procedures to be performed before Product Support can dial into the VNS:

- Configure the VNS's Serial Port to Emulate a VT100 Terminal.
- Connect and Configure the Modem for the VNS.

These procedures are for a typical connection. Refer also to the *Modem User's Guide*.

Configure the VNS's Serial Port to Emulate a VT100 Terminal

Typically the serial port on the VNS-AC or VNS-DC is factory-configured for 9600 bps and VT100 mode. If it is not, you can configure the serial port (A/B [Terminal]) as follows:

Step 1 Login to the VNS as superuser (i.e., root).

Step 2 Edit the /etc/ttytab file as follows:

```
ttyb “/usr/etc/getty D9600” dialup on remote
```

Step 3 Check to see if **getty** is running for ttyb by entering:

```
ps -aux | fgrep getty
```

Step 4 Note the process ID so you can kill it and restart the **getty**.

Step 5 If a **getty** is already running for the specified port, find its process id, then issue:

```
kill -9 <process ID>
```

Step 6 Restart init by entering:

```
kill -HUP 1
```

Step 7 This command restarts the new **getty**.

Note To connect a modem to a VNS-AC-E or VNS-DC-E, the factory-installed soft switch cable may have to be removed. Contact Cisco Customer Service for details.

Connect and Configure the Modem for the VNS

To connect and configure the modem for dial-in operation, follow these steps:

Step 1 Connect power to the modem.

Step 2 Temporarily attach a terminal to the modem EIA port, using a straight-through cable. The modem's EIA port will automatically match the 9600 bps setting of the terminal.

Step 3 Configure the modem for 8 bits, no parity, and 1 stop bit.

Step 4 Enter the commands listed in Table E.2 to set up the modem for proper operation.

Step 5 Disconnect the terminal and connect that end of the cable to the VNS port (A/B [Terminal]). (The other end remains connected to the EIA port on the modem.)

Step 6 Connect the modem to the phone line.

Step 7 Ask the Cisco Product Support to test the operation of the dial-in modem.

Table D-2 Setting up the Motorola V.34R Modem for Auto-Answer Mode

Step	Command	Function
1	AT&F&W	Reset to factory default and save.
2	ATS0=1	Enables Auto-Answer Mode (answer on first ring).
3	ATL1	Modem speaker at low volume.
4	AT*SM3	Enables automatic MNP error correction.
5	AT*DC0	Disables data compression.
6	AT*FL0	Disables XON/XOFF flow control.
7	AT&S1	Sets DSR to “normal”.
8	ATE0	Disables local character echo.
9	ATQ1	Disables result codes. (Modem will appear “dead”.)
10	AT&W	Saves current configuration settings in non-volatile memory.

Hayes Modems

Not all of the modem EIA leads are supported by the VNS. If a Hayes modem is used in place of the MotorolaV34 Modem, configure the Hayes modem using the following AT commands:

DCD - On	AT&CØ
DTR - On	AT&DØ
DSR - Normal	AT&S1
CTS - ON when connected	AT&R1
	ATSØ=1 (answer on first ring)

When the system is up, Cisco Product Support will be able to dial in to the VNS and login as any other user on the system.

Reinstalling VNS Interface Drivers

The interface drivers for the E1 Network Interface Cards (E1 NICs) and the Frame Relay Card are pre-installed at the factory. These drivers are supplied on tape in case there is an event that requires that they be reinstalled.

This appendix contains the following sections:

- E1 NIC Driver Installation
- Frame Relay Card Driver Installation

Note Never reinstall an VNS interface driver without first contacting the Cisco Product Support.

E1 NIC Driver Installation

Tape 3 contains the E1 NIC driver package (i.e., CoE1) and a readme file with these installation instructions. The CoE1 driver package is designed to run with Solaris 2.4, the operating system of the VNS. The tape is in tar format.

To extract the contents of the tape, follow these steps:

Step 1 Connect a tape drive to the VNS.

Step 2 Insert tape 3 into the tape drive.

Step 3 Extract the contents of the tape into a directory using the following command:

```
tar xvf /dev/<tape_dev>
```

where <tape_dev> should be replaced with the specific tape drive attached to your VNS.

The contents of the tape will be extracted under the directory: /tmp

Step 4 Change your working directory to the directory containing the E1 NIC driver, CoE1DRV.

```
cd /tmp/Release.2.1
```

Step 5 Add the driver package to the VNS with the command:

```
pkgadd -d `pwd` CoE1DRV
```

The system messages during pkgadd are self explanatory. The default installation of the directory of the E1 NIC driver package is /opt.

Step 6 Verify that the driver installed correctly with the following command:

```
pkginfo | grep CoE1DRV
```

A message similar to the following should be displayed:

```
system      CoE1DRV        CoSystems E1 Device Driver Release 2.9.1
```

If a similar line is not displayed, repeat the installation procedure, watching the screen closely for error messages.

E1 NIC Configuration

The E1 Line parameters of the E1 NIC must be changed to match the parameters of the CVM or CDP on the attached node. These parameters are similar to those configured with the node's configure circuit line (**cnfcln**) command. The parameters at the E1 NIC and the node's CVM or CDP must match one another.

To edit the E1 NIC configuration, use vi to edit the file:

/etc/default/comunich.sys

The following are the configurable parameters:

Line Coding	AMI or HDB3
Signaling	CAS or CCS
CRC	CRC disabled or enabled
Equalizer	75-ohm coaxial or 120-ohm twisted pair
International bit	Selected or not selected, bit value if selected
National bits	Selected or not selected, bit values if selected
Local loop back	Enabled or disabled
Remote loopback	Enabled or disabled

The parameters are declared as keyword=parameter pair. Each set is uniquely identified by unit number.

Starting the E1 NIC Driver Daemon

After you have set the E1 NIC configuration parameters, you can start the E1 NIC Driver Daemon by following these steps:

Step 1 Change your working directory to /opt/CoE1DRV/bin.

Step 2 To run the daemon, enter from the shell prompt

./comunichd -r

(if you have only one E1 NIC in your VNS) or

./comunichd -r -u

(if you have two E1 NICs in your VNS).

The LED on the E1 NIC should glow if the E1 NIC is up and the line is synchronized.

Deinstalling the E1 NIC Driver

To deinstall the E1 NIC driver, run:

```
pkgrm CoE1DRV
```

Frame Relay Card Driver Installation

To reinstall the Frame Relay Card driver, follow these steps:

Step 1 Login to your VNS as root.

Step 2 Connect a tape drive to your VNS.

Step 3 Insert Tape 1 into the tape drive.

Step 4 Type these commands:

```
#NONABI_SCRIPTS=TRUE
#export NONABI_SCRIPTS
# /etc/init.d/volmgt stop
# pkgadd -d /dev/????
```

Step 5 Reboot your VNS by entering the following Solaris command:

```
boot -r
```

(boot with reconfiguration)

As the VNS is rebooting, watch your terminal screen carefully for messages about address selection errors. If the system comes up without displaying any error messages, go to step 6. If an address selection error is indicated, to the Troubleshooting the Frame Relay Card Driver Installation section.

Step 6 Verify the installation, by entering the following command:

```
pkginfo -l | grep ADAX
```

The pkginfo program , with the -l for long argument, will list the Frame Relay Card drivers that have been installed. The output should appear similar to the following:

```
PKGINST:  ADAXapcs
   NAME:  ADAX apcs Driver
 VENDOR:  Copyright ADAX, Inc., 1988 - 1996
PKGINST:  ADAXfr
   NAME:  ADAX Frame Relay/PPP
 VENDOR:  ADAX, Inc.
```

If similar lines are not displayed, repeat the installation procedure, watching the screen closely for error messages.

Removing the Frame Relay Card Driver

To remove the Frame Relay Card driver, follow these steps:

Step 1 From the UNIX prompt, type the command:

```
# pkgrm
```

Step 2 Follow the menu-driven instructions for removing the software package. The pkgrm program displays a list of numbered options. Choose the number that corresponds to ADAX APC DRIVER and press Enter. A message similar to the following one will be displayed:

```
Confirm

Do you really want to remove ADAX APC BOARD DRIVER,
for APC-PCX/APC-MCX, Version x.x

Strike ENTER when ready
or ESC to stop.
```

Step 3 Press Enter. The pkgrm program displays these messages:

```
Checking . . .

Removing APC device driver . . .

The UNIX operating system will now be rebuilt.

The ADAX APC BOARD DRIVER,
APC-PCX/APC-MCX, Version 2.4.x is now removed.
```

You can now shut down the VNS and reboot it. If necessary, reinstall the Frame Relay Card software.

Frame Relay Card Configuration Files

The following VNS files are normally installed at the factory:

- Frame Relay General Configuration File (*fr.cf*)
- Frame Relay Port Configuration File (*fr_config*)
- Frame Relay Address Mapping (*fr_conv*)
- Network Command File for Networks (*rc.inet*).

If the Frame Relay Card drivers have to be reinstalled, these files should be checked to see if they contain the factory settings.

Note In any of the file fragments shown here, the “#” character precedes comments on the same line.

Frame Relay General Configuration File (fr.cf)

The Frame Relay General Configuration file (*fr.cf*) is installed at */usr/net/fr/fr.cf*. The contents of the *fr.cf* file should contain the following lines:

```
#
# ADAX Frame Relay daemon configuration file
#
mode          LAC        # TCP/IP compatibility mode:  ATT, SCO, LAC, or WOL
prom          YES
debug         0          # debug level:  0 (off), 1, 3, 5, 7, 9 (most output)
# End of fr.cf
```

Frame Relay Port Configuration File (fr_config)

The Frame Relay Port Configuration file *(fr_config*) is installed at */usr/net/fr/fr_config*. The contents of fr_config should contain the following lines:

```
port 0
HOST          RS449 N393 0 INARP NO
port 8
              PID 0xCC
port 9
              PID 0xDD TRANS
# End of fr_config
```

The factory sets the following necessary parameters:

- "N393 0" turns off LMI signaling.
- "INARP NO" turns off inverse address resolution.
- "TRANS" parameter for port 9 means include FR header when passing frames to the upper level application.

Frame Relay Mapping (fr_conv)

This Frame Relay Address Mapping file (*fr_conv*) is installed at */usr/net/fr/fr_conv.* It normally includes the IP address to DLCI mapping for any IP networks accessible across frame relay.

This file will appear similar to the following:

```
#
# ADAX Frame Relay IP address to DLCI (0, . . . , 1023) to port mapping
#
# IP Address Frame Relay DLCI Port
205.9.8.1120# Router’s Serial 0 (SV+ gateway)
#
# Raw Frame Relay port
-350359# PRI using DLCI 35
# End of fr_conv
```

Network Command File (rc.inet)

This Network Command file (*rc.inet*) is installed at */usr/net/fr/rc.inet*. It typically contains the appropriate network commands to enable routing across the VNS’s IP Frame Relay network. This shell script is executed at boot time from /etc/rc2.d/S72fr (normally installed at the factory).

This file will appear similar to the following:

```
ifconfig frmux0 frhost plumb -arp
ifconfig frmux0 frhost up
#
# frnet is defined in /etc/networks
# frhost is defined in /etc/inet/hosts
route add net frnet frhost 0
#
# Use cisco (router) serial port as gateway
# nms-net is defined in /etc/networks
# nms-net-gateway is defined in /etc/inet/hosts
#
/usr/net/fr/set_addr -h `nawk '/frhost/ { print \$1 } ' /etc/hosts` -port 0
# End of rc.inet
```

Note There must be only one "frhost" present in */etc/inet/hosts* for the "set_addr" line to work.

Upgrading to VNS 3.0 Software

An upgrade from VNS 2.1 to VNS 3.0 software is performed in several steps. Since the port record structure has changed in the VNS 3.0 database with the addition of configurable cause codes (see the PBX type field in the section Port Information in Chapter 7), the upgrade procedure has to convert the database format as well as load the new software.

The upgrade procedure involves taking the standby VNS in a redundant pair off-line. The user will need to schedule a maintenance window of at least 5 hours when performing the upgrade. During the upgrade, there will not be a redundant VNS. You should carefully schedule this upgrade.

The upgrade from VNS 2.1 to VNS 3.0 software follows this sequence:

- Shut down the standby VNS
- Copy and untar the new software (QSIG3.0) onto the standby VNS
- Prepare the VNS 2.1 database to be converted to the VNS 3.0 format
- Install the VNS 3.0 software
- Convert the database to VNS 3.0 format
- Shut down the active VNS still running 2.1 software and bring up the VNS running 3.0 software
- Test the VNS with 3.0 software
- Load the VNS 3.0 software onto the other VNS

Performing an Upgrade to VNS 3.0

To upgrade both VNSs in a VNS redundant pair to VNS 3.0 software VNS, follow these steps:

The first 7 steps determine which is the standby VNS in the redundant pair, then shut it down.

Step 1 Log in to one of the VNSs in a redundant pair.

Step 2 Start the VNS CLI.

Step 3 From the VNS CLI main menu, select option 3, Modify an Entry. (The Modify an Entry submenu, which is identical to the Add an Entry submenu, will appear.)

Step 4 From the Modify an Entry submenu, select option 12, More VNS Info and Redundancy Info. (A More VNS Info and Redundancy menu appears.)

Step 5 Search through these records until you find the record with the VNS Operation Role of 2 which indicates that VNS is the standby unit.

In this procedure, since the role of active and standby will change between the two VNSs, this VNS will not be referred as VNS A; the currently active VNS will be referred to as VNS B.

Step 6 On VNS A's VNS Info and Redundancy Info menu set the Admin Status to 4 (shutdown).

Step 7 Tab down to **Enter 'c' to commit changes or 'q' to quit [ ]** field. Enter c to commit the record. The VNS process will shut down after the grace period.

The next 2 steps (Step 7 and Step 8) copy the new software tar file onto the VNS.

Step 8 FTP the tar format software release to /tmp onto VNS A.

Note Software releases are made available through Cisco Customer Service. Contact Cisco Customer Service to find the location of the FTP server containing the VNS software.

Step 9 Untar the file:

```
tar xvf VNS_QSIG3.0.tar
```

This will create a directory QSIG3.0 in the /tmp directory.

The next 2 steps (step 10 and step 11) prepare to VNS 2.1 database on VNS A to be replaced by the VNS 3.1 database format.

Step 10 Remove the VNS 2.1 database:

```
rm -rf /usr/db_21
```

Step 11 Move current VNS 2.1 database into /usr/db_21 directory:

```
mv -f /usr/vns/db /usr/db_21
```

The next step (step 12) uninstalls the VNS 2.1 software:

Step 12 Execute the vsn_uninstall script to uninstall VNS 2.1 software:

```
/usr/vns/vns_uninstall
```

The next step (step 13) installs the VNS 3.0 software:

Step 13 Execute the VNS_install script. You have to choose whether you are installing QSIG or AT&T 4ESS software:

```
./VNS_install qsig 8.2.5
or
./VNS_install 4ess 8.2.5
```

Where qsig for 4ess is the Stack Type (the protocol) of the software you are installing and it is followed by the switched software release running in your network. 8.2.5 is the default switched software release, but your network could also be running 8.5.0. If you do not enter the stack type (qsig or 4ess) and the switched software release (8.2.5 or 8.5.0), you will receive an error message. The error message, which prompts you to enter the missing information, will be similar to the following:

```
Wrong Stack Name provided. Must enter 'qsig' OR '4ess'.
```

The next step (step 14) converts the database to the VNS 3.0 format.

Step 14 Execute the vns_convert script to convert the database:

vns_convert /usr/db_21 /usr/vns/db

The next steps (step 15 and step 16) shut down the active VNS (VNS B) and bring up VNS A with the VNS 3.0 software

Step 15 Log into VNS B (that is, the VNS on which you did not load VNS 3.0 software) and shut it down, by repeating step 3 through step 7.

Caution Make sure to leave VNS B in the shutdown state. If both VNSs become active before one is up and running VNS 3.0 software, you could get them in a database mismatch state.

Step 16 Reboot the VNS A on which you just loaded VNS 3.0 software.

```
sync, sync, reboot
```

VNS A will now come up with VNS 3.0 software and a VNS 3.0 database.

Step 17 Before proceeding, test VNS A. Run the VNS CLI and make sure that this VNS is able to make calls.

The next steps (step 18 to step 22) load the VNS 3.0 software on VNS B, which you shut down in step 15.

Step 18 FTP the tar format software release to /tmp onto VNS B.

Step 19 Untar the file:

```
tar xvf VNS_QSIG3.0.tar
```

This will create a directory QSIG3.0 in the /tmp directory.

Note You won’t have to convert the VNS 2.1 database on VNS B because when it comes up, it will be updated by VNS A with the VNS 3.0 database that is now active.

Step 20 Execute the vns_uninstall script on VNS B to uninstall VNS 2.1 software:

```
/usr/vns/vns_uninstall
```

The next step installs the VNS 3.0 software on VNS B:

Step 21 Execute the VNS_install script. You have to choose whether you are installing QSIG or AT&T 4ESS software:

```
./VNS_install qsig 8.2.5
or
./VNS_install 4ess 8.2.5
```

As described in step 13, you must enter the Stack Type (qsig or 4ess) and the switched software release (8.2.5 or 8.5.0) to run the VNS_install script.

Step 22 After the VNS 3.0 software is loaded on VNS B, make sure that VNS A is active, then reboot this VNS B:

```
sync, sync, reboot
```

VNS B will startup and receive a database update from the active VNS A.

APPENDIX G

SPNNI Operation

When there are multiple VNS areas (or domains), the VNS's are connected by a Frame Relay PVC. This Frame Relay connection uses the Cisco Proprietary Network to Network Interface (SPNNI) protocol and is added when the Local Adjacency Information menu is completed. This Frame Relay PVC uses the default Frame Relay class 0. When necessary, you can modify Frame Relay class 0 with the **cnffrcls** command. Modifying Frame Relay class templates is described in the *Cisco WAN Switching Command Reference* in the Chapter, Frame Relay Connections.

This SPNNI connection will use trunk bandwidth between the nodes to which the VNS's are attached. In some VNS WAN switching networks, you may have to modify the default SPNNI connection parameters for your requirements. First you must be able to calculate the amount of bandwidth required for this SPNNI connection. The traffic over the SPNNI connection varies with the number of calls the VNS has to process.

To calculate the typical amount of bandwidth required for a SPNNI connection, you can use the following guidelines:

- Maximum channels for each SPNNI link: 256
- Maximum octets for DPNSS messages: 45
- Maximum octets for SPNNI header: 50

Using these guidelines and the expected number of calls per hour, you can calculate the SPNNI Frame Relay bandwidth. For example, say your network expects to handle 50000 VNS calls per hour and each call requires 5 messages to build and tear down the call.

The Frame Relay bandwidth for this example could be calculated as follows:

```
  5  *   (45 + 50) * 50000 / 3600      =    6597        =  51.5 kbps

 no.       max        no.     sec.          octets          Frame Relay
  of       msg        of      per            per             Bandwidth
msgs       size     calls     hour          second
 per                on the
call                SPNNI
                    per hour
```

VNS Terminology

This section defines terms that are new to the Cisco vocabulary with the advent of Voice Network Switching and common terms that have specific meaning in this VNS manual. The *Cisco Internetworking Terms and Acronyms* book, which also can be found on the Cisco CD-ROM, defines most common internetworking terms.

Break-Out/Break-In (BOBI)
BOBI is a VNS feature that allows interworking between Euro-ISDN (ETSI) and other VNS-supported signaling variants, such as DPNSS and QSIG.

Call Detail Record (CDR)
The VNS record of voice or data SVCs, which includes calling and called numbers, local and remote node names, date and timestamp, elapsed time, and Call Failure Class fields.

Channel Associated Signaling (CAS)
CAS is inband robbed-bit signaling performed on T1 lines. CAS PBXs are supported in VNS 2.2 when they are connected to an IGX Universal Voice Module with Model B firmware, supported in switched software release 8.5. The UVM performs CAS-to-QSIG conversion.

Cisco BPX® 8600 series wide-area switch
The Cisco BPX switch is a standards-based high-capacity (19.2 Gigabit) broadband ATM switches that provide backbone ATM switching and delivery of a range of user services.

Cisco IGX™ 8400 series wide-area switch
The Cisco IGX switch is a wide-area switch designed to provide a backbone for enterprise data, voice, fax, and video applications. The Cisco IGX switch was formerly referred to as the Cisco StrataCom IGX switch.

Cisco IPX® wide-area switch
The Cisco IPX switch is a wide-area switch that has been replaced in the Cisco product line with the Cisco IGX switch. The Cisco IPX switch was formerly referred to as the Cisco StrataCom IPX switch.

Cisco MGX™ 8220 edge concentrator
The MGX 8220 is an interface shelf designed to concentrate ATM and Frame Relay traffic on the edge of a WAN switching network. The MGX 8220 was previously referred to as the AXIS interface shelf.

Cisco StrataCom network
See WAN switching network.

Cisco StrataCom node

See Cisco wide-area switches: Cisco BPX switch, Cisco IGX switch, and Cisco IPX switch.

D Channel

The signaling channel used for call setup control and network connection teardown in an ISDN interface. The D channel is typically DS0 24 in a T1 interface and timeslot (TS) 16 in an E1 interface.

Local adjacency

Two VNS's which control different VNS areas but communicate with one another through a Frame Relay PVC are considered to be locally adjacent.

Intelligent Network Server (INS)

The former name for a range of products adding specific capabilities to Cisco WAN switching networks. Voice Network Switching (VNS) is one INS application, and Dial-Up Frame Relay is the other. (You will occasionally see INS on a product label or on some of the software menus.)

Multihoming

Multihoming is a VNS feature that allows two or more links to the same end-user CPE. A site may be multihomed to multiply the bandwidth capacity to meet increased traffic requirements.

Signaling network

A virtual network over-laid on top of the traditional Cisco WAN switching network through which the VNS processors communicate with one another and with the nodes. This virtual signaling network is primarily created out of frame relay PVCs between the VNS processors.

SPNNI connection

A Frame Relay connection between two VNS's in different areas or domains. The SPNNI connection gets its name form the Cisco Proprietary Network to Network Interface protocol which operates over this connection.

StrataView Plus Workstation

The network management platform for managing Cisco WAN switching networks. Cisco StrataView Plus®, the application running on the workstation, provides status information for the VNS.

UNI port

The User-to-Network Interface (UNI) where the PBX connects to a Cisco VNS WAN switching network. This is typically an IPX CDP or an IGX CVM.

VNS

The rack-mounted adjunct processor that is normally co-located with a Cisco wide-area switch (IGX or IPX switch) and has IP connectivity to a StrataView Plus Workstation. VNS will be used to specify the hardware, that is the rack-mounted box, and to the application.This should not cause any confusion because the context will make it clear whether we are talking about an individual processor or a network-wide application. (Occasionally, the INS will be used in this document to refer to the hardware.)

Note Dynamic Network Switching (DNS) was an earlier name for Voice Network Switching (VNS).

VNS WAN switching network

A traditional Cisco WAN switching network which has been enhanced with VNS processors to perform Voice Network Switching. Voice Network Switching provides voice switched virtual circuits (SVCs) across a Cisco WAN switching network for PBXs using Digital Private Network Signaling System (DPNSS), QSIG, or ETSI signaling.

Voice Port

The port (CVM on the IGX switch, or CDP on the IPX switch) on the Cisco wide-area switch which connects to the VNS Network Interface Card. The VNS can connect to up to two voice ports, which carry signaling information to and from the PBXs.

WAN switching network

The public or private network built around Cisco wide-area switches (that is, the BPX, IGX, or IPX switch). These nodes utilize Cisco's patented FastPacket technology and/or standards-based Asynchronous Transfer Mode (ATM) and are designed to support multiple applications integrating voice, constant and variable-bit rate data, video, frame relay, and ATM services on one multimedia wide area network. The WAN switching network was previously referred to as a Cisco-StrataCom network.

Channel Associated Signaling Voice Switching

Voice Network Switching (VNS) release 3.0 also supports the VNS CAS 2.2 feature. CAS 2.2 is QSIG protocol variation that works in conjunction with the IGX's Universal Voice Module (UVM) with Model B or higher firmware to provide a way for PBXs using Channel Associated Signaling (CAS) to take advantage of Voice Network Switching. The UVM with Model B firmware is supported in Switched Software Release 8.5. With this feature, IGX switches with UVM cards will convert CAS signals to QSIG protocol messages that can be interpreted by the VNS. The VNS then switches voice or data calls from the CAS PBX, just as if they supported the QSIG protocol.

Note The Universal Voice Module's complete feature set is described in the *Cisco IGX 8400 Series Reference* document for Release 8.5. This appendix describes only the UVM with Model B firmware as it relates to CAS-to-QSIG conversion for Voice Network Switching.

This appendix contains the following sections:

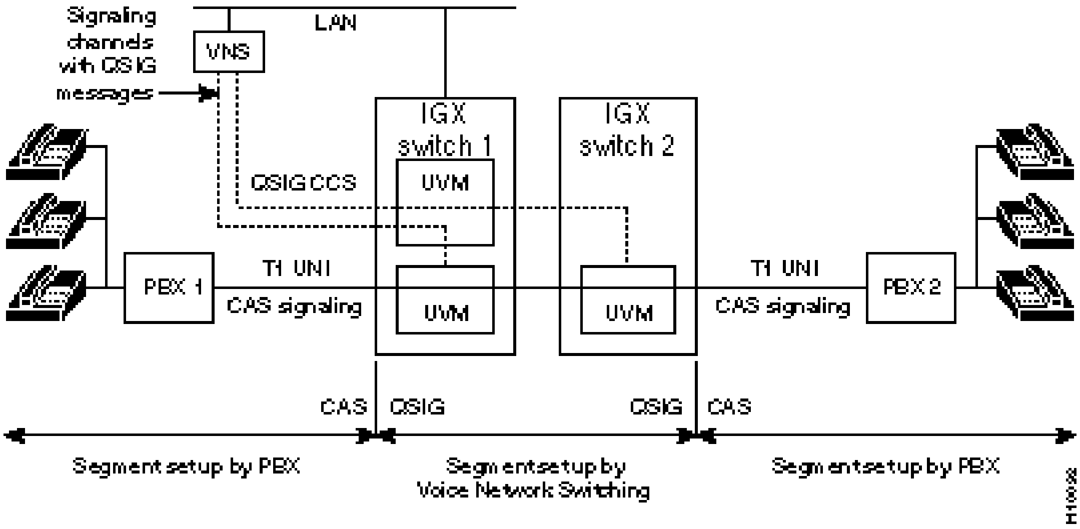
- CAS to QSIG Conversion
- Configuring CAS Switching

CAS to QSIG Conversion

The UVM card on the IGX switch converts CAS signaling and dual-tone multi-frequency tones to common channel signaling (CCS), that is, QSIG protocol, messages. The VNS subsequently routes the calls from the PBX over a Cisco WAN switching network, using voice switched virtual circuits (SVCs) under the control of a VNS.

Figure I-1 illustrates a simple CAS-to-QSIG VNS network. The two PBX's are CAS signaling. Both of their T1 trunks terminate in a UVM on an IGX switch. The UVM converts the CAS signaling to QSIG messages and routes these messages to the VNS. The VNS never sees the CAS signaling. In Figure I-1, the signaling links are shown as dashed lines; the voice or data connections (the bearer channels), which are setup and maintained by the signaling connection, are indicated by the solid line connecting the two PBX's.

Figure I-1 CAS-to-QSIG VNS Network



Signaling

There are two modes of signaling prevalent in T1 and E1 digital trunk interfaces. In the CCS mode, a single DS0 channel is dedicated to carrying signaling information for all the DS0 bearer channels. Moreover, the signaling information is carried in a message format (packets or frames). This is the mode used in T1- and E1-based ISDN trunks, and hence is the mode supported by the VNS.

In the CAS mode of signaling, DS0 channel states are encoded in bits and transmitted on the trunks in two possible ways. For CAS T1 trunks, a technique called robbed-bit signaling (RBS) is used. A single bit in every DS0 bearer channel is “stolen” from every 6th frame and used to carry signaling information. The robbed bit in frames which are odd-multiples of 6 (6th, 18th, 30th,...) is termed the ‘A’ bit, whereas the robbed bit in frames which are even multiples of 6 is termed the ‘B’ bit. In CAS E1 trunks, TS16 (timeslot 16) is used to carry the signaling bits for *all* channels, but in a bit-to-channel mapped format. Each frame, except the first, carries a 4-bit signaling payload for 2 DS0s. It thus requires 15 frames to deliver the signaling information for the 30 DS0 bearer channels.

Note VNS CAS 2.2 does not support E1 CAS.

Gateway Function

To enable connections on CAS trunks to be switched through a Cisco WAN switching network using the VNS, the CAS signaling information must be translated into near-equivalent CCS messages. This “gateway” function is performed by the UVM interfaces on the IGX switch that terminate the digital CAS trunks. Once the CAS signaling is converted to CCS signaling messages, they may be forwarded to and processed by the VNS.

With the CAS feature, the CCS protocol is operating between the IGX’s UVM card and the VNS. The UVM always performs the master role in channel allocation protocol, so the VNS must be set to slave.

DS0 25

Since all 24 DS0s (timeslots) of the CAS T1 interface are used to carry signaling and user information, the UVM CAS-to-QSIG conversion process creates a pseudo channel, DS0 25, to carry signaling messages to the VNS. DS0 25 is a logical channel that exists only between the UVM and the VNS. So, for CAS-to-QSIG UNI ports, the UNI Channel field of the Port Information menu must be configured as 25. The UNI Channel field is described in Chapter 7, Understanding the VNS Configuration Interface in the section, Port Information.

Configuring CAS Switching

CAS switching is similar to configuring Voice Network Switching for the other VNS protocols (that is, QSIG, DPNSS, JISDN and AT&T 4ESS ISDN.)

First you rack mount the VNS with its co-located IGX switch as described in Chapter 4, Rack Mounting the VNS. Next you connect power to the VNS as described in Chapter 5, Connecting Power to the VNS. Then you connect the VNS interfaces to the node as described in Chapter 6, VNS Interface Connections. Then you connect the CAS BPX to the IGX UVM as described in the *Cisco IGX 8400 Series Installation* manual and *Cisco IGX 8400 Series Reference* document for Release 8.5 in the section, Connecting the UVM to T1 Lines. The *Cisco Command Reference* for Release 8.5 also contains general procedures for setting up circuit lines and configuring voice connections.

When connecting the CAS PBX to the UVM for Voice Network Switching, however, there are some special configuration procedures that must be performed. For CAS-to-QSIG conversion, configure the UVM as follows:

Step 1 Use **upln** to activate a circuit line in the slot containing the UVM.

Step 2 Use **cnfln** to configure the line to match the CAS PBX.

Step 3 Use **cnfcassw** (configure CAS switching) to configure the CAS-to-QSIG feature. This command will bring a menu similar to the following:

```
vnsigx8        TN    StrataCom       IGX 16    8.5.B0    Sep. 15 1997 23:59 PST

Line 8.1 CAS Switching Parameters
   CASSW mode    [PBX-END]                 Parm 11       [00] (H)
   CCS Type      [ 1] (D)                  Parm 12       [00] (H)
   CAS Type      [ 1] (D)                  Parm 13       [00] (H)
   Conn Type     [a24   ]                  Parm 14       [00] (H)
   Country code  [00] (H)                  Parm 15       [00] (H)
   Interdigit TO [05] (H)                  Parm 16       [00] (H)
   Tone level    [00] (H)                  Parm 17       [00] (H)
   DTMF duration [0C] (H)                  Parm 18       [00] (H)
   Idle pattern  [7F] (H)
   Parm 6        [00] (H)
   Parm 7        [00] (H)
   Parm 8        [00] (H)
   Parm 9        [00] (H)
   Parm 10       [00] (H)

Last Command: cnfcassw 8.1


Next Command:
```

The **cnfcassw** command is used only for configuring CAS switching on the IGX's UVM. Only the first 9 fields of this screen are used at this time. Parm 6 through Parm 18 are reserved for future use. The first 8 fields and their possible values are:

- CASSW mode: p for PBX-end, s for Server-end, o for Off. The default is off. This parameter must be turned on (that is, p, PBX-END) for the UVM connected to the CAS PBX.

Note If CAS-Switching mode is set to Server-end, that is, the UVM is connected to a VNS, it will only allow the entry of CCS type as all remaining parameters are irrelevant. If CAS-Switching mode is set to OFF, then it will not allow any more parameters to be entered.

- Conn Type: any UVM supported voice type. The UVM supports all compression types for CAS VNS calls when there are UVMs on both ends of the call. Only two compression types are supported, however, when there is a UVM on one end and a CVM (or CDP) on the other end. In this case, you can select either a32 and a24. a32 is the default. (When configuring CAS switching, you must select a compression type supported by all the cards, that is UNI ports, in the VNS WAN switching network.)
- CAS Type: 1 to 32. 1 for AB bit signaling on a T1 line, the default.
- CCS Type: 1 to 4. 1 for Q.SIG, the default, the only supported protocol in VNS CAS release 2.2.
- Country code: 0 to 0xFF. 0 for US, the default.
- Interdigit TO: 0 to 0xFF. Interdigit timeout in (50 ms step); 05 is the default for 250 ms.
- Tone level: 0 to 0xFF. DTMF tone dB level below 0 dB; 00 for 0 dBm.
- DTMF duration: 0 to 0xFF. DTMF tone on/off duration in 5 ms step; the default is 0C for 60 ms On and 60 ms Off.
- Idle pattern: 0 to 0xFF. Data pattern for idle channel; the default is 7F for a T1 line.
- Parm (6 to 18): 0x00 to 0xFF. These parameters are put in the command for future enhancement. They have no meaning for VNS CAS Release 2.2. The only validation on these parameters is the range of 0 to 0xFF. The defaults are all 00.

Step 4 Use the VNS Configuration Interface to configure Voice Network Switching. The VNS Configuration Interface is described in Chapter 7. CAS-to-QSIG configuration is almost transparent to the VNS. For CAS switching, you must set the following parameters:

- On the VNS Information menu, the compression type field must be set to either a24 (1) or a32 (2); the SPNNI type must be set to QSIG (2).
- On the Cards Information menu, the Card Type field is set to 1 (CDP or CVM).
- On the Port Information menu the UNI channel must be set to 25 (the pseudo DS0 25); the First Channel and Last Channel fields will only go through a range of 1-24, for a T1 line; the Stack Type field must be QSIG (2).
- On the Port Information menu, set the Channel Alloc Role to 2 (side B, slave or user). (The UVM always performs side A, master or network, role of this protocol.)

Note There are no VNS Configuration Interface parameters that specify CAS.

Related IGX Switch Commands

In addition to **cnfcassw** (configure CAS switching), other IGX commands that relate to CAS-to-QSIG conversion are:

- **dspcd** (display card)
- **cnfchutl/dspchcnf** (configure channel utilization/display channel configuration)
- **cnfcl/dspclncnf** (configure line/display circuit line configuration)

IGX commands are fully documented in the *Cisco WAN Switching Command Reference* for Release 8.5.

dspcd

The IGX display card (**dspcd**) for Release 8.5 will indicate in CAS switching is supported on the UVM card. The following example screen shows a UVM which supporting CAS switching:

```
vnsigx8        TN    StrataCom       IGX 16    8.5.B0    Sep. 16 1997 00:01 PST

Detailed Card Display for UVM in slot 8

Status:          Active                (Front Card Supports CAS-switching)
Revision:        BC05
Serial Number:   336840
Integrated Echo Canceller
  Channels:      24
Backplane Installed
Backcard Installed
  Type:          T1-2
  Revision:      AB
  Serial Number: 289389




Last Command: dspcd 8


Next Command:
```

cnfchutl/dspchcnf

The configure channel utilization (**cnfchutl**) command for Release 8.5 permits the configuration of the CCS signaling channel (that is, the pseudo DS0 25) between the UVM and the VNS. This DSO 25 is not part of the T1 interface between the CAS PBX and the IGX UVM. The **cnfchutl** screen display is the same as the **dspchcnf**, shown in the example below. This example shows the configuration of connection vnsigx8.8.1.25. For a standard T1 interface, without the CAS-to-QSIG conversion on the UVM, slot.line.25 would not be configurable.

```
vnsigx8        TN    StrataCom       IGX 16    8.5.B0    Sep. 16 1997 00:03 PST

From       %   Adaptive          Gain (dB)  Dial   Interface       OnHk    Cond
8.1.25    Util Voice      Fax    In  Out    Type   Type         A  B  C  D Crit
8.1.25     40  Enabled  Disabled  0    0   Inband  Unconfig     ?  ?  -  -  a
8.2.25     40  Enabled  Disabled  0    0   Inband  Unconfig     ?  ?  -  -  a










Last Command: dspchcnf 8.1.25


Next Command:
```

cnfln/dspclncnf

In Release 8.5, the configure line command (**cnfln**) permits the setting of µ–law (Mu-law) for encoding the T1 line. It also displays the status of CAS switching. The dsplncnf command shows whether these parameters have been configured. The following example screen illustrates a T1 circuit line with µ-law encoding and CAS switching turned on. CAS-Switching with PBX-END indicates that CAS switching was turned on with the **cnfcassw** command.

```
vnsigx8        TN    StrataCom       IGX 16    8.5.B0    Sep. 16 1997 00:04 PST

LN   8.1 Config      T1/24                 UVM slot: 8
Loop clock:          No

Line framing:        ESF                        cnfg:            External
     coding:         B8ZS                           slot.line:  --
     CRC:            --                         CAS-Switching:   PBX-END
     recv impedance: --
  E1/J1 signaling:  --
     encoding:       u-LAW
     T1 signaling:  ABAB
     cable type:     ABAM
     length:         0-133 ft.
     56KBS Bit Pos:  msb
     pct fast modem: 20


Last Command: dspclncnf 8.1


Next Command:
```