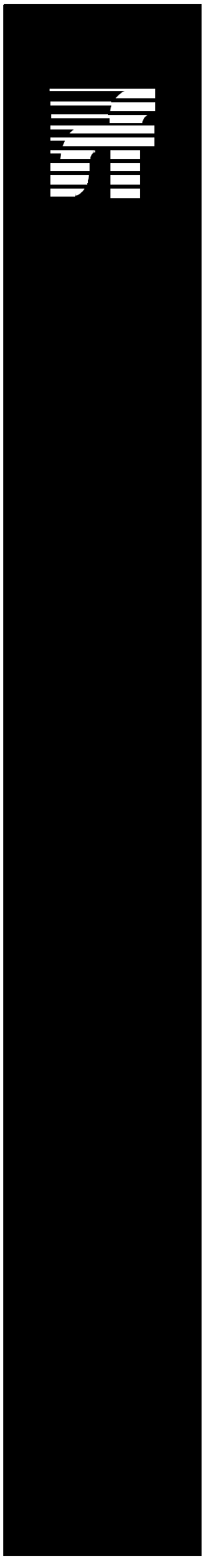


Summa Four

Generic V4.0 FSR02 PUN 22
Release Notes

61220300240-0DR

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference when this equipment is operated in a commercial environment. This equipment generated, used, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manuals, may cause interference in which case the user will be required to correct the interference at his/her own expense.

NOTICE: Customers connecting this device to the network shall, upon request of the telephone company, inform the telephone company of the particular lines such connections are made, the FCC registration number, and ringer equivalence number of this device. This information is contained on the label located on the rear panel of the system.

If this device causes harm to the network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. But if advance notice isn't practical, you will be notified as soon as possible. You will be advised of your right to file a complaint with the FCC.

Your telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the proper operation of your equipment. If they do, you will be notified in advance to give you the opportunity to maintain uninterrupted service.

If you experience trouble with the Summa Four switch, please contact Summa Four, Inc., 25 Sundial Avenue, Manchester, NH 03103-7251, 1-(800)-978-6624 for repair information. The telephone company may ask you to disconnect this equipment from the network until the problem has been corrected, or you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

61220300240-0DR

Released: 06.04.97

Revised: 09.19.97

Summa Four, Inc. reserves the right to change specifications without prior notice.

For further information about this product, contact:

Summa Four Inc.

25 Sundial Avenue

Manchester, NH 03103-7251

(603) 625-4050

Printed In U.S.A.

This symbol on the product's nameplate means it has been tested by Electronic Testing Labs, Inc.

Table Of Contents

SECTION 1 – CONTENTS OF THE RELEASE

Table Of Contents

Table Of Contents

Table Of Contents

Table Of Contents

Table Of Contents

Table Of Contents

List of Figures

List of Tables

PREFACE

These release notes provide important information about the Generic software, V4.0 FSR02. Readers of this document should be familiar with the system features and operation.

These release notes are organized as follows:

Section 1—Introduces Generic V4.0 FSR02 PUN 22 and describes enhancements and new features, as well as problems that have been corrected.

Section 2—Describes the system requirements.

Section 3—Contains the installation procedures for upgrading systems running V3.3 FSR03 or later and systems running V4.0 FSR00 or later.

Section 4—Lists known design constraints and where applicable, resolutions for these constraints.

Section 5—Lists known functional constraints and where applicable, resolutions for these constraints.

Appendix A—Provides instructions for removing and replacing firmware PROMS and PLDs, if necessary.

Appendix B—Provides instructions for installing V4.0 FSR02 on a new system.

Appendix C—Provides instructions for setting up the SNMPTALK program so you can run some simple SNMP tests on the system.

Appendix D—Provides instructions for database card configuration.

Section 1
CONTENTS OF THE RELEASE

1.1 INTRODUCTION

Generic V4.0 FSR02 is the system software for all SDS and VCO Series systems. Upgrade kits for V4.0 FSR02 PUN 22 consist of the following components:

> *Note: Before upgrading from a previous Generic version, review Section 3 for important information.*

- Software Generic V4.0 FSR02 PUN 22 diskettes (4) that contain Generic V4.0 FSR02 files. See *Appendix B* for information on installing generic software on new systems. Refer to Section 3 if you are upgrading to V4.0 FSR02 from an earlier release.
- For V4.0 Systems: V4.0 FSR02 Change Page Documentation Set for V4.0 FSR00 and FSR01 systems.
  or
  For V3.3 Systems: the V4.0 Documentation Set (may be shipped prior to system shipment) plus the V4.0 FSR02 Change Page Documentation.
- PROMs for the CPU, NBC-3, E1-CAS/R2 (No CRC4), E1-PRI, PRI, PRI/N, NTTPRI, NET5, 4xT1, 4xE1, and 340CPU cards. Customers who already have these cards need to update them by replacing the PROMs.
- For systems shipped with the Ethernet option: A Software Supplemental V4.0 FSR02 diskette that contains the Simple Network Management Protocol (SNMP) and the Summa Four, Inc. Enterprise Management Information Base (MIB) files. Install this disk on external workstations or PCs that are to be used as SNMP managers. The files on this disk are not to be loaded on SDS or VCO systems.

If any of the required diskettes or technical publications are not in this package, contact Summa Four, Inc. Technical Support at 1-800-9SUMMA4.

New systems shipped with V4.0 FSR02 software have all generic and download files installed on the system hard disk. If you are upgrading to V4.0 FSR02, you must install all files from the four V4.0 FSR02 diskettes onto the hard disk as part of the overall upgrade steps outlined in *Section 3*.

> *NOTE: Applications using new features developed for Generic V4.0 FSR02 may not run on systems running previous versions of Generic software. Applications written for V3.x are forward compatible and will run on systems running Generic V4.0 FSR02.*

1.2 ENHANCEMENTS IN GENERIC V4.0 FSR02 PUN 22

Generic Version 4.0 FSR02 contains the following enhancements and is compatible with V3.3 FSR05.

- Support for Japanese ISDN option (NTTPRI) (*Section 1.3*)
- Support for ISDN NET5 Overlap Sending and Receiving (*Section 1.4*)
- Host Link Failure Processing Extensions; Host Port Control Command Extensions (*Section 1.5*)
- All Ports Deactivated Alarm for PRI/N (*Section 1.6*)
- ISDN Conference with Concurrent CPA/ISDN Supervision (*Section 1.7*)
- Enhanced ISDN Port Change of State ($EA) Report Generation (*Section 1.8*)
- On-line Ethernet/NFS Parameters Configuration (*Section 1.9*)
- Configurable IP Subnet Mask (*Section 1.10*)
- Card Status Command and Report ($82) (*Section 1.11*)
- Port Status Command and Report ($83) (*Section 1.12*)
- Host Failure Detection (*Section 1.13*)

The following sections cover each of these enhancements.

1.3 Japanese ISDN

1.3.1 Overview

Japanese ISDN provides the SDS/VCO Integrated Services Digital Network Primary Rate Interface for the Nippon Telegraph and Telephone network. It emphasizes additional functionality for NTTPRI.

Japanese ISDN is based on the PRI/N card re-defined as the NTTPRI card type with the addition of new firmware. It is installed from its own installation diskettes.

For additional information, refer to the *Japanese ISDN Supplement* 61230200440.

1.3.2 Summary of Features

- NTTPRI provides call processing and administrative support for ISDN PRI calls. User Side JATE Symmetrical, CCITT Q.921/931 access to the NTT ISDN network is configurable for each PRI/N card in the system.
- Each PRI/N card provides 23 bearer-channels (B-channels) and a single D-channel for transmission of ISDN control messages (23 B+D). Users may select D3/D4 or Extended Superframe (ESF) format on a per card basis, with B8ZS bit encoding. The D-channel is not inverted.

- The PRI/N card can be inserted in any available Port Subrack slot. Physical interface to the card is accomplished via the PRI/T1 Adapter. This is the same adapter currently used to support connection to the T1 card.
- PRI/N card operation supports the Physical, Data Link, and Network Layers (1, 2, and 3) of the Open System Interconnect (OSI) model to provide interface with ISDN D-channel protocols. Application software, stored on the system hard disk, is downloaded to the PRI/N card by the generic software. This application interacts with the call processing functions running on the system controller.
- Full system administration support is provided to allow PRI/N card configuration, alarm detection and processing, and card maintenance functions. Enhancements to system call processing allow ISDN features and capabilities to be added to an application with no effect on existing applications. The added commands, reports, and Inpulse/Outpulse Rule tokens conform to existing system standards. ISDN Message Templates and rule processing enhance programmable reporting of ISDN events and facilitate the construction of outgoing D-channel messages. ISDN Supervision Templates enable users to control outgoing ISDN calls. These features support not only pure ISDN calls, but also calls which use a mixture of ISDN and non-ISDN resources. All internal resources are available for use by ISDN calls, including the Call Progress Analyzers (CPAs). These mixed-resource cases, called *interworking* scenarios, allow the system to act as a gateway between the ISDN and traditional services networks.

1.4 ISDN NET5 OVERLAP SENDING AND RECEIVING

ISDN NET5 Overlap Receiving was supported in V4.0 FSR02. Support for Overlap Sending is being added with V4.0 FSR02 PUN 22. This section describes Overlap Sending and Receiving as it exists in V4.1.

In earlier versions of NET5, the overlap function was implemented at the card level; the card would pass a SETUP with all called digits after it received a message that included information indicating that receiving was complete. In this release, the host has control of digit collection and time-outs for both sending and receiving.

In Overlap Receiving, when a SETUP is received, it is passed to the host. The host responds with the SETUP ACK message. If all digits are not received, the network passes additional digits in INFORMATION messages and the host determines when all the digits have been received. When it is determined that all digits have been received, the host then sends the CALL PROCEEDING message.

In Overlap Sending, the host has control of digit assembly and transmission. When a SETUP is sent, it is passed to the destination. The destination responds with a SETUP_ACK message, and the SDS/VCO enters the Outgoing Call Processing state.

1.4.1 Summary of Features

Generic support of ISDN Overlap Sending and Receiving includes the following:

- ON/OFF selection of Overlap Sending/Receiving feature via console
- SETUP and SETUP_ACK support for Overlap Sending/Receiving
- Multiple INFORMATION message support for Overlap Sending/Receiving
- New ISDN state I_OVRL support for Overlap Receiving and O_OVRL for Overlap Sending
- Host timer expiry support for Overlap Receiving

1.4.2 Features Not Supported

- $49 command with detach control for call clearing (aborting) on Overlap Receiving

1.4.3 User Interface—Overlap Receiving ON/OFF Control

The feature is configurable from the System Features screen. Selection enables both sending and receiving. See Figure 1.1.

When you enable the feature (set it to Y), the host has control of digit collection and time-outs, and acceptance of variable, unpredictable digit length is supported. The host also has control of digit assembly and time-outs, and transmission of variable, unpredictable digit length is supported. When the feature is disabled (set to N), the card hides the overlap function.

The initial default value of the Overlap Processing feature is N. When you change the value, the new value is saved in the database as the new default.

The feature change takes effect only when the NET5 card goes from out-of-service status to active status. Changing the feature value while a NET5 card is active has no effect. The feature flag is sent to the card.

```
                        S Y S T E M   F E A T U R E S

            FEATURES                FEATURES
                        ALLOWED (Y,N)                       ALLOWED (Y,N)
Redundant System                     Y  Send All ISDN Connect Reports     N
Output Periodic Alarm Reports        N  Enable $66 Cmd Host Checking      N
Card/Alarm Status at Init.           N  Cut Thru For Non-ISDN Alerting    N
Manual Intervention For SLIP/OOF     N  Enable 4th Column DTMF            N
Enable Grace Timing on Null Rule     N  Enable AllPortsDeactivated Alrm   N
Disable Card Error Report/Reset      N  $EA Reports on DChannel RESTART   N
Enable Digit Field Reporting         N  Enable NET5 Overlap Receiving     Y
Suppress PSC/Rule Abort Messages     Y
Enable Host Password Check           N
Force Bearer/Lap Activation          N
Enable MFC-R2 Supervised Clear       N
Enable SLIC Guarded Disconnect       N
Enable CPA Monitor Disconnect        N
Revert to Basic Redundancy           N
Send Reports Before Guard Time       Y
Enable ISDN Manual Disconnect        N
```

Figure 1.1: System Features Screen with NET5 Overlap Receiving

1.4.3.1 Overlap Receiving Indication

The new Generic software introduces a new ISDN state of I_OVRL (Incoming, OVeRLap receiving) for a call.

According to the standard (European Telecommunications Standards Institute), an Overlap Receiving situation occurs when a received SETUP message contains one of the following:

- no called number IE
- an incomplete called number
- a called number which the user can't determine to be complete

Since the called number IE is *not* mandatory in SETUP, it is not feasible for the Generic to judge whether a "no called number IE" situation is actually an Overlap Receiving case or a normal case. Since Overlap Receiving operates in a situation where there is a variable digit length for a called number, even when some number(s) do appear in the called number IE, it is not possible for the Generic to determine if the called number is complete.

Only the Host Application can determine if information about the called number is complete, and that the call can be routed to its destination. The Generic depends on the Host Application for an indication of Overlap Receiving occurrence. To do this, the Host Application sends SETUP_ACK down to the Generic through the $49 command with an inpulse rule specified.

Under the inpulse rule, a ISDN Tx template with SETUP_ACK as the message, does the processing. IEs required by the SETUP_ACK are either part of the ISDN template or attached to the $49 command.

1.4.4 Call State Transition

The Generic maintains two call states for a call: Major state and ISDN state. The ISDN state is affected when the Overlap Receiving feature is enabled.

For Overlap Receiving, a new intermediate state of I_OVRL is introduced into the ISDN state. The state transitions occur as follows:

When a SETUP is received by the Generic,

```
Major state: CP_IDLE    --> CP_SETUP (unchanged)
ISDN state: ISDN_IDLE   --> I_CPRSNT (unchanged)
```

When an outgoing SETUP_ACK is sent,

```
ISDN state: I_CPRSNT    --> I_OVRL
```

When the called number is complete and an outgoing CALL PROCEEDING is sent,

```
Major state: CP_SETUP   --> CP_WANS (unchanged)
ISDN state: I_OVRL      --> I_PRCEED
```

When CONNECT is sent and call goes to stable,

```
Major state: CP_WANS    --> CP_STAB (unchanged)
ISDN state: I_PRCEED    --> I_ACTIVE(unchanged)
```

For Overlap Sending, a new intermediate state of O_OVRL is introduced into the ISDN state. The state transitions occur as follows:

When a SETUP is sent by the Generic,

```
Major state: CP_IDLE    --> CP_SETUP (unchanged)
ISDN state: ISDN_IDLE   --> O_INITED (unchanged)
```

When an outgoing SETUP_ACK is sent,

```
ISDN state: O_INITED    --> O_OVRL
```

When the called number is complete and an outgoing CALL PROCEEDING is received,

```
Major state: CP_SETUP   --> CP_WANS (unchanged)
ISDN state: O_OVRL      --> O_PRCEED
```

When CONNECT is received and call goes to stable,

```
Major state: CP_WANS    --> CP_STAB (unchanged)
ISDN state: O_PRCEED    --> O_ACTIVE(unchanged)
```

The supplemental state, displayed on the Port Display screen, is always 0 because it is not used for any ISDN PRI calls.

1.4.5 Call Establishment

The following describes the data flow of a call establishment with and without Overlap Receiving.

1.4.5.1 Overlap Receiving with Indication from Host Application

The host application checks the received SETUP message and judges that the called number is incomplete; at that point, Overlap Receiving occurs.

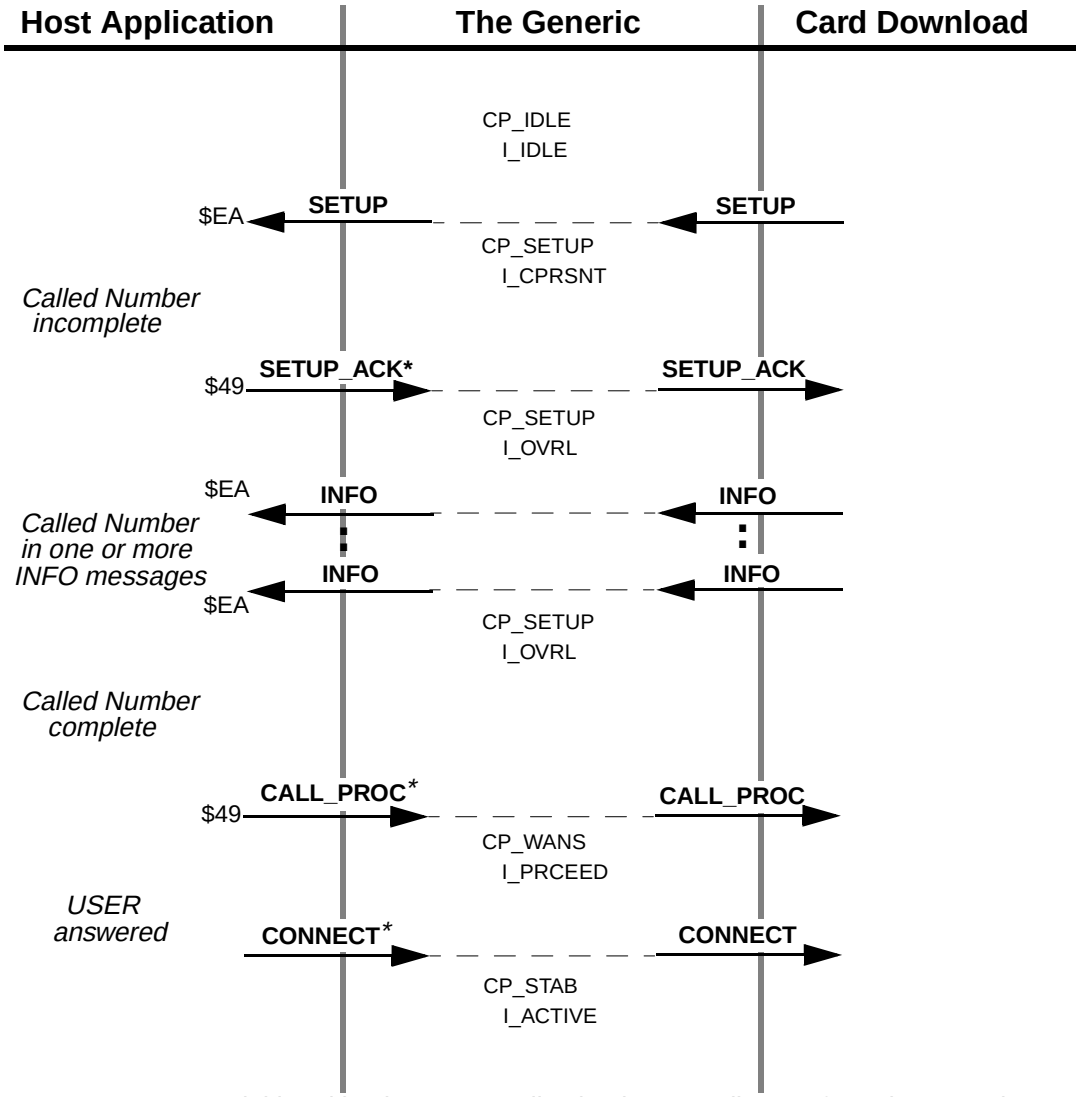
The host application then tells the Generic to send SETUP_ACK to the PRI card.

The outgoing SETUP_ACK serves as an indicator of Overlap Receiving to the Generic. I_OVRL state is entered.

One or more INFORMATION messages are received and passed to the host application until the host application considers the called number to be complete.

The host application then sends CALL_PROC out via the Generic.

The Generic considers this as an indicator of the end of Overlap Receiving; I_PROCEED state is entered. Refer to Figure 1.2.



* Messages are initiated by the Host Application but actually sent from the Generic

Figure 1.2: Overlap Receiving with Indication (SETUP_ACK) from Host Application

Note that in Figure 1.2, the $EA report, not the $ED report, is sent to the Host Application for the SETUP message.

Also note that in those figures, the CONNECT message is sent from the Generic but initiated by the Host Application, and that the $49 command is not necessarily the one that initiates the receiving.

1.4.5.2 Non-Overlap Receiving in Overlap Receiving Operation

It is possible and allowable in Overlap Receiving, for a SETUP message to already include the complete called number, and to not require further INFO messages.

In this case, the Generic does not enter I_OVRL state even if the feature is enabled and SETUP is received. The indicator of Overlap Receiving is never sent from the host application to the Generic.

The host application checks and determines that the call can proceed and sends out CALL_PROC right away.

1.4.5.3 Timer Expiry on Overlap Receiving

The system uses a timer (T302) when in Overlap Receiving to control call clearing (aborting). Refer to Figure 1.3. The timer resides in, and is controlled by, the card download.

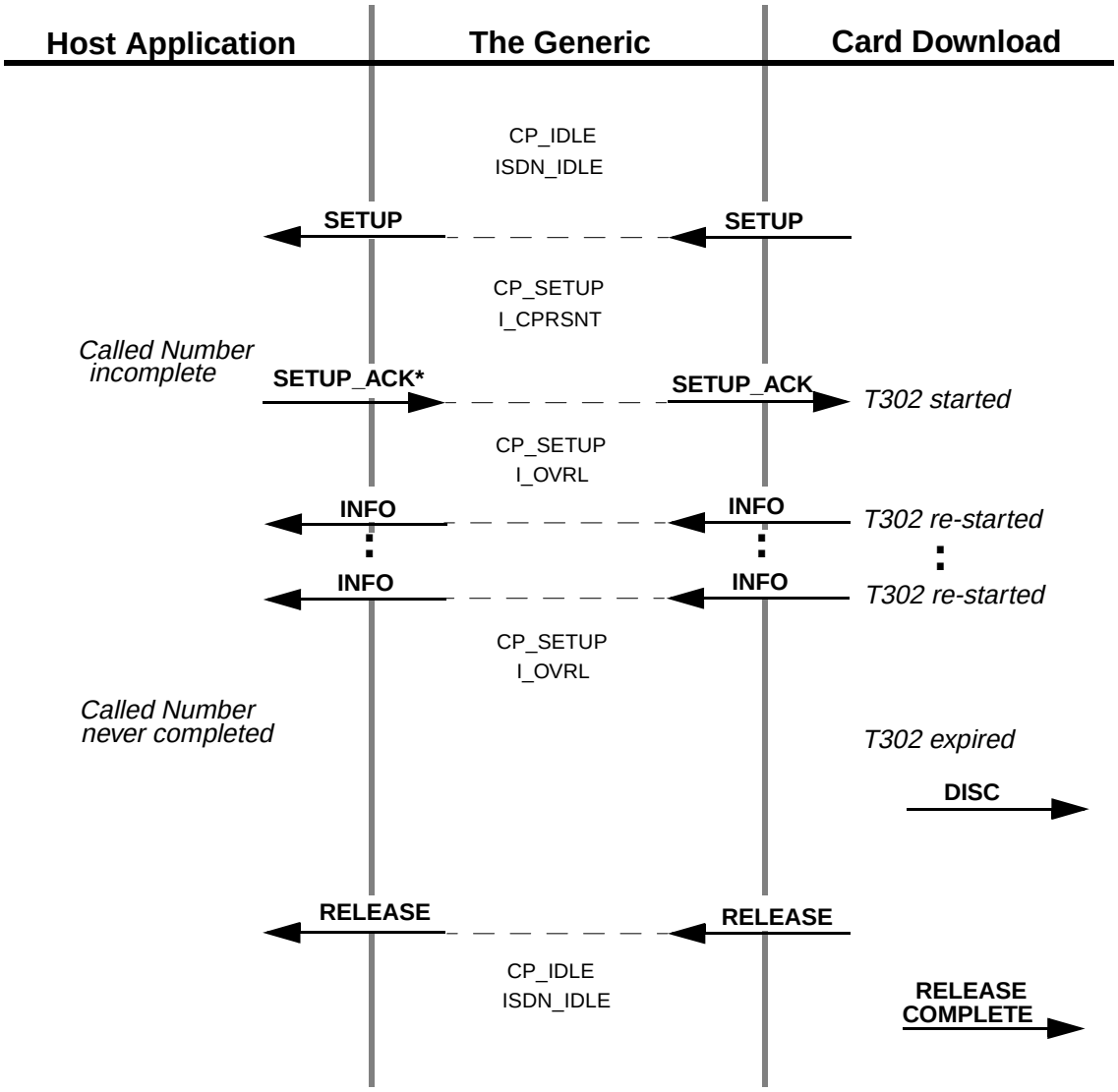
If the host application determines that the called number is incomplete, it initiates SETUP_ACK, Overlap Receiving begins, and the timer (T302) is started. The timer is restarted whenever an INFO message is received by the card download.

The timer is stopped when the card download receives CALL_PROC from the Generic. This occurs when the host application determines that there is sufficient information about the Call Number, or when Receiving Complete Indication is received. At this point, the Overlap Receiving operation ends.

T302 expires in the Overlap Receiving operation if the card download does not receive CALL_PROC within 10 to 15 seconds (the T302 value), and the host application determines that the called number is incomplete.

- Overlap Receiving operation is ended and the card download sends out DISC to the Network. At this point, there is no report of DISC from the card download to the Generic.
- The Network responds to DISC by sending back RELEASE, which is passed to the Generic and the host application.
- Call context at the Generic and the host application is cleared.
- The card download sends out REL_COMPL to the network to complete the call clearing.
- The CAUSE IE with outgoing DISC for this call clearing is #28: Invalid Number Format (incomplete number).

Figure 1.3 shows the T302 expiry and call clearing processing initiated by USER. The first call clearing message is RELEASE from NETWORK.



* Messages are initiated by the Host Application but actually sent from the Generic

Figure 1.3: T302 Expiry and Call Clearing from the Card Download

1.4.5.4 Overlap Sending with Indication from Host Application

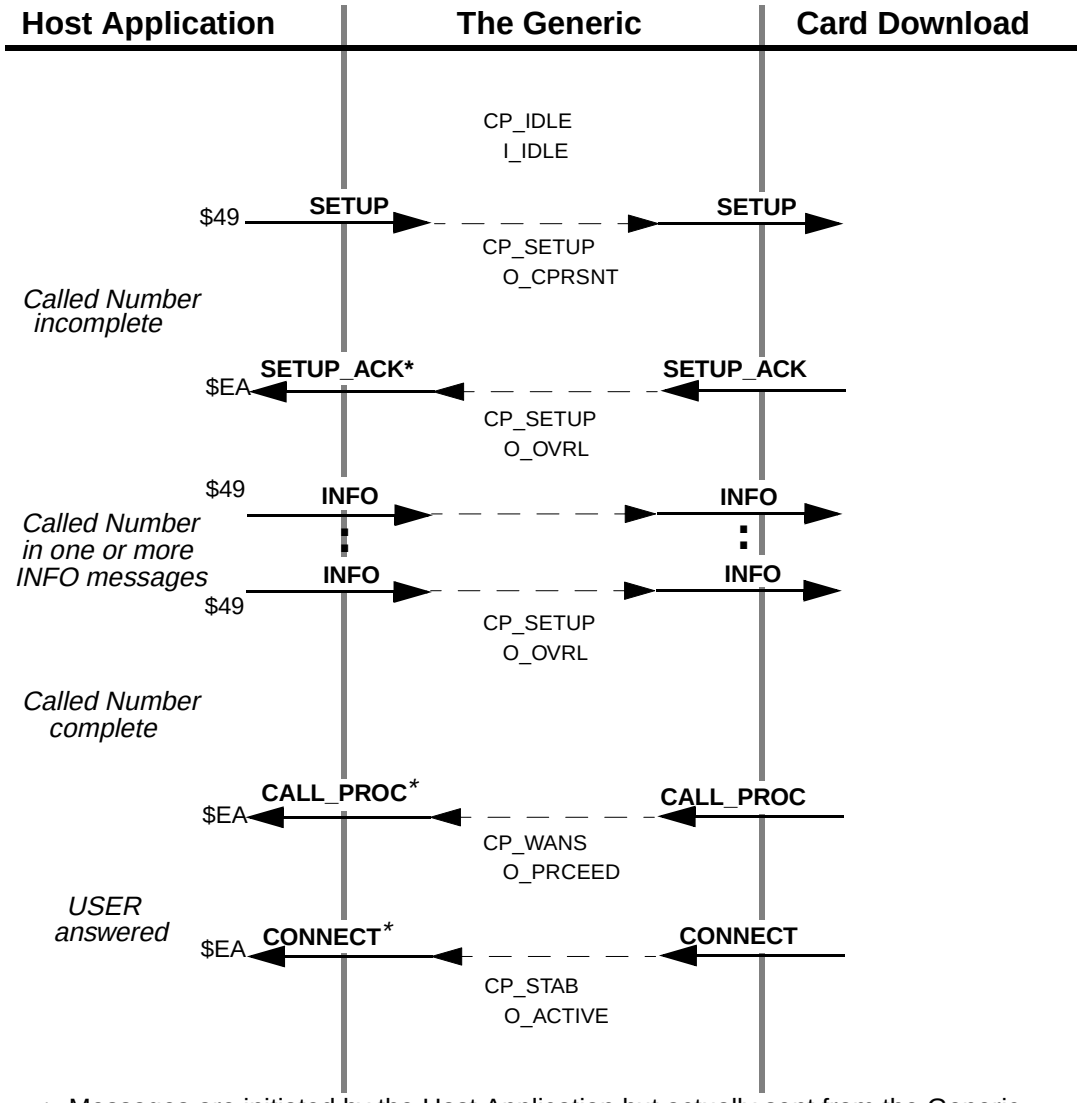
The host application initiates the SETUP message and waits for the acknowledgment.

The incoming SETUP_ACK serves as an indicator of Overlap Receiving to the Generic. O_OVRL state is entered.

The host then transmits the Called Number in one or more INFO messages.

The host application considers the called number to be complete when a $EA CALL_PROC message is received.

The Generic considers this as an indicator of the end of Overlap Sending and O_PROCEED state is entered. Refer to Figure 1.4.



* Messages are initiated by the Host Application but actually sent from the Generic

Figure 1.4: Overlap Sending with Indication (SETUP_ACK) to Host Application

Note that in Figure 1.4, the $49 report, not the $ED report, is sent to the host application for the SETUP message.

Also note that in those figures, the CONNECT message is sent from the Generic but initiated by the host application, and that the $EA command is not necessarily the one that initiates the sending.

1.5 Host Link and Host Control Extensions

1.5.1 Overview

The behavior of Host Link Failure is extended to include conference calls. The Host Assume/Relinquish Port Control command ($C0 05) is extended to include conference calls.

1.5.2 Summary of Features

The Host Link and Host Control extension changes result in the following new characteristics:

- A new system host configuration flag, “Conf Calls in Host Failure Proc,” is provided. The SDS host link failure processing is extended to conference calls, based on this host configuration flag setting.
- When a conference is set up, or ports are added to the conference by a host through the $6D command, the controlling host for all the associated ports is updated.
- The $C0 05 command processing is modified to bring the conference calls into its purview, in addition to the existing port control.
- A port involved in a conference is not relinquished by a host which is controlling that port and the conference, as this would lead to inconsistency of the controlling host maintenance for the conference.

1.5.3 Host Link Failure Processing for Conference Calls

The following subsections provide the details for the host link failure processing extension to conference calls.

1.5.3.1 New Feature Flag: Conference Calls in Host Link Failure Processing

A new feature, Conference Calls in the Host Link Failure Processing, is added to the System Host Configuration screen. Since the flag name display is limited to 32 characters maximum, the flag name is truncated as “Conf Calls in Host Failure Proc” (Figure 1.5). Users set this flag to either INCLUDED or EXCLUDED by pressing the **Select** or **Reverse Select** keys.

The initial setting after installation is EXCLUDED.

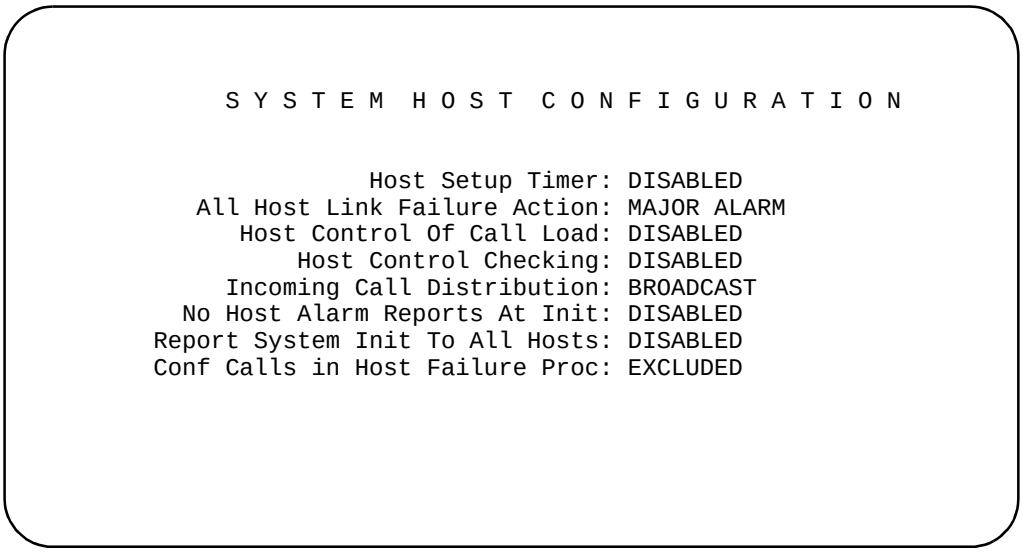


Figure 1.5: System Host Configuration Menu.

When the Conference Calls in Host Link Failure Processing flag is set to INCLUDED, the conference calls are handled on par with other calls, and one of the following occurs:

- The controlling host of the conference call and its associated ports is set to no controlling host.
- The call is cleared.
- No action is taken based on the Failure Action field setting of Clear Cntrl Host or Call Teardown or None in the Host Configuration screen against the failed host.

If you set this flag to EXCLUDED, the conference calls are *not* considered for the host failure processing and all the conference calls' status are maintained as they are.

On redundant systems, the standby side is kept in sync with the active side, via messages sent from the active side.

1.5.4 $6D Command Changes

1.5.4.1 Update Controlling Host for Ports

Prior to this release, the controlling host maintained the conference structure only for conference calls. This maintenance did not extend to the ports involved in the conference. Now, while initiating or adding ports to the conference, the system maintains the ports involved in the conference under the sole control of the host controlling the conference. (See U605070001 in *Section 1.14*.)

1.5.4.2 Port Count Processing

Prior to this release, adding a one-way port to a conference call which already had seven two-way and a one-way port would result in a $03 Syntax Error returned in the status byte. The command now supports port assignments as described in the *Programming Reference*. (See U611210043 in *Section 1.14*.)

1.5.5 $C0 05 Command Processing Extensions for Conference Calls

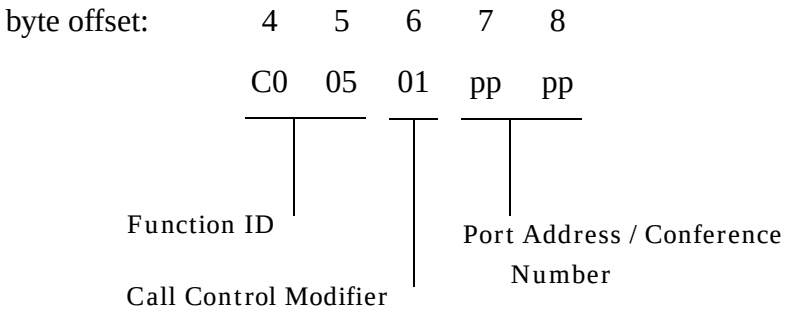
The $C0 05 command is enhanced in this release to support the following. Refer to the descriptions of byte offsets 6, 7, and 8 of the $C0 05 command in this document.

- Assume/Relinquish host control is extended to include conference calls.
- By issuing a single $C0 05 command, a controlling host can relinquish control of all conference calls that were being controlled by it.
- By issuing a single $C0 05 command, a new host can assume control of all conference calls that were being controlled by a particular host id.
- Assuming control of a port by a new host is not allowed if the port is involved in a conference that is controlled by another host, unless the entire conference is taken over by that new host.

See U605070001 in *Section 1.14* for more details.

1.5.5.1 Functional Description

($C0 05) Host Assume/Relinquish Port and Conference Control



Function ID (byte offset 4 & 5) - Bytes immediately following the Network Header; uniquely identifies the command to the system.

Call Control Modifier (byte offset 6) - Determines the type of action to be taken. Specify this byte according to the following list:

00 = Relinquish Port Control

01 = Assume Port Control

02 = Relinquish Conference Control by Conference Number

03 = Assume Conference Control by Conference Number

Port Address/Conference Number (byte offset 7 & 8) - Port Address or Conference ID for which control is being seized or relinquished. A '0000' will be invalid.

If Call Control Modifier is 00/01: byte offset 7 & 8 represent Port Address

If Call Control Modifier is 02/03: byte offset 7 & 8 represent Conference Number

A Call Control Modifier value of 00 (Relinquish Port Control) causes the switch to set the controlling host indicator to "no host" for the specified port and any other associated port. An alternate host can subsequently take control of that port (and any/all associated ports) by sending a command which affects that port.

A Call Control Modifier value of 01 (Assume Port Control) causes the switch to override any existing controlling host indicator for the specified port and any associated ports. The controlling host identifier for these ports is set to the host issuing the command. Assumption of control over a port is therefore equivalent to the aggregate behavior provided by a "relinquish control" command followed by "normal" host command processing which affects that port.

A Call Control Modifier value of 02 (Relinquish Conference Control by Conference Number) causes the switch to set the controlling host indicator to no host for the specified conference number. The controlling host identifier for the conference call as well as for all individual interface ports involved in that conference will also be set to no host. An alternate host can subsequently take control of that conference call (and all associated ports) by sending a command which affects that conference call.

A Call Control Modifier value of 03 (Assume Conference Control by Conference Number) causes the switch to override any existing controlling host indicator for the specified Conference Number. The controlling host identifier for the conference call as well as for all individual interface ports involved in that conference will also be set to the host issuing the command. This command mode helps in load sharing among controlling hosts.

The following table shows the return codes associated with the enhanced $C0 05 command. Refer to the *Programming Reference* manual for more information.

Table 1.1: $C0 05 Command Error Return Codes

Return Code	Description
$03	Syntax error.
$0C	No active conference with conference number specified in command. Indicates the conference number specified in the command does not correspond to any currently active conferences.
$0F	Call or conference is not controlled by this host. Indicates the host port from which this command was received does not correspond to the port controlling the call. This return code is possible only when relinquishing a port or conference call (Call Control Modifier value 00 or 02).
$11	Port in command is idle but should not be. Indicates the circuit identified by the port address specified in the command (usually a controlling port or incoming port) is in the CP_IDLE MState and the command cannot be processed.
$12	Port address in command is not a line or trunk. Indicates the circuit identified by the port address specified in the command is not a network interface circuit.
$1C	Line/trunk port in conference. Indicates the circuit identified by the port address is participating in a conference.

Table 1.1: $C0 05 Command Error Return Codes (Continued)

Return Code	Description
$23	Invalid Port Address or Conference Number specified in command. Indicates the either the port address byte values do not fall within the range $00 00 through $07 FF or conference number is not in the range $0001 to $00FF.
$29	Internal Error — command can not be completed. Indicates an SDS/VCO processing error.

1.5.6 Port Relinquishing Not Allowed While in Conference

Prior to this release, it was possible for an inconsistency to occur between the controlling host of a conference call and the individual ports participating in the conference. This happened when the host relinquished a port while the port was involved in a conference.

Initially, when a conference was controlled by a host, all the ports involved in that conference would also be controlled by the same host. It was possible for the host to issue a $C0 05 command, relinquishing a port, even though the port was still in a conference, provided that the conference was controlled by the same host. The relinquished port's controlling host would then be set to "no controlling host" allowing another host to assume control of that port. At the same time the port was allowed to remain in the conference. The result was a port participating in a conference while being controlled by a host other than the host controlling the conference.

The processing of the $C0 05 command has been modified in this release so a port cannot be relinquished by a host when that port is involved in a conference. An attempt to do so will result in rejection of the command with a returned NSB of $1C.

The $C0 05 command now functions as follows:

1. A port involved in a conference controlled by one host cannot be taken away by another host with the $C005 command.
2. A port involved in a conference controlled by a host cannot be relinquished even by the same host, because this permits the same loss of control.

The system now automatically rejects the $C0 05 command if it is issued to a port which is in conference. This rejection includes the case where a host that is already controlling a port issues a $C0 05 command to assume control of the same port. In this case there is no logical point in processing that command because the port is already under control of the host. An NSB of $1C is also returned in this case.

If a port in conference has to be relinquished by the host, delete the port with a $6D command and then relinquish it with the $C0 05 command.

1.6 All Ports Deactivated Alarm for PRI/N

If you enable this option in the System Features menu, the system generates an alarm when all the ports of a PRI or PRI/N card are deactivated. Refer to Figure 1.6.

```
                        S Y S T E M   F E A T U R E S

            FEATURES                              FEATURES
                         ALLOWED (Y,N)                         ALLOWED (Y,N)
Redundant System                      Y  Send All ISDN Connect Reports     N
Output Periodic Alarm Reports         N  Enable $66 Cmd Host Checking      N
Card/Alarm Status at Init.            N  Cut Thru For Non-ISDN Alerting    N
Manual Intervention For SLIP/OOF      N  Enable 4th Column DTMF            N
Enable Grace Timing on Null Rule      N  Set MVDC-Backplane to A-Law       N
Disable Card Error Report/Reset       N  Enable AllPortsDeactivated Alrm   N
Enable Digit Field Reporting          N  $EA Reports on DChannel RESTART   N
Suppress PSC/Rule Abort Messages      Y  Enable NET5 Overlap Receiving     Y
Enable Host Password Check            N
Force Bearer/Lap Activation           N
Enable MFC-R2 Supervised Clear        N
Enable SLIC Guarded Disconnect        N
Enable CPA Monitor Disconnect         N
Revert to Basic Redundancy            N
Send Reports Before Guard Time        Y
Enable ISDN Manual Disconnect         N
```

Figure 1.6: System Features Menu

Major functionality of this feature includes:

- Alarm report generation when all the ports of a PRI/N card are deactivated
- Generation of alarms for cards in an NFAS group on a per card basis
- Alarm clear report generation when at least one port of PRI/N card becomes available, once the alarm is set
- Notification of alarm condition to the standby-side controller whenever card status is reported
- Clearing of the minor system alarm only when all PRI/N alarms of this type are cleared
- Ability for users to enable or disable the above functionality through a system feature flag.

1.6.1 Functional Description

When all the ports of a PRI/N card are deactivated, a card alarm is raised and the event is logged. An Alarm Condition report ($F0) is sent to the host specifying which card caused the alarm. A Minor system alarm is raised and the event is logged if the system alarm condition does not already exist.

The new alarm is raised only when *all* the ports are deactivated through the Card Maintenance screen, the $90 command from the host, or through a far end port-state transition to “out of service.”

When at least one of the deactivated ports becomes available for use, the card alarm is cleared and the event is logged. An Alarm Condition report ($F0) is generated to the host, specifying the card in which the alarm condition is cleared. The Minor system alarm is cleared and the event is logged, if there are no other occurrences of the same alarm.

For the alarm to clear, a port which has been deactivated must be made available through

- The Card Maintenance screen
- Control from the far end
- The Change Port Status command ($90) from the host

When all the ports of a PRI/N card are deactivated, a card alarm is raised and this event is logged. The message is as follows:

FRM103: All Ports Deactivated - RLS X,X,X (CARD ALARM SET)

An $F0 Alarm Condition report is sent to the host specifying the card in which the alarm condition is detected. Refer to *Section 1.6.2* for a description of the $F0 report.

A Minor system alarm is raised, and this event is logged if the alarm does not already exist. The system issues the following message:

FRM503: Minor Alarm Set For - ALM061: All Ports On Card Deactivated

When at least one port of the card in which the alarm condition exists becomes available, the card alarm is cleared and this event is logged:

FRM104: All Ports No Longer Deactivated - RLS X,X,X (CARD ALARM CLRD)

An $F0 Alarm Condition report is sent to the host specifying the card in which the alarm condition is cleared. The format of the report is given later in this document.

The Minor System Alarm is cleared if no other occurrence of the same alarm exists. The clearing of the alarm is logged. The log message is as follows:

FRM510: Minor Alarm Clear For - ALM061: All Ports On Card Deactivated

You can see the alarm condition on the System Administrator's console through the System Alarm Display option. The alarm message, where *N* is the number of occurrences, is as follows:

ALM061: All Ports On Card Deactivated N

You can also see the alarm condition through Card Alarm Display Option. The alarm message which includes the Rack, Level, Slot of the card is as follows:

R L S All Ports Deactivated

The following additional line appears on the System Feature Configuration screen:

Enable All Ports Deactivated Alarm N

The Enable All Ports Deactivated Alarm feature is disabled by default. If you enable the feature flag, the alarm is raised when such a condition occurs. If users disable the feature flag, the alarm is cleared if already set.

The alarm is cleared, if set, when users delete the card.

The alarm is cleared, if set, when the card moves to OOS, Diagnostics, or Remote Loopback, and is set again if the card moves to the Active state.

The standby-side controller is updated with alarm conditions whenever the card status is reported to the standby side.

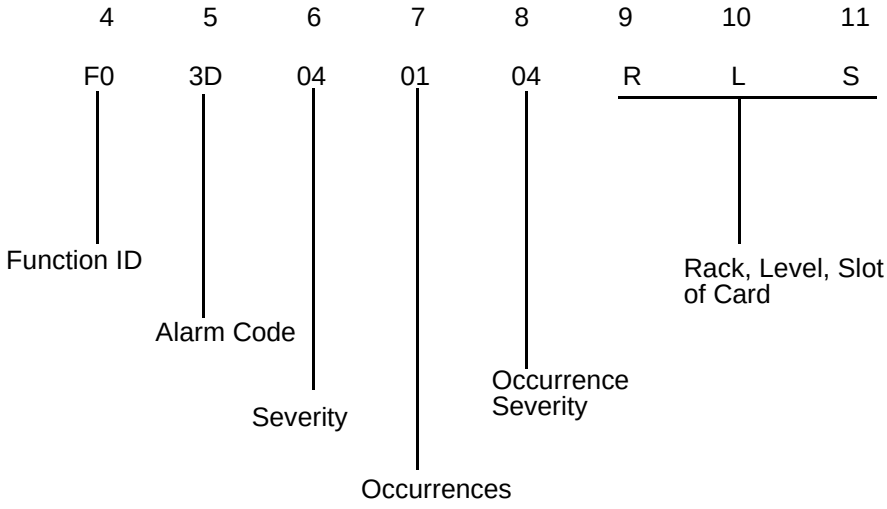
Alarms for cards in an NFAS group are generated for individual cards and are not generated for NFAS groups.

The Display Card Data screen, under the Diagnostics menu, shows the following message if the alarm exists for a particular card:

All Ports Deact

1.6.2 $F0 Report Format

The format of the $F0 Alarm Condition report when the alarm is set or cleared, is as follows:



Function ID (byte offset 4) – Function ID for alarm condition report.

Alarm Code (byte offset 5) – Identifies the alarm being reported. $3D refers to the new All Ports Deactivated alarm report for PRI/N cards.

Severity (byte offset 6) – The severity level for this alarm is Minor. The value for Minor alarm is $04.

Occurrences (byte offset 7) – Indicates the number of alarm occurrences that exist, in hex.

Occurrence Severity (byte offset 8) – Indicates the severity of the occurrence being reported. The byte is $04 when alarm is being raised and is $00 when alarm is being cleared.

Additional Data Bytes (byte offset 9 - 11) – The three bytes refer to the Rack, Level, and Slot respectively, of the card in which the alarm is set or cleared.

1.7 ISDN Conference with Concurrent CPA/ISDN Supervision

This release of the generic contains enhancements which enable the system to monitor Answer Supervision (in-band supervision) concurrent with ISDN supervision during the setup of a conference call. The switch provides audible feedback of the call progress tones, if any, to the caller during the setup of the conference call. This results in the following new capabilities:

- Allowing answer supervision concurrent with ISDN supervision
- Allowing an ISDN PRI port to be added to a conference during supervision processing

The new features are enabled through the addition of the following components:

- New Outpulse Rule token function and new Outpulse Rules
- ISDN Port Addition to Conference

Compatibility with other current applications is maintained.

1.7.1 New Outpulse Rule Token Syntax

ISDN ports use ISDN (D-channel message) signalling, while non-ISDN ports use answer (in-band) supervision. Supervision processing is invoked through Outpulse Rule tokens. Tokens invoke either answer or ISDN supervision on a port. For a description of how the Outpulse Rules function, refer to the *SDS or VCO System Administrator's Guide*, Section 2 (P/N 61210200040).

1.7.1.1 New Tokens/Rules

This section describes the enhancements that support a new Outpulse token definition and new Outpulse Rules. These features provide the function of either answer supervision, ISDN supervision, or both, on an ISDN port.

WAIT SUP — Token Type: *Supervision Control*. This token defines intermediate supervision during Outpulse Rule processing. When the WAIT SUP token is executed, Outpulse Rule processing pauses while Supervision Template processing begins for the template(s) specified by the preceding ANS SUP [xx] and /or ISDN SUP [xx] tokens. If a supervision event is detected that successfully ends template processing, the WAIT SUP token is satisfied and Outpulse Rule processing resumes. If a supervision event is detected that indicates a supervision error or call failure, rule processing is aborted.

FINAL SUP — Token Type: *Supervision Control*. This token defines final supervision after Outpulse Rule processing ends. FINAL SUP tokens function as set-up tokens and can be defined anywhere within a rule. Once Outpulse Rule processing ends, final supervision processing begins for the template(s) specified by the preceding ANS SUP [xx] and/or ISDN SUP [xx] tokens. Final supervision processing continues until a supervision event is detected that ends template processing. Resources attached to the call, such as receivers, are released once Outpulse Rule processing ends. However, if an accompanying ANS SUP template requires call progress tone detection, a CPA port remains allocated to the call.

ANS SUP [xx] — Token Type: *Supervision Control*. The ANS SUP [xx] token functions as a setup token for a subsequent WAIT SUP or FINAL SUP token. When this token is encountered, call processing stores the number of the Answer Supervision Template for later processing. The additional data entry field specifies the supervision template. The value can be a number from 1 to 24, the letter *A* (answer), or the letter *W* (wink).

TIME SUP [xx] — Token Type: *Supervision Control*. TIME SUP [xx] works in conjunction with WAIT SUP and FINAL SUP tokens to perform grace or supervision timing. This token should immediately precede a WAIT SUP or FINAL SUP token in an Outpulse Rule. The additional data entry field of the TIME SUP [xx] token specifies the timer's duration (1 to 60) in seconds. The SDS response to the timer's expiration is indicated by the Answer Supervision Template identified by the accompanying ANS SUP [xx] token. If the timer expires during template processing, the SDS performs the action specified by the condition token in the template's Time event field.

ISDN SUP [xx] — Token Type: *Supervision Control*. The ISDN SUP token specifies which ISDN Supervision Template is used during Outpulse Rule processing. The ISDN SUP [xx] token functions as a setup token for a subsequent WAIT SUP or FINAL SUP token. The additional data field specifies the number of the ISDN Supervision Template to use. Valid values for the additional data field are the numbers from 1 to 24.

Syntax

One new token is added and three existing tokens are redefined. Table 1.2 describes the function of these ISDN tokens.

Table 1.2: Token Functions

Token Name	Current Function	New Function
ANS SUP [xx]	N/A	Sets up the answer supervision template number. This token should precede the related WAIT SUP or FINAL SUP token.
ISDN SUP [xx]	Sets up the ISDN supervision template number. Performs the action of ISDN supervision.	Sets up the ISDN supervision template number. This token should precede the related WAIT SUP or FINAL SUP token.
WAIT SUP	Sets up the answer supervision template number. Performs the action of intermediate answer supervision.	Performs the action of intermediate answer and/or ISDN supervision. Uses the setup(s) of the preceding ANS SUP and/or ISDN SUP tokens.
FINAL SUP	Sets up the answer supervision template number. Sets up the action of final answer supervision. The action occurs at the end of the rule processing. Can be anywhere in Outpulse Rule.	Sets up the action of final answer and/or ISDN supervision. The action occurs at the end of the rule processing. Uses the setup(s) of the preceding ANS SUP and ISDN SUP tokens (subsequent to a WAIT SUP token, if any). Can be anywhere in Outpulse Rule.

With the new token and the new definitions you can define the following call setups.

Table 1.3: Call Setups

Function	Current	New
Intermediate Answer Supervision	WAIT SUP[xx]	ANS SUP [xx] WAIT SUP
Intermediate ISDN Supervision	ISDN SUP [xx]	ISDN SUP [xx] WAIT SUP
Final Answer Supervision	FINAL SUP[xx]	ANS SUP [xx] FINAL SUP
Final ISDN Supervision	N/A	ISDN SUP [xx] FINAL SUP
Concurrent Intermediate Supervision	N/A	ANS SUP [xx] ISDN SUP [xx] WAIT SUP
Concurrent Final Supervision	N/A	ANS SUP [xx] ISDN SUP [xx] FINAL SUP

Concurrent supervision is satisfied when either Answer or ISDN supervision template processing is complete.

Affected Screens

The following two administration screens have Supervision Processing fields. Information indicates what changes have been made on these screens and to related lists of valid values.

- Outpulse Rule Screen — No changes on screen. However, the new token ANS SUP is now in the token list. You can also enter data in the [xx] field of the WAIT SUP and FINAL SUP tokens. This feature is left enabled so you can use the current syntax if necessary.
- Call Progress Tones Monitor Screen — No changes on screen. However, the enhancement enables you to specify an ISDN port number in the RLSP or PA field.

1.7.1.2 SDS Port States

This enhanced version of the generic software supports the addition of an ISDN port to a conference immediately following a SETUP message. To enable this feature, support is now included that allows an ISDN port to enter the CP_WTFSUP state.

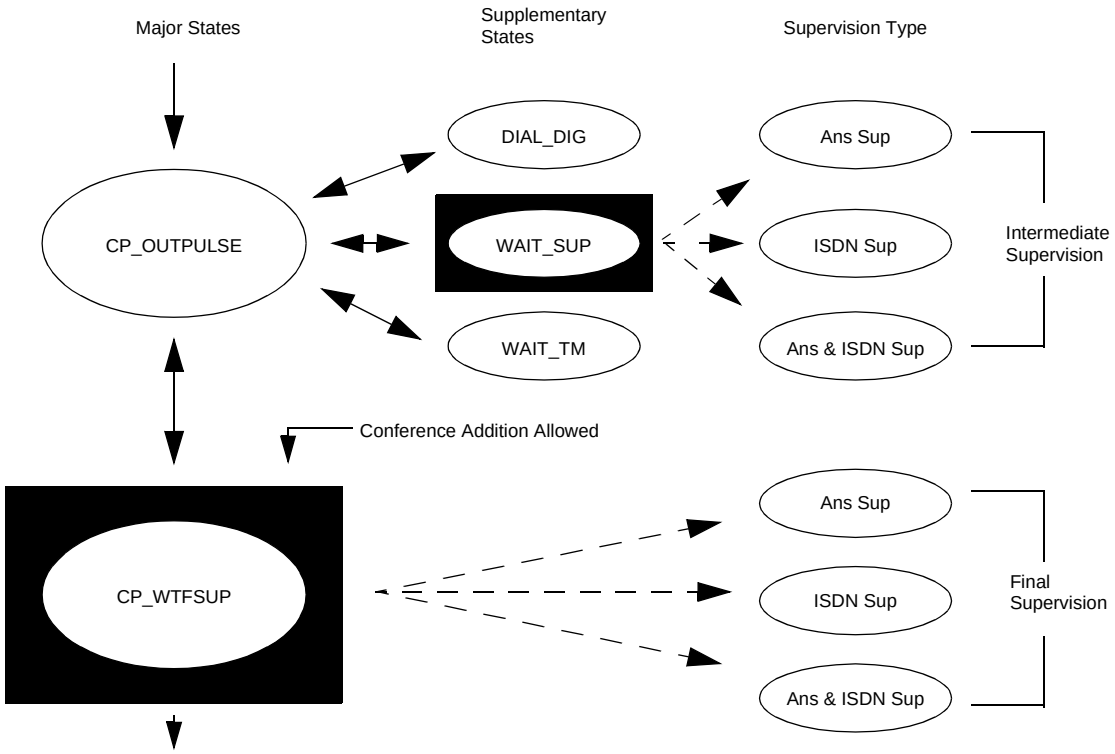


Figure 1.7: Adding an ISDN Port to a Conference Call

In the current version a non-ISDN card has two modes of supervision, each mode corresponding to a specific port state:

Intermediate Supervision — Port has a Major State of CP_OUTPULSE with a Sub-State of WAIT_SUP.

Final Supervision — Port has a Major State of CP_WTFSUP.

The new Outpulse Rules syntax, by allowing you to specify a FINAL SUP token for an ISDN port, enables the ISDN port to enter the CP_WTFSUP state. In the CP_WTFSUP state you can add the ISDN port to a conference. This is consistent with other port types. As a result of this new syntax, the switch can add an ISDN port to a conference immediately after the D-channel SETUP message has been sent.

1.7.1.3 Compatibility

The new support is compatible with other current applications. Compatibility issues are resolved through database conversion software that converts the Outpulse Rules in application databases to the new syntax.

1.7.1.4 Installation Instructions

Follow the instructions for incremental installation (*Section 3*) in these release notes.

When you perform the database conversion in the installation, the software converts Outpulse Rules to the new syntax. This new syntax enables you to specify concurrent supervision.

In some cases (for example, Outpulse Rules that use all or nearly all of the maximum of 16 tokens), the conversion utility displays a message that it could not convert a particular rule. In these cases the remaining rules are converted.

You can leave the unconverted rule(s) in the old syntax if you do not need concurrent supervision for that rule. You can convert the rule manually by using a GOTO RULE token to construct a rule with more than 16 steps. The software will operate properly with Outpulse Rules written in either the old syntax or the new syntax.

Note: Do not mix the old syntax and the new syntax in a rule

It is not necessary to re-install any of the SDS options.

Only the first conversion has any effect on the database. If you inadvertently perform the conversion more than once, the second and any subsequent conversions are ignored.

1.7.1.5 Hardware/Firmware Changes

There are no hardware/firmware changes associated with this enhancement.

1.8 Enhanced $EA Report Generation

Previously, the system did not generate the $EA report for the B-channels when it received a D-channel RESTART. This feature enhancement now generates an ISDN Port Change of State for all the associated B-channels.

1.8.1 Summary of Features

The ISDN Port Change of State Report is reported to the host when a D-channel RESTART message is received through a PRI interface. This enhancement adds the generation of ISDN Port Change of State reports for B-channels associated with the D-channel.

You control the enhanced reporting feature with the new system feature flag “$EA Reports on D-Channel RESTART.” (Refer to Figure 1.6.) Specify Yes or No to enable or disable the generation of ISDN Port Change of State reports for associated B-channels upon receipt of a D-channel RESTART message. The default value of this feature flag is N.

Major functionality of this feature includes:

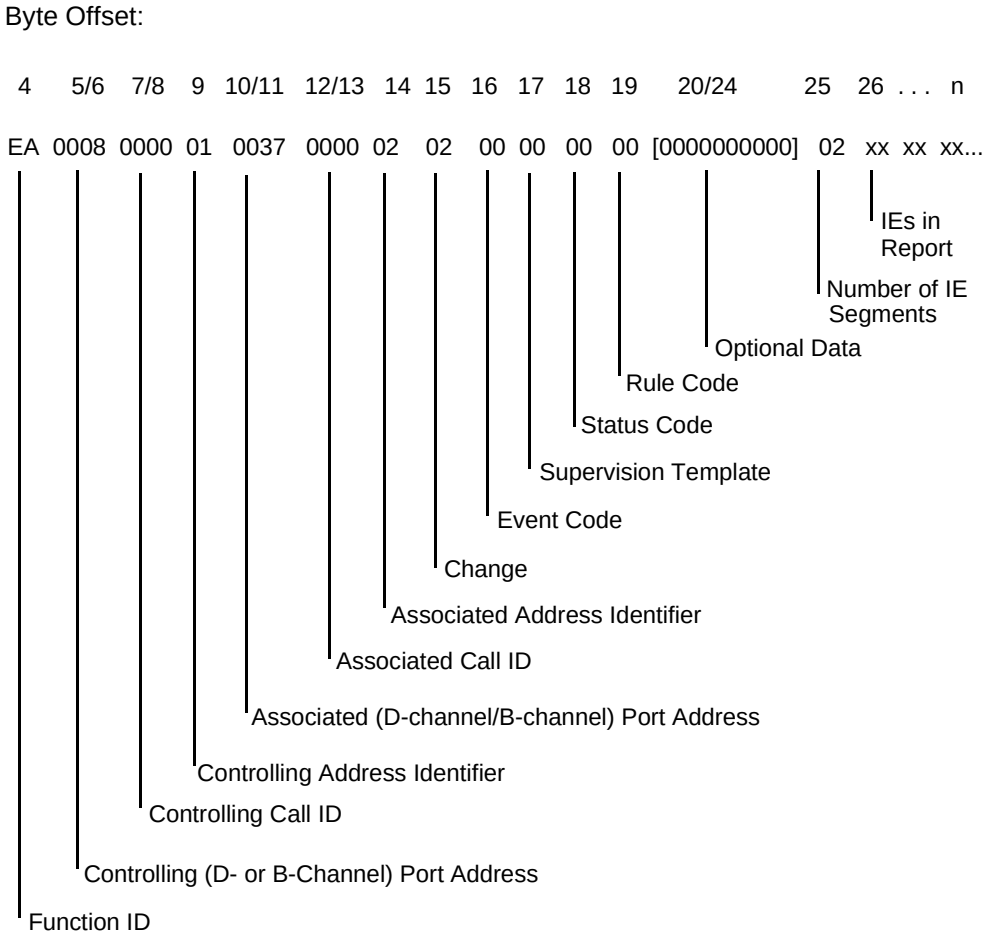
- D-channel RESTART message handling
- Enhanced $EA report generation
- Enhanced System Feature Configuration

1.8.2 Functional Overview

This enhancement generates an ISDN Port Change of State ($EA) report for all the associated B-channels when a D-channel RESTART message is received. The reporting extends to all B-channels in an NFAS group or selected interfaces of the NFAS group, depending on the interfaces specified in the D-channel RESTART message received. Processing of the received RESTART message, and generation of the $EA report for the D-channel itself, are unchanged by this enhancement.

1.8.2.1 $EA Report Format

When a D-channel RESTART message is received, the standard ISDN Port Change of State ($EA) report is generated in the format shown on the next page:



Controlling Port Addr (byte offset 5/6) – Hex representation of the controlling port circuit address for which the report is sent.

Controlling Call Id (byte offset 7/8) – Specifies the ISDN Call ID for the controlling port. Controlling Call ID is 00 00 for non-ISDN port address.

Controlling Addr Identifier (byte offset 9) – Byte indicating the controlling port address (byte offset 5/6) identification.

value 01 — byte offset 5/6 represents B-channel or non-ISDN port address

value 02 — controlling port is specified by D-channel and Call ID

Associated Port Addr (byte offset 10/11) – Hex representation of the associated port circuit address for which the report is sent.

Associated Call ID (byte offset 12 &13) – Specifies the ISDN call id for the associated (outgoing) port. Associated Call ID is 00 00 for non-ISDN port address.

Associated Addr Identifier (byte offset 14) – Byte indicating the associated port addr (byte offset 10/11) identification.

value 00 — indicates no associated port

value 01 — byte offset 10/11 represents B-channel or non-ISDN port address

value 02 — associated port is specified by D-channel and Call ID

Change (byte offset 15) – Specifies the type of change detected.

New value:

02 — port becomes IDLE due to a received D-channel RESTART message

This byte value is "RESERVED" for future enhancements in the existing $EA report.

The received ISDN message is indicated in the Event Code (byte offset 16).

Event Code (byte offset 16) – Specifies the D-channel message received.

46 — RESTART message received

Supervision Template (byte offset 17) – Specifies whether the outgoing port is considered answered (ANS condition token processed in ISDN Supervision Template), and the number of supervision template used.

value 00 — if no supervision template used or call failures occur

Status Code (byte offset 18) – Indicates whether an error was encountered.

01 — no error

8B —D-channel Failure

Rule Code (byte offset 19) – Indicates the number of the OP rule if the change byte (byte offset 15) is 04; else 00.

Optional Data (byte offset 20 -24) – These bytes are reserved for future use.

IE Code (byte offset 25) – Indicates the number of Information Elements (IEs) included in this report.

IEs (byte offset 26 -n) – Indicating IEs if IE code is > 00

Note: No IEs are included in $EA reports generated for B-channels as a result of a D-Channel Restart.

The $EA report is generated and sent to the host in the following cases:

- D-channel RESTART received for a single interface card (if card is not in an NFAS group).

  Reports for all ports except those ports which are Deactivated or in the major state, CP_IDLE.

- D-channel RESTART received for a single interface in an NFAS group.

  Reports for all ports except those which are Deactivated or in the major state, CP_IDLE, if the state of the interface card is Active (A), Maintenance (M), or Camp on Busy (C).

- D-channel RESTART received for the entire NFAS group.

  Reports for all ports except those which are Deactivated or in the major state, CP_IDLE, if the state of the interface card on which the port resides is Active (A), Maintenance (M), or Camp on Busy (C).

The $EA report is not generated for the ports on an interface card in an NFAS group which is in OOS (O), Diagnostics (D), or Remote Diagnostics/Remote Loopback (R) mode.

In addition to reporting the RESTART event to the host, all the calls on the restarted interface B-channels (or the T1 channels in the NFAS group), are torn down. The channels are put back to CP_IDLE state, clearing the call IDs allocated. The CP_IDLE channels in the interface(s) are unaffected.

The calls in progress are torn down and all the resources attached to the call are released. The call IDs allocated are cleared, the rule processing is aborted, and the ports are put back to CP_IDLE.

The ports associated with the call (i.e., ports which are in connection with the call) on the restarted interface, are unlinked and idled, and the standard RELEASE procedure for releasing the ISDN calls is followed.

1.9 On-Line NFS Parameters Configuration

This feature enhancement allows users to reconfigure Ethernet and NFS without having to go through the Ethernet installation procedure.

The new configuration takes effect only after a reboot of the system.

1.9.1 Summary of Features

This feature includes the following functionality:

- On-line Ethernet and NFS configuration
- Message logging of Internet address during boot up and after reconfiguration
- Message logging for Ethernet/NFS parameters reconfiguration
- Access to screen controlled through the Screen Access Configuration screen

1.9.2 Functional Overview

The System Configuration menu is extended to include an option for Ethernet and NFS reconfiguration. The new System Configuration Menu appears as follows:

```
S Y S T E M  C O N F I G U R A T I O N  M E N U


A) Peripheral Configuration
B) File System Configuration
C) Host Configuration
D) Password Configuration
E) Clock/Calendar Configuration
F) System Feature Configuration
G) Screen Access Configuration
H) Software/Firmware Configuration
I) License Configuration
J) System Host Configuration
K) Ethernet/NFS Configuration


              Enter Selection: __
```

Figure 1.8: System Configuration Menu

Previous releases allowed you to view and configure Ethernet and NFS parameters during the installation process only. This enhancement allows you to view and configure the following Ethernet and NFS parameters on-line, through the System Administration console:

- System Internet Address
- NFS Server Internet Address
- NFS Server Name
- NFS Server Mount Directory
- Target System Name
- Target System User ID
- Target System Group ID
- Target System Umask

NOTE: The new Ethernet and NFS parameters will not take effect until you reboot the system.

Ethernet/NFS Configuration will not be allowed if the Ethernet option is not installed. The following error message appears on screen:

Ethernet Option Not Installed

The new Ethernet/NFS Configuration Screen is shown below:

```
                E T H E R N E T / N F S   C O N F I G U R A T I O N


  Current System Internet Address       = 204.160.248.126___

  New System Internet Address On Reboot = 204.160.248.126___
  Enable NFS File Access                = Y
  NFS Server Internet Address           = 204.160.248.81____
  NFS Server Name                       = venus_____________
  NFS Mount Directory Point             =
          /home/server/sds_____________________________
  Target System Name                    = shields___________
  Target System User Id                 = 131_______
  Target System Group Id                = 12________
  Target System Umask                   = 0_

  Gateway Routing Configuration         = _
```

Figure 1.9: Ethernet/NFS Configuration Screen

Current System Internet Address field is display only.

Use the **NEXT FIELD** and **PREV FIELD** keys to navigate between the input fields. Use the **EXIT** and **PREV MENU** keys to cancel the operation and go back to System Configuration Screen. Use the **MAIN MENU** key to cancel the operation and go back to Main Menu. Use the **ENTER** key to terminate inputs.

If you cancel input through **EXIT**, **PREV MENU** or **MAIN MENU**, the following message appears on-screen:

Ethernet/NFS Configuration Aborted

If you press **ENTER**, the following message is shown on-screen to prompt you for your confirmation:

Update Ethernet/NFS Configuration (Y/N)?

If the confirmation is Yes, the entered parameters are stored in NVRAM. The new parameters will take effect only on reboot. The following message is logged, sent to the printer, and shown on screen:

PRM052: Ethernet/NFS Params Updated. Address On Reboot Is A.B.C.D

If the confirmation is No, the following message appears on screen:

Ethernet/NFS Configuration Aborted

Refer to Table 1.4 in this section for the formats and recommended values for the input fields. This table also appears in the *Ethernet Supplement*.

Internet addresses entered are validated when the cursor moves out of the respective fields. If the validation fails, the following message appears on the screen and the cursor is re-positioned on the same field:

Invalid Internet Address

The Enable NFS File Access field accepts characters Y and N only. If you enter any other character in this field, the input is taken as N, and the field is updated with character N when the cursor leaves the field. If you enter numeric characters or non-alpha characters, the following error message appears on screen:

Numeric Key Input Not Allowed

NFS Server Name and Target System Name fields take alphanumeric input. NFS Mount Directory fields takes alphanumeric input as well as special characters such as the slash (/).

Target System User ID and Target System Group ID take decimal input. If you enter alpha characters in these fields, the following message appears on screen:

Alpha Key Input Not Allowed

Target System Umask takes hexadecimal input. The field is validated when the cursor leaves the field and the following message appears on screen in case of error:

Invalid Hexadecimal Input

If you access the Ethernet/NFS Configuration screen again before rebooting, the new parameters will be shown, which can be edited if required.

While booting, the following message appears on screen, showing the current internet address:

System Internet Address Is A.B.C.D

The above message is sent to the printer and logged.

The Ethernet/NFS Configuration screen is added to the Screen Access Configuration screen so that the access level can be controlled. The following line is added to Screen Access Configuration screen:

Ethernet/NFS Configuration 0 __

Standby system's Ethernet option can be reconfigured using the procedure defined above, via the standby side's system console.

The following error message appears on screen when user enters input with leading spaces in any of the fields:

Leading Spaces Not Allowed

Table 1.4: Ethernet/NFS Configuration Requirements

Parameter	Definition	Options	Recommend Value
System Internet Address	Internet address assigned to the SDS that the host uses to control the system	Valid Internet address in standard notation (12.13.14.15)	Value must be supplied by Ethernet administrator
NFS Server Internet Address	Internet address assigned to the device (usually the host computer) on which the Log and Trace file are to be stored	Valid Internet address in standard notation (12.13.14.15)	Value must be supplied by Ethernet administrator
NFS Server Name	Name assigned to the device (usually the host computer) on which the Log and Trace file are to be stored	Valid Ethernet name (alphanumeric)	Value must be supplied by Ethernet administrator
NFS Server Mount Directory	Name of the mount directory device into which the Log and Trace files are to be stored	Valid directory spec. created for SDS Log and Trace files	Value must be supplied by Ethernet administrator
Target System Name	Name assigned to SDS by the Ethernet system administrator	Valid Ethernet Name (alphanumeric)	Value must be supplied by Ethernet administrator
Target System User ID	UNIX user id assigned to the SDS by the Ethernet system administrator	Valid user id in decimal notation	Value must be supplied by Ethernet administrator
Target System Group ID	UNIX group id assigned to the SDS by the Ethernet system administrator	Valid group id in decimal notation	Value must be supplied by Ethernet administrator
Target System Umask	User mask assigned to the SDS by the Ethernet system administrator	Valid user mask in hex notation	Value of “0” unless used on LAN

1.10 CONFIGURABLE IP SUBNET MASK

Previously, SDS/VCO systems supported only class C subnets. Class A and B subnets are now also supported.

1.10.1 Summary of Features

With this release, you can:

- configure the subnet mask from the on-line Ethernet/NFS Configuration menu or from the Ethernet installation disk
- reboot the system after changing the subnet mask in order for the new value to take effect

1.10.2 User Interface

For on-line configuration of the subnet mask, the Ethernet/NFS menu has changed. A new System Subnet Mask field has been added for specification of the desired subnet mask. See *Figure 1.10*.

```
                E T H E R N E T / N F S   C O N F I G U R A T I O N


Current System Internet Address       = 204.160.248.126___

New System Internet Address On Reboot = 204.160.248.126___
Enable NFS File Access                = Y
NFS Server Internet Address           = 204.160.248.81____
NFS Server Name                       = venus_____________
NFS Mount Directory Point             =
        /home/server/sds_____________________________________
Target System Name                    = shields___________
Target System User Id                 = 131_________
Target System Group Id                = 12__________
Target System Umask                   = 0_
System Subnet Mask                    = 255.255.255.0_____

Gateway Routing Configuration         = _
```

Figure 1.10: Ethernet/NFS Configuration Menu

When Ethernet is initially installed, the system reads the Current System Internet Address and supplies a default value for Class A, B, or C subnets in the System Subnet Mask field. If you want to change the class after the initial installation, type one of the values shown in the table below into the field. If you assign a new class of IP address at some point after the initial installation, you must also type in the appropriate system subnet mask. The system will not automatically reconfigure subnet mask based on your new IP address.

IP Address Class Type	Default Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Section *Section 3* and Appendix *Section B* of this manual reflect the addition of the configurable subnet mask feature.

1.11 Card Status Command and Report ($82)

The Card Status command allows the host to query the status of a particular card or range of cards.

One Card Status report is generated for each of the cards specified in the Card Status command. In the case of a multi-span card, Card Status reports are generated for each of the spans.

1.11.1 Card Status ($82) Command

Command Type: System Status

Description:

Use the Card Status ($82) command to obtain the Card Status ($82) report. You can specify a single card or a range of cards.

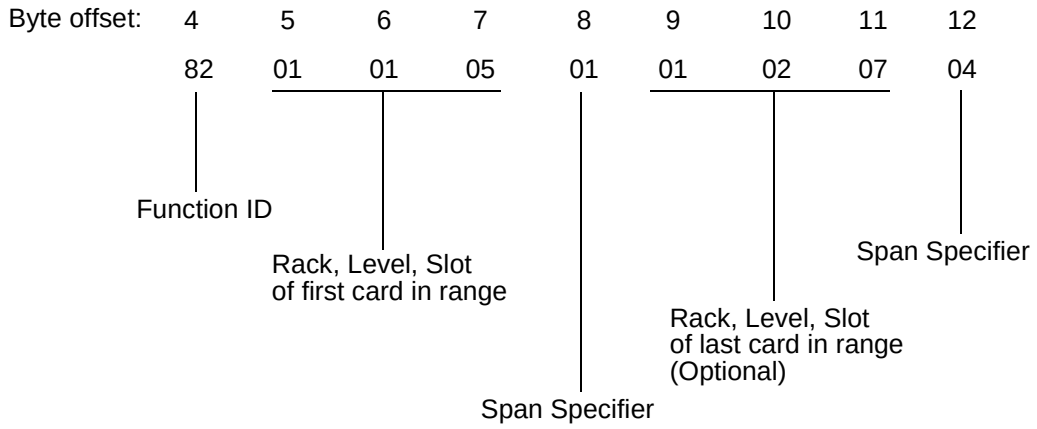
Specify the card by its rack, level, and slot (RLS) position. Specify a range of cards by encoding the starting RLS and ending RLS in the command. One Card Status ($82) report is generated for each of the cards specified in the range. For single cards, the starting RLS and the ending RLS should be the same.

Usage Guidelines:

The Card Status ($82) report takes the form of a command returned with a network status byte set to $01. The report includes the status of the card and the type of the card.

It is recommended that you use the command during periods of low traffic volume because of the communications link and SDS processing overhead.

Format:



Function ID (byte offset 4) – Byte immediately following the Network Header; uniquely identifies the command to the SDS system.

RLS of the first card in range (byte offsets 5, 6, and 7) – Rack, level and slot number of the first card in the range for which the status is requested. These three bytes correspond to the rack, level and slot location of the card, represented in hex. Valid values for rack are 1 or 2; valid values for level are 0 through 3; valid values for slot are from 1 to 21 (i.e., 0 through 15 in hex). Convert the decimal value of the slot into hex for encoding.

Span Specifier (byte offset 8) - Specifies the span number of the first card in the range. Value of zero specifies that the request is for all spans of a multispan card. For a single span card, this value can be either 0 or 1.

RLS of the last card in range (byte offsets 9, 10, and 11) - This is an optional field. Represents the rack, level and slot number of the last card in the range for which the status is requested. These three bytes correspond to the rack, level, and slot location of the card represented in hex. Valid values for rack are 1 or 2; valid values for level are 0 through 3; valid values for slot are 1 to 21 (i.e., 0 through 15 in hex). Convert the decimal value of the slot into hex for encoding.

Span Specifier (byte offset 12) - This is an optional field. Specifies the span number of the last card in the range. Zero specifies that the request is for all spans of a multispan card. For a single span card, this value can be either 0 or 1. If a report is required for a single card, the bytes 9 through 12 are not required in the command.

The rack, level, and slot encoding in bytes 9 through 11must designate a location at the higher end of the range than the rack, level, and slot specified in byte 5. For example, if bytes 5 through 7, specify Rack 1, Level 2, and Slot 1, bytes 9 through 11 can not specify Rack 1, Level 1 and Slot 1; however, Rack 2, Level 0, and Slot 1 would be valid.

If bytes 5, 6, 7, and 8 (first RLS and span), specify Rack 1, Level 2, Slot 1 and Span 0, and bytes 9, 10, 11, and 12 (last RLS and span) specify Rack 2, Level 0, Slot 1 and Span 2, a Card Status ($82) report is generated for all spans of a card at 1,2,1 (if it is a multi-

span card), and for all spans of each of the cards in between, and for spans 1 and 2 of a card at 2,0,1.

If any of the slots falling within the range contains a multi-span card, an $82 report will be generated for each of the spans in the slot.

SDS Response:

One Card Status ($82) report is generated for each of the cards specified in Card Status ($82) command. For any multi-span card, a separate report is generated for each of the spans. If the command is processed without any errors, the $82 report indicates $01 as the network status byte (NSB).

An NSB of INVALID_RLS_CODE ($4A) indicates that the RLS encoding is not valid.

An NSB of INVALID_COMMAND_LENGHTH ($41) indicates invalid command length.

An NSB of INVALID_RLS_RANGE ($52) indicates that the RLS range specified in the command is not valid. This could be because the ending RLS is sequentially lower than the starting RLS.

An NSB of INVALID_SPAN_CODE ($53), indicates that the span specified in the command is invalid. This will be the return code for cases where a single span card status is requested with a span specifier greater than 1, or for a multi-span card with a span specifier greater than 4.

Example:

The following command requests the status of the cards located at 1,1,6 and 1,1, 7:

82 01 01 06 00 01 01 07 02

Function ID = Card Status ($82) command

Starting RLS = 1,1,6

Span specifier = 0

Ending RLS = 1,1,7

Span specifier = 2

Request for all spans of the card at 1,1,6 and for spans 1 and 2 of the card at 1,1,7

1.11.2 Card Status ($82) Report

Report Type: System Status

Destination VCA: Same as Source VCA of command requesting this report

Description:

Informs the host of the status of a card. The card location is represented both by the port address and the physical rack, level, and slot (RLS) address. The report includes the status of the card and the type of the card.

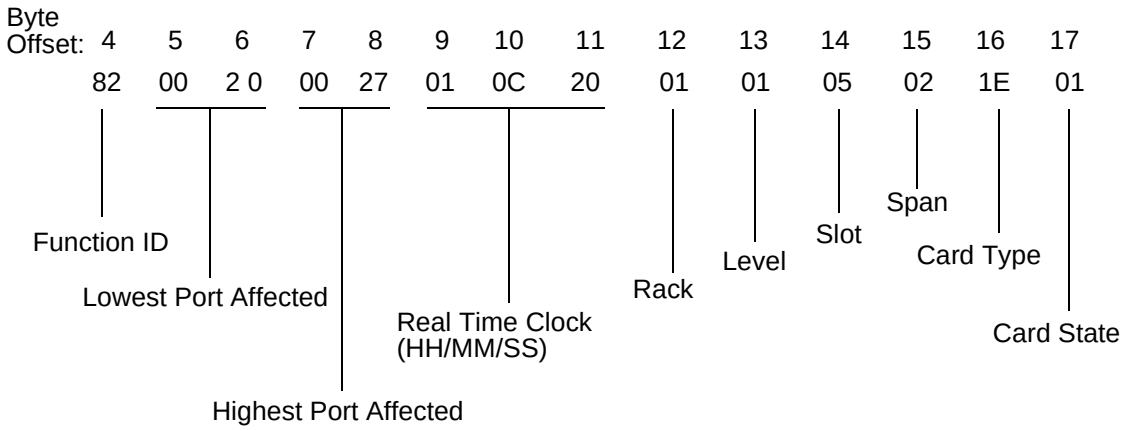
One Card Status ($82) report is generated for each of the cards specified in the Card Status ($82) command. In the case of a multi-span card, an $82 report is generated for each of the spans in the slot.

The Card Status ($82) report takes the form of a command returned with a network status byte set to $01.

Action Causing Report Generation

The system's response to the Card Status ($82) command is a separate Card Status ($82) report for each card specified in the $82 command from the host. In the case of a multi-span card, a separate $82 report is generated for each interface.

Format:



Function ID (byte offset 4) – Byte immediately following the network header; uniquely identifies the report from the system.

Lowest Port Address Affected (byte offset 5 & 6) – Hex representation of the first port address on the card for which the report is sent. This is also useful in identifying the span for which the report is sent in the case of a multi-span card. This field is set to $00 if the card is not found in the database.

Highest Port Address Affected (byte offset 7 & 8) – Hex representation of the last port address on the card for which the report is sent. This is also useful in identifying the span for which the report is sent in the case of a multi-span card. This field is set to $00 if the card is not found in the database.

Real Time Clock (byte offset 9 - 11) – Time represented in the format Hours:Minutes:Seconds; hours, minutes, and seconds are represented separately in hex.

Rack-Level-Slot Code (byte offset 12 - 14) – Specifies the rack, level, and slot in which the card is located. Valid values for rack are 1 or 2, for level, 0 through 3, and for slot, from 1 to 21 (i.e., 0 through 15 in hex).

Convert the decimal value of the slot into hex for encoding.

In the case of a multi-span (4 span E1/T1), if the query has a zero as the span specifier, (representing all four interfaces), there will be four responses, one for each interface. In this case, the Card Status ($82) reports contain the same RLS for all the spans, but the lowest and highest ports affected are differentiated. The span specifier indicates the span for which the report is generated.

Span Code (byte offset 15) – Represents the interface (span) number for a multi-span card, for which the report is generated. The value is 1 for a single-span card status report.

Card Type (byte offset 16) – Type of the card for which the report is generated. This field is set to $00 if the card is not found in the database. The possible values of the field, if the card is present in the database, are shown below:

0x1 Subscriber Line Interface Card (SLIC-2)
0x3 E&M Trunk Card (E&M)
0x4 T-1 Trunk Card (T1)
0x5 Digital Tone Generator (DTG)
0x6 Digital Voice Card (DVC)
0x8 DTMF Receiver Card 8 Port (DRC-8)
0xA MF Receiver Card (MRC)
0xB Direct Inward Dial Card (DID-2)
0xC Universal Trunk Card (UTC-2)
0xD Network Bus Controller (NBC)
0xE Bus Repeater Card (BRC)
0xF Digital Conference Card (DCC)
0x11 Speech Recognition Card (SRC)
0x12 Call Progress Analyzer (CPA)
0x13 Primary Rate Interface (PRI)
0x14 E1 Interface Card (E1)
0x15 MFC-R2 Transceiver Card (MFCR2)
0x16 DTMF Receiver Card 24 Port (DRC-24)
0x17 DTMF Receiver Card 48 Port (DRC-48)
0x18 Integrated Play/Record Card 8 Port (IPRC-64)
0x19 Primary Rate Interface/NFAS (PRI/N)
0x1A DPNSS E1-PRI (DPNSS)
0x1B DASS2 - Network Termination E1-PRI (NTDASS2)
0x1E Four Span T1 Interface Card (4xT1)
0x1F Four Span E1 Interface Card (4xE1)
0x20 Integrated Prompt/Record Card 8 Port (IPRC-8)
0x21 Integrated Prompt/Record Card 128 Port (IPRC-128)

Card State (byte offset 17) - Card states are defined below:

00 card not defined in database
01 active state

02 maintenance state
03 diagnostic state
04 out of service state
05 standby state
06 camp on state
07 card in diagnostics mode with remote loopback
08 card in diagnostics mode with payload loopback
FF unknown state

Example:

The following command requests the status of the cards 1,1,6 and 1,1, 7:

82 01 01 06 00 01 01 07 02

Function ID = Card Status ($82) command

Starting RLS = 1,1,6

Span = all spans

Ending RLS = 1,1,7

Span = spans 1 and 2

The following are the two reports generated for the above command:

First Report:

82 00 20 00 3F 01 0C 20 01 01 06 01 19 01

Function ID = Card Status ($82) report

Lowest Port Affected = $0020

Highest Port Affected = $003F

Real Time Clock = 1:12:32 am ($01 = 1; $0C = 12; $20 = 32)

RLS = 1,1,6

Span = 1 (single span card)

Card Type = $19 (PRI/N card)

Card State = $01 (Active)

Second Report:

82 00 40 00 5F 01 0C 20 01 01 07 01 1F 02

Function ID = Card Status ($82) report

Lowest Port Affected = $0040

Highest Port Affected = $005F

Real Time Clock = 1:12:32 am ($01 = 1; $0C = 12; $20 = 32)

RLS = 1,1,7

Span = 1 (span # 1)

Card Type = $1F (4 span E1 card)

Card State = $02 (Maintenance)

Third Report:

82 00 60 00 7F 01 0C 20 01 01 07 02 1E 02

Function ID = Card Status ($82) report

Lowest Port Affected = $0060

Highest Port Affected = $007F

Real Time Clock = 1:12:32 am ($01 = 1; $0C = 12; $20 = 32)

RLS = 1,1,7

Span = 2 (span # 2)

Card Type = $1E (4 span E1 card)

Card State = $02 (Maintenance)

1.12 Port Status Command and Report ($83)

The new port status command allows the host to query the status of a particular port or a range of ports.

More than one Port Status report is generated for each Port Status command if the status reports of all the ports could not be accommodated in one report.

1.12.1 Port Status ($83) Command

Command Type: System Status

Description:

Use the Port Status ($83) command to obtain the Port Status ($83) report. The command queries the status of a range of ports specified by either a port address range or the rack, level and slot (RLS) encoding of a card, with the specified span or resource group.

In the case of a query for ports in a multi-span card (through RLS specification), you must also specify the span (interface).

Usage Guidelines:

You can specify a range of ports in different ways, depending upon the application. You can get the status of all the ports on a card by specifying the RLS encoding for the card in the command.

You can also get the status of all ports within a port address range by specifying the port address range, which can span cards. If the starting port address and the ending port address are same, the report is generated for that particular port.

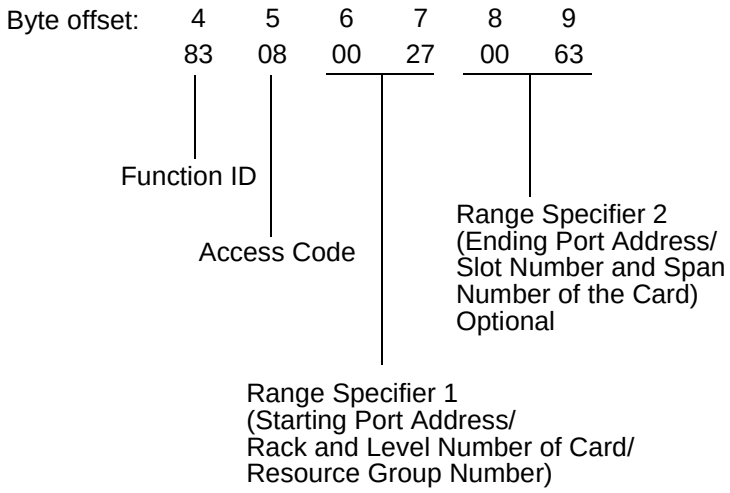
You can get the status of all ports within a resource group by specifying the resource group number.

The Port Status ($83) report takes the form of a command returned with a network status byte (NSB) set to $01. The report contains a series of status report elements; each element contains the port address and its call processing state.

More than one Port Status ($83) report may be generated for one Port Status ($83) command if all the port status report elements could not be accommodated in one report. There is an indicator in such a group of reports, that all these reports are generated for one Port Status ($83) command.

It is recommended that the command be used during periods of low traffic volume because of the communications link and SDS processing overhead.

Format:



Function ID (byte offset 4) – Byte immediately following the network header; uniquely identifies the report from the SDS system.

Access Code (byte offset 5) – A port address range can be specified in different ways. The access code specifies the way in which the port address range is chosen. Construct byte in binary according to the descriptions below, then convert to hex for use in the command.

C000 AGR0

C = always set to 0 in $83 command

Used by $83 report to indicate that there are more fragments of the report

A = 1 if port address range is specified, 0 otherwise

G = 1 if Resource group is specified, 0 otherwise

R = 1 if RLS of card is specified, with or without the span information, 0 otherwise

Range Specifier 1 (byte offset 6 and 7) – Set the field after converting the corresponding values into two bytes, right justified, in hexadecimal.

If bit A in Access Code byte is set, specify the starting port address.

If bit G in Access Code is set, specify the Resource Group number.

If bit R in Access Code is set, specify the rack and level number of the card. These two bytes specify the rack and level in which the card is located.Rack can have a value of 1 or 2; level can have a value of 0 through 3.

Range Specifier 2 (byte offset 8 and 9) – This is an optional field. If bit G is set in the Access Code, this field should not be included in the command.

The field should be set after converting the corresponding values into two bytes, right justified, in hexadecimal.

Specify the ending port address if bit A in the Access Code byte is set.

These two bytes specify the slot number and the span number of the card if the R bit in the Access Code is set. Valid slot numbers are from 1 to 21 (i.e., 0 through 15 in hex); valid span numbers range between 0 and 4.

Convert the decimal value of the slot into hex for encoding.

System response:

The Port Status ($83) report is generated by the system with a NSB set to $01, if the command is processed successfully.

If the port range for which the status report is requested is such that one $83 report can not accommodate all the port status report elements, the report is split into as many $83 reports as necessary.

NSB of OK_MSG ($01) indicates successful processing of command.

NSB of INVALID_ACCESS_CODE ($49) indicates invalid Access Code.

NSB of INVALID_COMMAND_LENGTH ($41) indicates invalid command length.

NSB of INVALID_RLS_CODE ($4A) indicates invalid RLS encoding.

NSB of BADGRP_MSG ($0D) indicates out of range Resource Group number.

NSB of WRGGRP_MSG ($39) indicates undefined Resource Group number.

NSB of BADMAT_MSG ($23) indicates that the port address range specified in the command is not valid. This could also be because the ending port address is less than the starting port address.

NSB of INVALID_SPAN_CODE ($53), indicates that the span specified in the command is invalid. This will be the return code for cases when the port status of a single span card is requested with a span specifier greater than 1, or for a multi-span card with a span specifier greater than 4.

Example:

The following command requests status reports for ports $27 and $28. The command specifies the range through port addresses:

83 08 00 27 00 28

Function ID = $83 - Port Status ($83) command

Access Code = 0000 1000 (C000 AGRS)

C = 0; A = 1 (Address Range specified); G = 0; R = 0;

Staring Port Address = $0027

Ending Port Address = $0028

1.12.2 Port Status ($83) Report

Report Type: System Status

Destination VCA: Same as Source VCA of command requesting this report

Description:

Informs the host of the status of a range of ports. The command, for which the report is generated, forms the leading portion of the report. This leading portion is followed by a series of port status report elements, each of which is three bytes long. The first two bytes specify the port address; the third byte specifies the call processing status of the port.

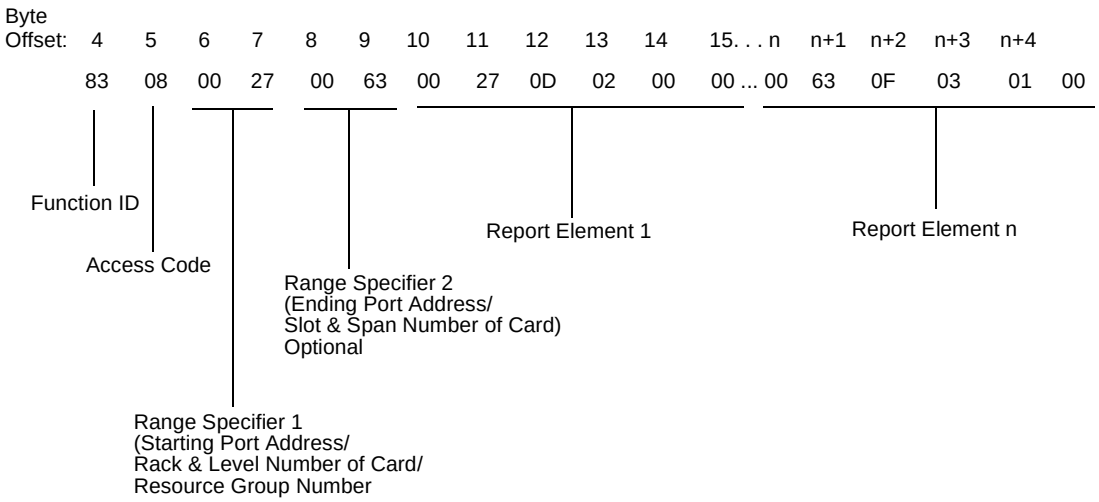
If the port range for which the status report is requested, is such that one $83 report can not accommodate all the port status report elements, the report is split into as many $83 reports as necessary. Such fragments are distinguished from each other through a continuity bit.

Up to 82 port status report elements can be in one Port Status ($83) report, considering that the maximum length of the report is 256 bytes.

Action Causing Report Generation:

The Port Status ($83) command generates the Port Status ($83) report. If the Port Status ($83) command is successfully processed, the network status byte (NSB) is set to $01.

Format:



Function ID (byte offset 4) – Byte immediately following the Network Header; uniquely identifies the report from the system.

Access Code (byte offset 5) – Copied from the Port Status ($83) command for which the report is being generated. Only bit C is modified, if required.

A port address range can be specified in different ways. The access code specifies the way in which the port address range is chosen.

C000 AGR0

C = 1 if this is a fragment of a $83 report in response to a $83 command and more fragments will be sent.

0 if this is the last or only fragment of the $83 report

A = 1 if port address range is specified, 0 otherwise

G = 1 if Resource group is specified, 0 otherwise

R = 1 if RLS of card is specified, with the Span information, 0 otherwise

Range Specifier 1 (byte offset 6 and 7) – Copied from the Port Status ($83) command for which the report is being generated.

Range Specifier 2 (byte offset 8 and 9) – This is an optional field in $83 command. Copied from the Port Status ($83) command for which the report is being generated.

Report Element 1 (byte offset 10 - 14) – If Range Specifier 2 is not present, the first Report Element starts at byte offset 8. This forms the single report element containing the port status report for one port. Other similar report elements follow.

The first two bytes (byte offsets 10 and 11) specify the port address; the third byte (byte offset 12) specifies the call processing state of the port. The following table lists the various call processing states:

CP_IDLE	0
CP_WAIT	1
CP_WWINK	2
CP_DIAL	3
CP_STAB	4
CP_WANS	6
CP_DCON	7
CP_GARD	9
CP_FEXC	0xB
CP_WTIM	0xC
CP_MBUSY	0xD
CP_MFWT	0xE
CP_SETUP	0xF
CP_PRIMARY	0x10
CP_RDR	0x11
CP_MF	0x12
CP_ATT	0x13
CP_DIAG	0x14
CP_DISC	0x15
CP_HOST	0x16
CP_FDIG	0x17
CP_DIG	0x18
CP_INPULSE	0x19
CP_DTMF	0x1A
CP_TALK	0x1B
CP_TONE	0x1C
CP_CONF	0x1D
CP_MON	0x1E
CP_OUTPULSE	0x1F

CP_WTONE	0x20
CP_SPEECH	0x21
CP_SELFTEST	0x22
CP_WTFSUP	0x23
CP_ANALYZE	0x24
CP_RECORD	0x25
CP_CPAMON	0x26
CP_DONECOLLECT	0x27
CP_DELAY	0x28
CP_WAITACK	0x29
CP_OOS	0xFE (If the card containing the port is OOS)
CP_NOTINDB	0xFF (If the card containing the port is not defined in DB)

Byte offset 13 indicates the supplementary state of the port with respect to the major state of the port. The following are the possible values of the supplementary state of a port.

/* REORDER substates */

RDR_FBUSY	0x01
RDR_QUIET	0x02
RDR_DONE	0x04

/* TNK wait substates */

WT_DTMF	0x01
DIALING	0x02
WT_DIAL	0x03
WT_SPC	0x04
WT_ANNC	0x04
WT_BEEP	0x08
SPC_ATT	0x10
WT_TALK	0x10
WT_PSC	0x20

```
                WT_TIM          0x40
                WT_MF           0x80
/* Guard Substates */
                GD_NORMAL       0x00
                GD_WTRLS        0x01
                GD_WTRLSH       0x02
/* Diagnostic/Maintenance Busy substates */
                DIAG_IDLE       0x00
                DIAG_CMAINT     0x01
                DIAG_PATH       0x02
                DIAG_OEND       0x03
                DIAG_AUTO       0x04
                DIAG_INTRN      0x05
                DIAG_TEST       0x06
/* Conference port substates */
                CF_1WAY         0x01
                CF_2WAY         0x02
                CF_SET          0x04
                CF_ACK          0x08
                CF_RSRV         0x10
/* Receiver Enabling Substates  */
                DLY_TIME        0x01
                DLY_WINK        0x04
                DLY_ANS         0x08
                DLY_ANN         0x10
/* Dialing substates */
                D_UNK           0x00
/* Outpulse Rule Substates */
                DIAL_DIG        0x01
                WAIT_SUP        0x02
                WAIT_TM         0x03
```

CARD_OOS_STATE	0xFE (If the card containing the port is OOS)
NOT_INDB_STATE	0xFF (Card containing the port is not defined in DB)

Byte offset 14 indicates the ISDN state of the port. The following are the possible values of the ISDN state of a port.

PT_ACTIVE	0x00
PT_OOS_NE	0x01
PT_OOS_FE	0x02
PT_MAINT_NE	0x03
PT_MAINT_FE	0x04
PT_DCHAN	0x05
PT_OOS_FE_MAINT_NE	0x06
PT_NON_CNTRLD	0xFD (If the card containing the port is not ISDN controlled)
PT_OOS_STATE	0xFE (If the card containing the port is OOS)
PT_NOT_INDB	0xFF (Card containing the port is not defined in DB)

Byte offset 15 indicates the ISDN sub-state of the port. The following are the possible values of the ISDN sub-state of a port.

ISDN_IDLE	0x00
O_INITED	0x01
O_OVRLP	0x02
O_PRCEED	0x03
O_ACTIVE	0x04
O_DELIVRD	0x05
I_CPRSNT	0x0B
I_OVRLP	0x0C
I_PRCEED	0x0D

I_CONNECT	0x0E
I_DELIVRD	0x0F
I_ACTIVE	0x10
DISC_IND	0x14
DISC_REQ	0x15
DISC_RLS	0x16
ISDN_WAIT	0x80
PORT_NON_CNTRLD	0xFD(If the card containing the port is not ISDN controlled)
PORT_OOS	0xFE (If the card containing the port is OOS)
PORT_NOT_INDB	0xFF (Card containing the port is not defined in DB)

Example:

The following command requests status reports for ports $27 and $28. The command specifies the range through port addresses:

83 08 00 27 00 28

Function ID = $83 - Port Status ($83) command

Access Code = 0000 1000 (C000 AGRS)

C = 0; A = 1 (Address Range specified); G = 0; R = 0;

Starting Port Address = $0027

Ending Port Address = $0028

The following report is generated for the above command:

83 08 00 27 00 28 00 27 0D 02 FD FD 00 28 00 00 00 00

Function ID = $83 - Port Status ($83) report

Access Code = 0000 1000 (C000 AGRS)

C = 0 (Only fragment); A = 1 (Address Range specified);

G = 0; R = 0; S = 0;

Starting Port Address = $0027 (Copied from command)

Ending Port Address = $0028 (Copied from command)

Port Address = $0027 (Report Element 1)

Port Status = $0D (CP_MBUSY)

Supplementary State = 02 (DIAG_PATH)

ISDN State = $FD (Not ISDN controlled)

ISDN Sub-state = $FD (Not ISDN controlled)

Port Address = $0028 (Report Element 2)

Port Status = $00 (CP_IDLE)

Supplementary State = 00 (IDLE)

ISDN State = 00 (PT_ACTIVE)

ISDN Sub-state (ISDN Idle)

1.13 HOST FAILURE DETECTION

Prior to this release, if there was an Ethernet link failure and the host did not close the socket properly, the time frame for detection could be two to three minutes for two or more hosts configured for cyclic call distribution. This time frame was unacceptable.

The detection of Ethernet link failure is now done in a reasonable time frame, 6 to 15 seconds, and failure handling can be configured on a host-by-host basis. You can configure the system to do nothing, to tear down calls on a link, or to clear the controlling host. (Refer to the *System Administration Guide* for these existing features.)

1.13.1 Summary of Features

The major functionality in this release includes:

- detection of lost-of-host connection via a probing packet (ping) from the switch over each link
- user-defined time between probes, and number of consecutive failed probes to determine a broken link, on a per-link basis
- automatic closing of the connection, and the generation of alarms when there is a lost connection
- support for the previous one-minute ping frequency scheme

If the consecutive failure count reaches the limit you've specified, the connection is considered to be broken. The switch closes the connection by freeing up all sockets tied to the local ports, and generates alarm messages.

> *Note: The ping mechanism is mandatory for all network devices supporting the Internet suite of protocol. It detects any link failure but does not give much information about the state of the host application software. However, the current Generic contains a feature that deals with host application problems, such as shortage of processing time, host application bug or network congestion. There is a* Host Timer *option in the System Configuration screen that you can enable and for which you specify a time-out period for a call setup. If the host does not respond within the defined period of time, the Generic tears down the call and logs the error condition, but performs no necessary steps to restore the service.*

1.13.2 User Interface

Once the host is configured with *Ethernet* from the Host Configuration Screen, enter the probe frequency and failed probes limit to facilitate this feature. There are two new fields in the Host Configuration Screen. Refer to *Figure 1.11* and note the new fields which are illustrated in bold type.

```
          H O S T  C O N F I G U R A T I O N


Interface   Interval    ___________________
Host Name   Overlay
Trace (1/0) 0



Interface   Ethernet    Connect.Password  _______________ Loc. Port2000
Host Name   Host0       Rem. Inet. Addr   1.2.3.4         Rem. Port2001
Trace (1/0) 1           Failure Action    Call Teardown
Protocol    TCP         Alarm State       On              Ping Freq   6
Reset Time  60          Ping Fail Limit   2

Interface   ___________ ________________  ____________  _________   _____
Host Name   ___________ ________________  ____________  _________   _____
Trace (1/0) __          ________________  ____________  _________   _____
__________  ______      ________________  ____________  _________   _____
__________  ______      ________________  ____________  _________   _____
```

Figure 1.11: Host Configuration Screen

The **Ping Frequency** field defines the time in seconds between probes. The range for this field is 0 to 60. The default for this field is zero (0), which indicates that probing will occur as it did prior to this enhancement—once every minute.

The **Ping Fail Limit** defines the number of consecutive failed probes to determine that a connection is lost. The range for this field is 0 to 10.

The **Ping Fail Limit** default is one (1), if the Ping Frequency is non-zero. (The default of one can be overridden with any value other than zero.) The default is zero (0) if the Ping Frequency is zero. (The default of zero cannot be overridden.) This is the previous once-a-minute probing. Any missing probe will be declared a lost connection.

In the sample screen in *Figure 1.11*, the probe frequency is set to six seconds and the number of failed probes is set to two. This means that the system will probe the remote host every six seconds and the switch will determine that a connection is lost when there is no response from two consecutive probes. This configuration defines a 12-second time frame for failure detection.

To disable the feature, set the **Ping Frequency** to zero. To disable all pinging, set the Remote Internet Address to INADDR_ANY.

1.14 PROBLEMS CORRECTED IN V4.0 FSR02

The following problems have been corrected in V4.0 FSR02.

Note: Bold TR numbers are V4.0 FSR02 issues. The others are V3.x issues included as reference for those who are upgrading from that system.

TR #	Corrected Problems
U307154089	Previously, when only an END CHAR was dialed, it was not displayed in the IFLD. In all other cases, the END CHAR was present at the end of the dialed digits in the IFLD. It now displays correctly.
U602291004	NBC cards can send a packet with a bad checksum to a 4x card. When a bad checksum is received a NACK is supposed to be sent back. Only ACKs were being returned. NACKs are now properly sent in response to a bad checksum.
U605070001	Prior to this release, the controlling host maintained the conference structure only for conference calls and not for the ports involved in the conference. While initiating or adding ports to the conference, the system checked only to verify that the controlling host was set to “no controlling host.” This meant that the port involved in the conference was not under the sole control of the host controlling the conference. Also prior to this release, the $C0 05 host processing command (Host Assume/Relinquish Port Control) supported assuming or relinquishing host control to the ports involved in a call only, and not to conference calls. The command supported only two modes of port control for ports not involved in conference calls: 1) Relinquish Control, and 2) Assume Control. In this release, four modes are added which extend control to ports in conference calls. See *Section 1.5*.
U609230005	Previous to this release, outgoing ports on Single Span T1 cards intermittently became stuck in CP_OUTPUL after incoming seizures.
U609240002	Previously, when there are several simultaneous alarms, only one $F0 Report was sent to the host. All alarms are now sent.
U609300002	Normal operation for a MVDC span going to a T1 OOF maintenance state is for stable ports to go into CP_GARD. Ports should stay in the CP_GARD state until the alarm clears. However, the ports remained in CP_GARD even after the alarm cleared. Card access to the span status has been changed. Operation is now consistent with 4xT1 behavior.

TR #	Corrected Problems
U610160001	The MVDC erroneously reported PRI D-Channel Failure as a failure. This occurred even though the switch did not have either the PRI or PRI/N option installed. The correct alarm is T1 OOF. This was caused by an error string mismatch within alarm look-up. The correct alarm is now displayed.
U610310005 U610310006/ U507215134/ U602260003 TR 5134	In previous releases, the Four Span E1 card did not support broadcast download. This intermittently caused an internal card failure on a span. The 4xE1 card now supports broadcast download the same as 4xT1 card.
U610310007 U610110001	Remote Loss of Carrier Alarm (Yellow Alarm) caused ports to be stuck in CP_GARD. When the Generic received the remote carrier alarm, it assumed the port state to be CP_GARD because that is true for single-span T1 cards. The 4xT1 card has been modified to operate like a single-span card in this respect. Now, after the alarm is generated, the call is torn down, the port goes to CP_GARD, the card generates a guard expired message, and the port goes to CP_IDLE.
U611210002 U306234066 TR 4066	For ISDN calls, the outpulsing of hexadecimal data and 4th column DTMF digits to a T1 was not handled correctly and caused remote alarms on that T1. This has been rectified.
U611210007 U307154087 TR 4087	If an inpulse rule was called out to be executed from an outpulse rule, upon returning to the outpulse rule from the end of the inpulse rule, the voice path was cut over. This occurred regardless of the VV bit settings in the $69 command. Now, the cutting of the voice path will be performed according to the VV bit settings in the $69 command.
U611210010 U501094860 TR 4860	Previously, If users deleted a prompt from the database through the Prompt Library Maintenance screen, and re-downloaded the prompt library files, the deleted prompt still played. This occurred because it was deleted from the hard disk but not from the IPRC's prompt library. Now, the prompt is successfully removed from both places.

TR #	Corrected Problems
U611210013 U504054986 TR 4986	Previously, when a SLIC port was configured with an IP RULE which contained the tokens RETAIN IPR, LIBRARY1, SPEAK 1, SPEAK2, SPEAK3, SPEAK4, or RELEASE IPR, no prompts were played. However, if a WAIT TIME token was placed just before the RELEASE token, the prompts were played. The cause for this problem was that when the generic encountered a RELEASE IPR token in the IP rule, the generic aborted the voice prompts that were being played and released the IPRC port from the call chain. IPRC ports should be released only after the voice prompts are completely played. If there was a WAIT TIME token just before the RELEASE token, the execution of the WAIT TIME token allowed the voice prompts to play and execute the RELEASE token only after the completion of the voice prompts. Now, when there is a RELEASE IPR token immediately after the SPEAK tokens, the voice prompts are played completely, and only then is the IPRC resource released.
U611210014 U504265013 TR 5013	Previously, the RELEASE DTG token could cause an error which generated the following response: “FRM334: Invalid Outpulse Rule Token Identifier -9.” The RELEASE token is now executed properly and no FRM334 message is generated.
U611210016 U505085034 TR 5034	Previously, when a user attempted to place an active DTG in out-of-service state from the administration terminal, the transition would not occur, even when there was a standby DTG in the system. Now, when a standby DTG exists in the system, the active DTG can be taken OOS through the administration terminal.
U611210017 U505265071 TR 5071	Previously, an IPRC could not be attached to a port involved in a conference call, hence no prompts could be played on it. Similarly, MRCs and SRCs could not be attached to a port in conference call. When a $6C, $6E, or $68 command was given to a port in a conference call to attach an IPRC, SRC, or MRC, respectively, it was returned with an error code of $1C. The system now checks for conference calls in $6C, $6E, and $68 command processing, so that IPRCs, SRCs, and MRCs can be attached and used with a port.
U611210018 U507145118 TR 5118	Previously, if a user set the “Return All” option in the $6C (Enhanced) command to allocate an IPRC port from a resource group and play prompts, the returned command did not include the allotted IPRC port address in it. The allotted IPRC port address is now returned with the command.
U611210019 U507215136 TR 5136	An Out Of Service indication (green and yellow LEDs lit) was being given for a PRI/N card that had been taken from an Active to a Maintenance state, then to Diagnostics and back to Active again. The card could be used in a call as normal, but the LEDs were incorrectly showing it to be OOS.

TR #	Corrected Problems
U611210021 U507265148 TR 5148	Previously, an A2 port went off-hook when a user “P’d” it out in the Card Maintenance screen. No indication of the change of state was received when the port was brought back to service. Now, when a port is “P’d” in through the Card Maintenance screen, if the class of service of the port is A2, the major state of the port is set to IDLE and the supplementary state is set to zero. A $D3 report is generated stating the change in service.
U611210023	See *Section 1.14.1*
U611210026 U508185192 TR 5192	An incoming call would come into the switch and be routed through an outgoing trunk port to a far-end port. In this scenario, the incoming port would go on-hook, but the far-end port would remain off-hook, leaving the outgoing port in state CP_DISC. Then, if the host application sent a $69 command to force the outgoing port to idle and generate a $DA, the port could go to CP_IDLE (in the case of a T1 port), but a $DA report was never generated. The solution to this problem is to change the $69 command processing so that, if a $69 command is issued for an outgoing port with a null controlling port, and the outgoing port is in an uncontrollable state (i.e., CP_RDR, CP_DISC, or CP_GUARD major state), the $69 command will be rejected with a network status byte of $26 (“Port Is In An Uncontrollable State”).
U611210031 U508285228 TR 5228	Previously, a scenario occurred where a $69 command was sent to attach two T1 ports, but was rejected with an NSB of $20 (“Outgoing Port Specified In Command Is Not Idle”). This was because the outgoing port was in the CP_DTMF state. However, a subsequent $49 command sent to connect the same two T1 ports was returned with an NSB of $01, even though the ports were not actually connected. The $49 command processing has now been updated to properly return error status codes in the NSB when appropriate.
U611210032 U508285229 TR 5229	A problem was reported in which a $49 command (ISDN Port Control) was issued to connect a T1 OGT (specified as controlling port) to a T1 IDLE port (or ICT, specified as the associated port). In this case, the generic should have interpreted the associated port as being the port of “incoming direction.” However, it did not, and as a result, the IDLE T1 port’s class of service remained as 2 instead of changing to T2. In addition, in this particular case, the controlling port which was an OGT did not have any start and end records allocated to it or the associated IDLE port. Thus, there were no start and end records allocated to this call. Now, when the $49 command specifies the controlling port as an OGT and the associated port as an ICT (or an IDLE port), the class of service of the specified associated port is set to T2 and the start and end records are allocated to it.

TR #	Corrected Problems
U611210033 U509125248 TR 5248	A $69 command was issued to remove an outgoing port which was involved in a conference call. The command was returned with an NSB of $01. However, even after all ports involved in the conference had gone on-hook and were idle, the aforementioned outgoing port was still in the conference call, and the conference remained active. To correct this problem, an outgoing port in conference cannot be detached with a $69 command. Such a $69 command will be returned with an NSB of $1C (“Line/Trunk Port In Conference”).
U611210035/ **U611210052** U509190002 U610010008 TR 5253	Previously, when a $49 command was issued to idle an incoming port which was in SETUP, and a DTMF port was attached to it, the port was idled but the DTMF port remained in the CP_ATT major state. This problem was found to exist for all resource types. This problem has been corrected so that now when a port in CP_SETUP with resources attached is idled with the $49 command, all the resource ports attached to it are released and set to CP_IDLE state. An additional problem was addressed by this TR. When a $67 command was issued to an ICT in CP_SETUP or CP_STAB to play prompts and collect DTMF digits, after the prompts were played and digit collection was complete, the port major state remained as CP_TALK, instead of returning to its original CP_SETUP or CP_STAB. This problem has been rectified so that the port’s major state will revert back to CP_SETUP or CP_STAB.
U611210037 U510230001	A problem occurred when a $69 command had seized a T1 port “A” using a virtual port. Port “A” answered. T1 port B went offhook, and a $6B command was used to change the virtual port to B. If port A did not answer until after the $6B was issued, the AB bits remained high, as they should have. However, if port A answered before the $6B command, RX AB bits on port B remained low, and no $70 command was sent to the incoming T1port. A $70 command is now sent.
U611210040 U511010001	Previously, if a user typed CTRL-S from a telnet session to stop the screen, and then CTRL-] to close the session, the user would be locked out and could not login to any of the three administration ports (TTY01, Remote, or Telnet). The system has been changed so that the status of the XON/XOFF feature is now controlled from the administration console. If XON/XOFF is disabled, CTRL-S is ignored. If CTRL-S and then CTRL-] is entered from a telnet session without a CTRL-Q in between, the lock-out will occur.

TR #	Corrected Problems
U611210041 U511060001	There was a problem with prompt count validation for the $6C and $6C (Enhanced) commands, both when they were sent alone and as a segment in a $6A command. If the number of prompts specified in the Prompt Control byte was different from the number of prompts actually included in the command, the command would generally be returned with an NSB of $01 and unpredictable behavior could result, e.g., some prompts would not be played, invalid prompts would be played, etc. Now, such a command will be returned with an NSB of $03 (“Syntax Error In Command”) or $27 (“Too Many Prompts In DVC Port Control ($6C) Command”), whichever is appropriate.
U611210043 U511130010	Previously, adding a one-way port to a conference call with seven two-way and one-way ports with the $6D command, could result in a $03 Syntax error being returned as the status byte. The possible combination of ports that should be allowed in a conference are: a) maximum of eight two-way ports and no 1-way ports, or b) maximum of seven two-way ports and any number of one-way ports, as limited by the total ports in the system. The system now accepts the port count as per the description of the $6D command in the Programming Reference. The system will not fail for a $6D command with a mix of two-way and one-way ports, even though the total number of ports exceeds eight. If the count is invalid, the command is returned with an NSB of $54. If there are duplicate ports in the command, it is rejected with an NSB of $55.
U611210045 U511270006	If the Ethernet subsystem fails, a FATAL alarm is returned instead of a MAJOR, as had been the case previously. The FATAL alarm condition triggers a system reset (switchover to the standby side) in a redundant configuration. The system must be reset.
U611210046 U511280003	During a telnet session, if the escape character was set to anything other than ^] (Control, right square bracket), entering ^] would cause the system to crash. This problem has now been corrected.
U611210048 U603070004	Previously, if the span of a 4xT1 card went into maintenance as a result of reaching a SLIP/OOF limit, or if the span was manually taken into maintenance by the system administrator, or if the port was busied-out with a $90 command, the AB bits of the port were not raised. The bits could be raised, however, if the ports were manually P’d out from the Maintenance menu. The port’s state in this case was CP_MBUSY. The far end equipment connected to this span had no way to determine that the ports were not available for calls. This also applied to T1, E1, and 4xE1 cards. The Generic has been modified to raise the AB bits and place busied-out ports back into service.

TR #	Corrected Problems
U612020002 U403133352 U403144452 TR 4452	The 4xT1 declared port release ($3A) before the far end. If users had a stable call and the far end went on hook on a 4xT1, the 4xT1 did not wait for guard time before it declared that the port had released. It transmitted the idle code and sent a $3A message before the guard time expired. Now, the 4xT1 card waits for guard time before declaring that the port is released.
U612020003 U403164460 U407154615 TR 4460 TR 4615	Previously, clear 4xT1 ports were not passing through A and B bits. If users cleared a specific port without clearing the entire span, the port did not clear. Now, users can set individual ports to clear channel signalling on the 4xT1/4xE1.
U612020004 U404274520 U501164873 TR 4520	If both a voice prompt and a digit collection (with a first-digit timeout configured) were specified for an incoming call, and if the first-digit timeout condition occurred after the prompt was played, the DRC port remained attached to the trunk port in the WAIT state until any other event occurred that allowed it to advance. If a subsequent collection occurred on this port, digits could be collected; however, the collection parameters from the previous collection applied. This problem has been corrected so that a first-digit timeout is handled properly by the DRC port.
U612020006 U411154770 TR 4770	The gain/law ROMs did not perform the A-law stream to Mu-law for the 4xE1 card. This problem has been corrected.
U612020007 U5011648731 TR 4873	Timers on the 4xT1 to ESF-NR were being ignored; the long and short duration timers did not work on the 4xT1 when the signalling mode was ESF-NR. There was no response from the 4xT1 card running ESF-NR for the short and long duration timer commands. Now the short and long duration timer commands work for clear (SF-NR/ESF-NR) ports.
U612020008 U507195131 TR 5131	There was a problem in which the standby side crashed when an incoming DASS2 call was received and enhanced redundancy was turned on. This problem has been corrected.
U612020010 U509015237 TR 5237 TR 5244 TR 5243	The generic was sending the 4xT1/4xE1 firmware some redundant messages that are specific to a T1 card. These messages were simply ignored. However, when multiple 4xT1/4xE1 cards booted up, these messages consumed sufficient bandwidth to potentially cause queue overflows.
U612020011 U509065243 U601240002 TR 5243 TR 5237 TR 5244	A system with a large number of 4xT1 cards (>15) experienced queue overflow problems at initialization when trying to download all the cards. The generic software has been improved to handle such a scenario.

TR #	Corrected Problems
U612020012 U509065244 TR 5244 TR 5237 TR 5243	Additional queue overflow problems were being seen after the 4xT1 cards were downloaded, during span configuration. This problem has been corrected
U612020013 U509270001 TR4717	Previously, an established ISDN call in a NFAS group with no backup D-channel and with both port states CP_STAB could be randomly torn down with a RELESE COMPLETE of cause 45 (pre-emption) on one side. The corresponding port state became CP_IDLE. Operation now depends on the SETUP request and bearer channel specification: 1.) Incoming SETUP request specifies an “exclusive” bearer channel or a “preferred” bearer channel whose major state is not CP_IDLE or CP_STAB — an ISDN glare condition is detected and the incoming call pre-empts the outgoing call. 2.) Incoming SETUP request specifies an “exclusive” bearer channel whose major state is CP_STAB — an ISDN glare condition does not exist and the incoming call will not pre-empt the outgoing call. The incoming call attempt fails. 3.) Incoming SETUP request specifies a “preferred” bearer channel whose major state is CP_STAB — the incoming call will try to find another available channel on the same interface to complete its call establishment.
U612020014 U601240002	During initialization of each span of a 4xT1 download, it was possible for the span to become busy printing boot status information to the diagnostic port while the span configuration command was transmitted. This command instructs the span as to which clock source to transmit to the far end. The second problem was in the generic software. If the primary incoming clock source was driving the incoming reference clock and experienced a remote alarm, the secondary clock source was enabled. However, the generic never instructed the primary timing source to release the reference. As a result, two clock sources were simultaneously driving the incoming reference clock. If was difficult or impossible for the NBC to lock on this corrupted clock signal. Now, when an active timing source encounters an alarm, the timing source is disabled from the reference signal. In addition, the 4xT1 card will now default its transmit clock to the system clock, and the span will not declare itself available for service until the completion of the initialization routine.
U612020015 U602280001	A customer reported that their 4xT1 cards were exceeding the slip limit. It was later determined that a single frame slip caused the interrupt to fire multiple times. This has been corrected so that the 4xT1 now properly tracks slips.

TR #	Corrected Problems
U612030001 **U612050001** **U611210044/** U504255009/ U502104904/ U511212001/ TR5009/ TR4904	There was a problem in which the RETAIN token was supported for only the IPRC and DRC in the inpulse rules, and only partially supported in the outpulse rules. Also, the RELEASE token was supported in the screen manager for the resource types IPR, MRC, DRC, DTG, and CPA but was not fully supported in the run time processing. There was also an inconsistency in that the resources DTG and CPA, were not relevant to the IP rules but were supported for the RELEASE token. Resources IPR, MRC, and DRC were not relevant to OP rules, but were supported for the RELEASE token. In addition, it was not possible to add a resource type for only an IP or OP rule. As a result, the following changes have been implemented: 1.) The screen processing for the RELEASE token allows DRC, MRC, IPR, CPA, DTG, and MRC (MFCR2). The run-time processing for the RELEASE token releases the specified resource for either Inpulse or Outpulse rules. 2.) The RETAIN token is supported in Inpulse rule processing for the resource types DRC, MRC, IPR, and MRC. 3.) The RETAIN token is supported in Outpulse rule processing for the resource types CPA, DTG, and MRC.
U612160001 U511220001	A system failure occurred when a $69 command was issued to disconnect an incoming ISDN port attached to a ringing phone (the port was in CP_WANS state). A $49 command was issued to let the incoming ISDN port execute an oprule which contained a DISC_T token but no CAUSE_IE token. A CAUSE_IE token is mandatory for disconnecting ports.
U612160002 U605070003	E1 signaling did not allow reception of far end busy. The system now operates properly.
U612160003 U602130001	Occasionally, during a system watch-dog time-out, the system would dump information into the log file which would show that a call chain got corrupted, causing the watch-dog time-out. Now, calls are properly torn down and the service port is placed back in Idle.
U612160004 U603220003	Improper hardware configuration of the 4xT1/E1 cards in earlier versions caused individual ports to be activated with incorrect gain and/or law configuration. Symptoms included noisy voice paths and diagnostic failures. This was more likely on international systems.
U612160007 U607160001	A problem occurred in which the $67 command was issued with voice prompts and delayed first digit timer. If a user entered either clear character or digits followed by clear character while the prompt was playing, the prompt was halted. When the digit collection was restarted, the first digit timer was not enabled. This caused the receiver port to hang while it waited for digits or for a time-out.

TR #	Corrected Problems
U612160008 U607260003	An issue existed in which a port would be stuck in CP_GARD when the call was torn down if the Remote Alarm had been set for an E1-PRI card configured for DPNSS. The Yellow light would turn on, and the card would be in Camp On state, but the call established on this card remained in CP_STAB.
U612160009 U608050001	In earlier versions, when an Enhanced $67 command was issued to set to collect two digits on a DRC8 port, and more than two digits were entered, the DRC8 port was detached even though the Retain flag had been set. The DRC8 port now remains attached.
U612160010 U608100001	Normally, when a user places any E1-PRI card into Maintenance state from Active state, the ISDN states of all the ports on the card go to MAINT-NE state. A problem occurred when the card was brought back to Active and ports 31 and 32 stayed in MAINT-NE state. This resulted in unusable ports until these two ports were P'd out/in. Now every port goes back into IN_SERV.
U612160011 U608160001	In earlier versions, the Generic inappropriately issued a command to the DRC8 card between each field of digits collected in a multiple-field DTMF collection. This resulted in the second digit of each field, other than the first field, being dropped.
U612160013 U609200001	On occasion, when a conference call was being torn down or a port was being deleted from the conference through the $6D command, the standby side would fail with a bus error exception. Now, after a $6D command to tear down a conference call or delete a port from a conference is issued, the port goes back to CP_SETUP. Resources are detached on the Active side, and the standby side will not fail.
U612160014 U609230006 U602130001	Occasionally, during a system watch-dog time-out, the system would dump information into the log file which would show that a call chain got corrupted, causing the watch-dog time-out. Now, calls are properly torn down and the service port is placed back in Idle.
U612160015 U610110002/ U610150001	Previously, if the host setup timer was set when a port with COS A2 went off-hook, and the host did not respond before the setup timer expired, the call was terminated. The port went back to IDLE, and since the port had COS A2, the port status stayed in off-hook. However, the SBY side port status went back to on-hook for the same port. The problem occurred during switchover. The new Active side saw the port as idle and on-hook. This resulted in an unusable port (the far end was already off-hook, because the Summa side appeared to be off-hook). This could be seen from the card display screen. Now both Active and SBY side hook states are consistent.

TR #	Corrected Problems
U612200001 U607290002	Auto make-busy counters were not being cleared at midnight. The system now functions as documented—make-busy counters are reset at midnight. Note: if the card is already in the make-busy state, the counters will not be cleared, and the card will not be brought back into service.
U701090001	The 340 processor receives a DID (Device IDentification) signal from each of the spans and then waits for BCYC (Bus Cycle). Previously, while waiting for BCYC, it printed the message 'Wait for NBC BCYC." The time to print the message would occasionally cause the 340 to miss detection of BCYC from the NBC during the allocated 5 seconds for detection. The 304 comm test was declared a failure and DID would not be raised even if the card had a valid ID. The print has been eliminated
U701140005 **U611210051** U607240006	Previously, Ethernet parameters could not be changed from the standby (SBY) side. The parameters in the Ethernet/NFS Configuration screen, such as Current System Internet Address, are now configurable on the standby side. The following message is shown on the screen: Update Ethernet/NFS Configuration (Y/N)? When the user selects Y, the parameters are stored in NVRAM and a message similar to the following is shown on the screen: PRM052: Ethernet/NFS Params Updated. New Address On Reboot Is XXX.XXX.XXX.XXX.
U701140006 U603210003	Prior to this release, spans receiving short hits from the network (fewer than 2 seconds) would generate an alarm. An alarm should not be generated until a hit has existed for at least two seconds.This occurred with 4xT1 and 4xE1 cards. The network polling rate is once per second, and is now checked on the third, rather than on the second, poll.
U701240003 U612200003	When a $6D command was issued to bring an ISDN port into a conference, the command was rejected with a status byte $21 indicating that the port was off-hook. The problem was caused by a failure to either send or receive a CONNECT message on the switch side. The system now adds an ISDN port into conference after responding to the SETUP message. The $6D command is not rejected.
U701240004	Previously, when a DRC-48 was taken OOS from the card maintenance screen, the subsequent $D9 report showed an incorrect DRC port address. The port address range should have started with $4000 or above. Instead the range was $0000-$002F. For instance, if the DRC-48 had ports from $4000 to $402F, the $D9 report would show $0000 to $002F. The correct range is now shown. Also, if a user P'd out a DRC port from the card maintenance screen, the generated $D3 report showed the same problem discussed above; the range failed to start with $4000 or above. The correct range is now shown.

TR #	Corrected Problems
U702040001	On V4.0 systems with NBC-3s, if a user changed the configuration of a 4xT1 or 4xE1 span that was being used as a Primary timing source, the timing source changed from Primary to Internal. If the system had been configured for Primary only, and the Secondary timing source was not defined, the system would not switch back to Primary. If the used had defined the Secondary timing source, the system would switch to Secondary, the NBC-3 sent a T1 synchronization loss message to the Generic, and the Internal timing remained in effect. The addition of an NBC message code to the NBC-3 download permits the Generic to respond properly by immediately reverting to Primary timing.
U702260003	Previously, when an Out of Frame condition existed for a card and/or the card had a Major or Minor alarm condition, no $F0 report was sent to the host. A $F0 report is now sent to the host when either the Major or Minor alarm is set.
U703050003	Previously, the PRI/N ALL Ports Deactivated Alarm feature was not being reported to the standby side. Operation is now correctly reported.
U703140002	Previously, when a 4xE1 card had a port busied out from the far end, it would occasionally not return to the Idle state.The problem was a failure to properly distinguish between off-hook and far-end busy. The far-end, busy-out condition is now handled correctly with the new 4xE1 download and appropriate firmware. See *Section 2*.

1.14.1 Expanded Description of U611210023

Previously, there was no easy way to get information about the Product Unit Number (PUN), though it was available in the database. This information is now displayed in the Administrator Main Menu (Figure 1.12) and the Software/Firmware Configuration screen (Figure 1.13), where the version, revision, and FSR information is displayed. You can also display this information in the screen message line (right bottom line) on any screen when you depress **CONTROL/V**.

```
        A D M I N I S T R A T O R   M A I N   M E N U

        Generic Version.Revision 4.0 002

A) Data Base Administration Menu
B) System Configuration Menu
C) Maintenance Menu
D) Diagnostics Menu
              Enter Selection: ___
```

Figure 1.12: Administrator Main Menu with PUN Information

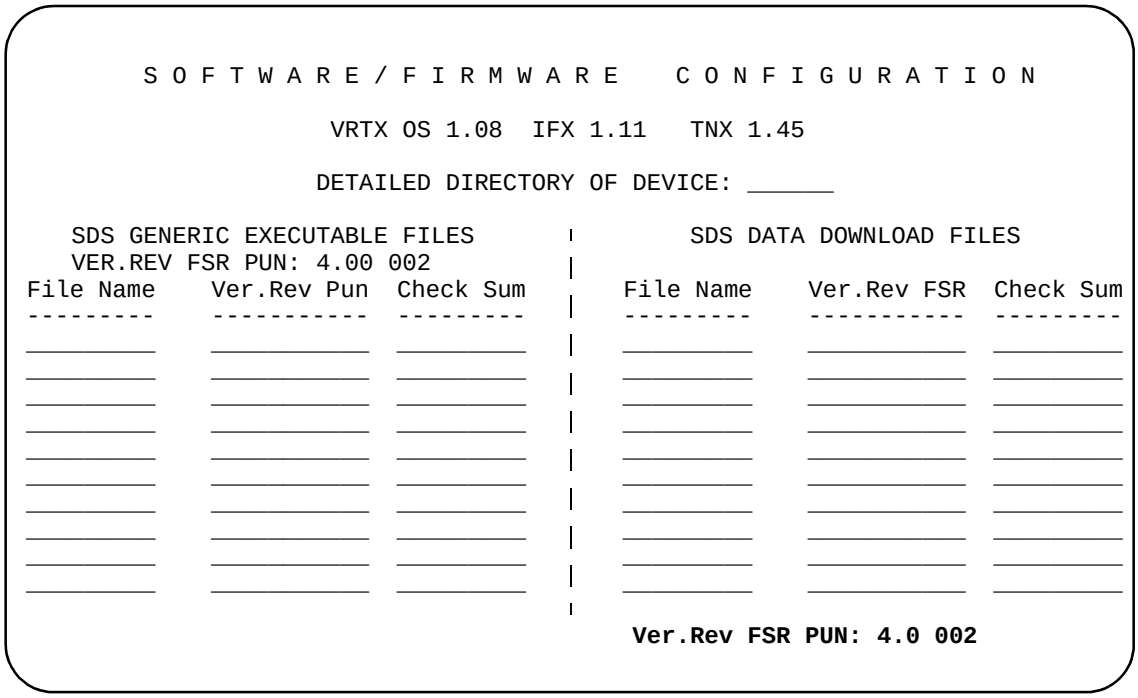


Figure 1.13: Software/Firmware Configuration Screen with PUN Information

1.15 PROBLEMS CORRECTED IN V4.0 FSR02 PUN21

The following problems have been corrected in V4.0 FSR02 PUN21.

TR #	Corrected Problems
U702180002	Customers using subrate switching without C-bus who request a large number of timeslots could cause a failure and cause the system to store an invalid port address. The problem arose because the timeslots were not allocated contiguously. Timeslots are now allocated contiguously, and if a timeslot is not available, an error is generated.
U703270001	VCO20 systems with a single SSC card and with four or more 4xT1s in the data base, would fail to come into service on reboot. The SSC times out before all four of the 4xT1 cards can be reset by the NBC. Each 4xT1 is treated as four separate reset operations. The SSC card now becomes active with all 4xT1 cards in the data base.

TR #	Corrected Problems
U704170001	After approximately 28,000 subrate paths had been established and torn down, the system would start exhibiting memory allocation errors with the message: "Architecture Error 1: Memory Allocation Error." No subrate call processing would then be performed. The system no longer experiences memory allocation errors and will operate to many times the 28,000 threshold without error.
U705290008 U703200002	Previously, if a non-active ISDN port was added into a conference, when the port was deleted from conference or the conference was torn down, the port went to CP_IDLE instead of staying in CP_SETUP, even with $6D command specifying to leave the port in CP_SETUP. Now the ISDN port is left in CP_SETUP state.

1.16 PROBLEMS CORRECTED IN V4.0 FSR02 PUN22

The following problems have been corrected in V4.0 FSR02 PUN22.

TR #	Corrected Problems
U609270002	Prior to this fix the NBC would NACK the expected buffer rather than ACKing a retransmitted buffer. NACKing the expected buffer had two possible effects: 1) the expected buffer was transmitted before it was ready, 2) the expected buffer was transmitted twice. In case 2, this could cause a chain of double buffer transmittals. This could result in a system failure because of the way the system handles a FLUSH string when a buffer is sent. The system now recovers from the FLUSH condition.
U611120002	Previous systems would communicate over a network only if Class C IP addressing was used. That is, the first three bytes of the address had to be the same on both machines. The system now supports Class A and Class B type subnets in addition to Class C. See *Section 1.10*.
U704240003	The previous release (V4.0 FSR02) unintentionally reset function key mapping when earlier systems were upgraded. This was not seen by customers receiving new systems, because it was corrected at Summa Four prior to shipment of new systems. Function keys now retain the default key mapping that existed prior to upgrade.

TR #	Corrected Problems
U705010001	Previously the NSB returned values of $54 and $55 were improperly assigned to two different commands. For the $65 command these are now assigned with the following values and meanings: $5F - Subrate channel must be greater than zero and less than or equal to eight. $60 - Subrate channel crosses bearer channel boundary.
U705070007 U702140002	Previously, an NFAS group could loose both primary and backup D-channels and then return with all the B-channels in OOS-NE. This resulted in unusable ports. Now both primary and backup D-channel cards stay in MAINT state; and after the D-channels are back, the B-channels are in IN-SERV state.
U705120013	Prior to this fix the IPRC-8, -64, and -128 cards could fail diagnostics run from the Test Service Circuit option of the Diagnostics menu. Failure results in the following message type: DGN08: IPRC RLS xxx No Response From DRAM Test, where xxx is the rack, level, slot of the IPRC card. A message indicating test failure follows. All tests run to normal completion and report success or failure within three minutes. Results are displayed and sent to the log.
U705120014	Prior to this fix the diagnostic utility for IPRC-8, -64, and -128 cards did not indicate which of the three tests (DRAM, SCSI Interface, or PCM Interface) failed. Test failure type is now presented in the message "DGN10 IPRC RLS xxx <Test Type> Failed." This message is sent to the terminal and to the log file.
U705290004	Previously, if a LOC alarm was generated on a 4x span, a $D9 report was generated to the host. When this alarm was cleared, another $D9 report was sent to the host. However, immediately following the alarm clear another Remote alarm was generated. This alarm was cleared immediately and generated another $D9 report. The two $D9 reports could not be handled by the SS7 interworking software. Now only one report is generated for each span.
U705290005	Previously, when an incoming ISDN call in Overlap Receiving state was routed to an outgoing NON-ISDN call and a true answer was detected from the outgoing side, the CONNECT message did not get propagated back to the incoming port. I_OVRLP has been added to the list of states in the Generic that support CONNECT message propagation. Stable calls are now established.

TR #	Corrected Problems
U705290006	Previously, in systems configured with primary/secondary incoming timing, if the primary timing was not available on system reboot, the secondary timing source was shown incorrectly as 1-1-1. Now, when the system is rebooted, the correct timing source is always displayed.
U705290007	When a $49 command was sent by the Host for processing an outpulse rule requiring CPA for supervision on the outgoing port, the system failed to reject the command when the CPA port was unavailable. Now, if a CPA resource limitation exists, the $49 command will be rejected with a NSB of $3A, no CPA port available.
U705290009	Prior to this fix, a burst of host commands sent to the switch could overflow the CP_MSG queue. In some installations, this occurred during host initialization. It could also occur following a host link failure as calls were reassigned. Data was lost and the system may have rebooted. CP_MSG no longer overflows.
U705290010	Occasionally, all the ports on a 4xT1 or 4xE1 span would become stuck in Major state CP_DISC and Supplementary RDR_QUIET. Now, when the Generic receives a $C6 report from a span with an error code of 1A to 1D (depending on the span) indicating a time-out error, it logs the error and resets the span.
U705290013	Previously, when a $69 command was issued to process an outpulse rule on an Idle COS A2 or 2 port, the system would become stuck in CP_OUTPULSE state. The port would remain stuck even after going off-hook and then on-hook, or being P'd out. The only way to clear the port was to take the card OOS and then reactivate it. Now processing using the $69 command is possible only on an outgoing port that is already off-hook.
U706030003	Occasionally the system would shut down with Network manager failure or "Call Chain Dump:..." following system reboot under load. The system no longer shuts down with a Network manager failure.
U706030004	Previously, when a $82 command was issued to request card status for the DRC24/48, the command could return the wrong port address for the card. The correct port address is now returned.

TR #	Corrected Problems
U706040001	A problem existed if the following scenario occurred: A user would telnet into the active side of the switch and select Diagnostics from the Main menu. The user would then run Display Card Data and open another telnet session into the active side. If he pressed any key on the system console, after waiting for a period of time, “PRM013: Invalid Field Number Specification” was displayed. A login screen would appear with an erroneous login and password and the screen would lock up. Since the telnet session was not disconnected, the system console was also affected. This problem has been corrected.
U706060001	Prior to this fix, when a 4xE1 port configured for CAS Mercury received an incoming call, the 4xE1 did not transmit signaling bits to seize. The call timed out and was torn down. Signaling bits are now sent.

Section 2
SYSTEM REQUIREMENTS

2.1 INTRODUCTION

This section provides a listing of system requirements for running Generic V4.0 FSR02. These requirements are divided into database, hardware, firmware, and software. Contact Summa Four, Inc. Technical Support at 1-800-9SUMMA4 for any site-specific information.

2.2 DATABASE CONFIGURATION

The VCO system is shipped to you with:

- the Generic software installed on the hard drive
- the licenses configured in the database
- the NBC-3 and DTG/DTG-2 cards configured in the database
- all cards physically installed inside the enclosure

Appendix D contains an overview of the steps you must follow to add and configure the cards in your system.

2.3 HARDWARE REQUIREMENTS

To operate V4.0 FSR02, a system must be equipped with the following components:

System Controller

- 8 MB 68030-based CPU (central processing unit)
- CPU Transition Module (CPU-TM) or Storage/Control I/O module
- VME-147 System controller card (must have updated boot PROMs) or Combined Controller
- SWI Version A0AR

Storage Subsystem

- SCSI interface hard drive, 42 Megabytes or larger
- 3.5" SCSI Interface Floppy Drive

Control Circuit Cards

- NBC-3 card Rev C0GR (or later) or E0AR (or later)
  (Two NBC-3 cards are required for redundant systems; one NBC-3 for non-redundant systems.)
- BRC—Bus Repeater Card—*not required for VCO/20 systems*
  (A BRC is required for each expansion rack—one in slot 1 in non-redundant systems, one each in slots 1 and 2 in redundant systems. SDS and VCO/80 systems only.)

Service Circuit Cards

- DTG/DTG-2—Digital Tone Generator
  (All systems require a tone card to provide a quiet tone to the network.)

SNMP

- Ethernet connection

If you are planning to use SNMP on your system, an SNMP Network Management Station (NMS) application or platform is recommended. You will need the NMS or an alternative application to perform SNMP tests on your system. One alternative is to use the tools available with applications such as Hewlett Packard's OpenView™ or Sun Microsystem's Net Manager®.

The components listed in this section are installed in new systems prior to shipment.

For information on the NBC-3 card hardware requirements, see the *Technical Description: Network Bus Controller-3 (NBC-3) Card*.

2.4 FIRMWARE REQUIREMENTS

System firmware requirements common to all systems are listed in Table 2.1. Table 2.2 lists domestic (U.S.) firmware requirements. Refer to the technical descriptions in Volumes 3 and 4 of your hardware documentation set for firmware locations for each card. Instructions for removing and replacing firmware PROMS are contained in *Appendix A* of this document.

Notes:

[1]*The firmware label applied by Summa Four may list only the last four digits of the checksum.*

[2]*The checksum for the NBC-3 LP125 is not given because the programming for this item is part of the NBC-3 download file and is included in the checksum for the NBC download file..*

Table 2.1: Common Firmware Requirements

Card	Firmware	Checksum[1]	Vers.	Location	Changed Since FSR01?
North American Requirements					
BRC	BRC	2412	2.01	U2	N
CPA	CPA	A7A2	1.03	U2	N
CPU	Boot Even Boot Odd VME147 1 VME147 2	0065CCA3 007C942C 000028D7 0000D471	4.02 4.02 2.43 2.43	U1 U15 U30 U22	Y Y N N

Table 2.1: Common Firmware Requirements (Continued)

Card	Firmware	Checksum[1]	Vers.	Location	Changed Since FSR01?
DID-2	DID-2	10C3	1.41	U2	N
DRC-8	DRC	9625	5.23	U2	N
DRC-24/48	DRC-2	4241	3.08	U2	N
DVC	DVC	95BE	2.07	U2	N
E+M	E+M	D381	2.06	U2	N
E1-CAS	E1-CAS/MERC E1-CAS/R2 E1-31B E1-CAS/R2 (No CRC4) CAS PROC 32 CHAN SETUP GAIN/LAW PROM	F1C6 2654 EF58 EFD3D 1E78 CDDE 11D2	2.13 2.01 3.03 3.42 1.04 1.00 1.02	U23 U23 U23 U23 U85 U113 U45/53	N N N Y N N N
IPRC-8	IPRC 8-PORT	220D75	1.03	U2	N
IPRC-64	IPRC 64-PORT	220DC1	1.03	U2	N
IPRC-128	IPRC 128-PORT	220E0A	1.03	U2	N
MRC	MRC	EE80	3.08	U2	N
MVDC-T1	Local Bus	0D373B	LP100A	U35	N
	Com Bus	186169	LP101A	U19	
	Interrupt	0AE787	LP102	U75	
	PCM Interface	1748E3	LP103A	U107	
	Framer	05FE2C	LP104	U76	
	Gain/Law	05A153	LP105B	U49	
	T1 Clock	0BE051	Lp106	U80	
	Gain/Law	776220	—	U50	
	Boot PROM	0065B028	1.06	U10	

Table 2.1: Common Firmware Requirements (Continued)

Card	Firmware	Checksum[1]	Vers.	Location	Changed Since FSR01?
NBC-3 Card Rev C	LP122 SWI	00194974	LP122C	U66	
	LP123 Counter	0018E096	LP123E	U13	
	LP124 Chip Select	000D7B43	LP124C	U12	
	LP125 Com Bus FPGA[2]	__	LP125C	U43	N
	LP126 Com Bus EPLD	0005CED8	LP126B	U47	
	LP127 Mezzanine Add.	0006C919	LP127A	U105	
	Boot PROM	00F597BE	1.02	U4	Y
NBC-3 Card Rev E	LP141 SWI	0019204D	LP141A	U31	
	LP140 Counter	0018B52F	LP140A	U73	NEW
	LP139 Chip Select	000D4209	LP139A	U30	
	LP125 Com Bus FPGA[2]	__	LP125C	U53	N
	Boot PROM	00F597BE	1.02	U1	Y
SSC	Com Bus Control	186169	LP101A	U24	
	PCM Interface	00185A34	LP130A	U76	
	Quad 9 to 1	0017878C	LP129A	U71/U70	
	Redundancy Control	0017F249	LP128A	U100	N
	Subrate Matrix Control	000BB573	LP131	U31	
	Boot PROM	003FF71B	1.01	U10	
SLIC-2	SLIC-2	10B9	1.41	U2	N
SRC	SRC	E5C7	1.07	U2	N
T1	T1 T1 Aux Proc	2BA5 7125	1.26 1.00	U2 U45	N N
UTC-2 Rev A UTC-2 Rev B	UTC UTC	F91E ECF0	6.00 6.54	U2 U2	N N

Table 2.1: Common Firmware Requirements (Continued)

Card	Firmware	Checksum[1]	Vers.	Location	Changed Since FSR01?
4XT1/E1	4XT1/E1 68340 VIRT CM	291041	1.08	U10	Y
	4XT1 68302 ODD	277039	1.12	U48, 94, 151, 186	N
	4XT1 68302 EVEN	24479B	1.12	U47, 93, 150, 185	N
	GAIN/LAW CCITT G.711	0FCD68	1.03	U25, 28, 67, 78, 120, 131, 158, 170	N
	PATH SETUP ROM	CDDE	1.00	U35, 86, 116,178	N
	4XE1 68302 ODD	268B57	1.01	U47, 93, 150, 185	Y
	4XE1 68302 EVEN	232FCC	1.01	U48, 94, 151, 186	Y
International Requirements					
E1-PRI	E1-PRI FW Odd E1-PRI FW Even E1-PRI 32 Chan Setup PCM Gain/Law	105999 DA6C3 CDDE 11D2	1.03 1.03 1.00 1.02	U38 U39 U113 U45/53	Y Y N N

Table 2.1: Common Firmware Requirements (Continued)

Card	Firmware	Checksum[1]	Vers.	Location	Changed Since FSR01?
International Requirements (Continued)					
NET5	Net5 Odd Net5 Even	105997 DA683	1.01 1.01	U38 U39	Y Y
PRI	PRI FW Odd PRI FW Even 32 Chan Setup PCM GAIN/LAW	107EA5 DB30B CDDE 11D2	1.02 1.02 1.00 1.02	U38 U39 U29 U45/53	Y Y N N
PRI/N	Odd Even 32 Chan Setup PCM Gain/Law	116A29 DECA0 CDDE 11D2	1.08 1.08 1.00 1.02	U38 U39 U29 U45/53	Y Y N N

Table 2.2: Domestic (U.S.) Firmware Requirements

Card	Firmware	Checksum	Vers.	Location	Changed Since FSR01?
DCC	DCC LIN/PCM 0 DB LIN/PCM -3 DB PCM/LIN Odd PCM/LIN Even	A575 B9A2 AB04 AFA2 B736	2.02 1,00 1.00 1.00 1.00	U2 U43 U44 U33 U34	N N N N N
DTG/DTG-2	DTG-FW Tone Odd Tone Even	77AD 0078 4217	1.23 2.04 2.04	U2 U54 U53	N

2.5 SOFTWARE REQUIREMENTS

Valid software versions and checksums for Generic V4.0 FSR02 software and optional software product FSRs (Field Support Releases) are listed in Table 2.3. Use the Software/Firmware Configuration utility to identify the version and checksum of each software file installed on the system (refer to the *System Administrator's Guide* for more information). Generic software files are distributed across four floppy diskettes. Each optional software product is contained on a single floppy diskette.

Table 2.3: V4.0 FSR02 Software Requirements

Software Product	S/W Vers.	S/W FSR	Filename	Check-sum	File Vers.	Changed since FSR01?
GENERIC	4.0	02	GLOBALS.EXE	02404959	4.02	Y
			HOSTMGR.EXE	023DF2C7	4.02	Y
			SYSWD.EXE	003E59C7	4.02	Y
			REDMGR.EXE	00000000	4.02	Y
			PERMGR.EXE	013CEBB5	4.02	Y
			NETMGR.EXE	00D3ACCB	4.02	Y
			INSTALL.EXE	0267F6BF	4.02	Y
			GENKERN.EXE	217BD37	3.02	Y
			MVDCT1.DWN	00E572F5	1.03	Y
			SNMP.EXE	0504EF8D	4.02	Y
			NBC.DWN	1096E76	1.03	Y
			SSC.DWN	006C84CB	1.00	N
			CPA.DWN	00053D1A	8.09	N
			DVC.DWN	005ADA02	1.00	N
			IPRC.DWN	0022E1EA	1.04	Y
			DTMF.DWN	003079F3	2.02	N
			4XT1.DWN	0033DE71	1.44	Y
			4XE1.DWN	00372C22	1.28	Y
			VRTX OS	—	1.08	N
			IFX	—	1.11	N
			TNX	—	1.45	N

Table 2.3: V4.0 FSR02 Software Requirements (Continued)

Software Product	S/W Vers.	S/W FSR	Filename	Check-sum	File Vers.	Changed since FSR01?
Options						
ETHERNET	4.0	02	ETHERMGR.EXE	7B0C	4.01	Y
TELEROUTER	4.0	02	TELERTE.EXE	7ADA	4.00	N
ISDN Options						
ISDN-NFAS	4.0	02	NFAS.EXE	7B0C	4.01	N
ISDN-PRI	4.0	02	PRI.DWN	8612E7	5.04	N
ISDN-PRIN	4.0	02	PRIN.DWN	8BDE62	5.04	N
NTTPRI	4.0	02	NTTPRI.DWN	8D86FE	1.00	NEW
NTDASS2	4.0	02	NTDASS2.DWN	9ED3E9	3.03	Y
DPNSS	4.0	02	DPNSS.DWN	AB8906	3.06	Y
NET5	4.0	02	NET5.DWN	82669D	1.05	Y

Section 3
UPGRADING TO V4.0 FSR02

3.1 INTRODUCTION

This section describes the procedures for installing Generic V4.0 FSR02 PUN 22 on systems currently running Generic V4.0 FSR00 or later, or V3.3 FSR03 through V3.3 FSR05.

> *Note: Call Summa Four at 1-800-978-6642 if you are running a version of the Generic other than those listed above.*

> **CAUTION: This section provides detailed installation instructions for loading system software and upgrading hardware. Deviating from these instructions can result in lost data. Read all the material in this section prior to installing the software. If you encounter any problems during the installation, contact Summa Four.**

To perform an upgrade of the system and/or optional software, you must take both redundant and non-redundant systems off-line for a brief period.

> **CAUTION: Upgrading to V4.0 FSR02 on SDS-1000 or VCO/80 systems, with any card other than the NBC-3 configured in slot 2 of the Master Port Subrack, can cause the CPU to crash during the reboot after the data base conversion is performed. There is also a potential risk that the database cannot be converted back to its original state after the CPU crashes.**
>
> **To avoid this condition on redundant systems, verify that the redundant NBC-3 is correctly configured in slot 2 before you begin the upgrade. On a non-redundant system, verify that slot 2 is empty and not configured in the database.**

3.2 REFERENCES

Before you install the software, make sure you familiar with the material contained in this section. You may also want to refer to the following documents:

- SDS and VCO *Installation Manual*
- Technical Description: Network Bus Controller 3 (NBC-3) Card
- Product supplements for optional software, including:

– *VCO V4.0 Management Information Base (MIB) Reference Guide*
– *VCO V4.0 Management Information Base (MIB) User's Guide*
– *TeleRouter Reference Guide*
– *ISDN Supplement*
– *Ethernet Supplement*
– *DPNSS Supplement*
– *DASS2 Supplement*
– *IPRC Supplement*
– *ISDN NET5*
– *Japanese ISDN Supplement*
– *Applicable country supplements*

3.3 OVERVIEW OF THE INSTALLATION PROCEDURE

To upgrade a system you must perform six tasks.

1. Database backup (*Section 3.5*)
   This is a precaution against any possible loss of data.
2. Hardware and firmware replacement (*Section 3.6*)
   Install the NBC-3 card.
3. System software installation (*Section 3.7*)
   Install the Generic and optional software.
4. Database conversion (*Section 3.8*)
   Update the database tables.
5. Install software on the B-side (*Section 3.9*)
   Redundant systems only.
6. Host software installation (*Section 3.10*)
   Install the MIB on your network management system.

Each of these tasks is organized as a separate section. Because redundant systems require software installation on both sides, and because the optional software varies from customer to customer, there will very likely be a slightly different path for each upgrade. If you follow the instructions sequentially and perform the tasks as they apply to your system, you will be assured of a successful installation.

As you perform the upgrade, note that task 3, system software installation, is more detailed because it also deals with optional software installation.

3.4 WHAT YOU NEED

You need the following hardware, firmware and software to do the installation. Make certain you have:

Software:

- Four (4) diskettes labeled as follows:

  VCO SYSTEMS V4.0 FSR02 PUN22
  GENERIC
  DISK *x* OF 4

  Note: The *x* is a number from 1 to 4. The number indicates the sequence in which the diskettes must be loaded when you install the generic software. Only Disk 1 contains the installation utilities.

- Diskettes containing the installation utilities for any optional software packages, for example, TeleRouter, ISDN-NFAS and/or Ethernet.
- MIB - Supplemental Disk Files (optional) to install the MIB software on your network management system.

Hardware:

- NBC-3 card, Rev C0GR (or later) or E0AR (or later) (Two cards for redundant systems.)

Firmware

- V4.0 FSR02 U1 CPU PROM labeled EVEN (CPU Boot PROM V4.02)
- V4.0 FSR02 U15 CPU PROM labeled ODD (CPU Boot PROM V4.02)
- NBC-3 Boot PROM V1.02. (U4, Rev C; U1, Rev E)

Other

- Blank diskettes to back up the system database.
- System printer with paper (powered on) so you have a printed record of the installation process.

For redundant systems, be sure you can connect a system console to both system controllers. Depending on your equipment's arrangement, you can:

- Set up a separate system console for each controller (A- and B-side).
- Use an A/B transfer switch wired to both system controller CPU-TM front panels to switch access.
- Physically remove and reconnect the system console cable from one CPU-TM front panel to the other.

3.5 BACKING UP THE DATABASE

Back up the database prior to beginning this installation. Do not try to back up the system database during the installation or after replacing the hardware and firmware (as described in *Section 3.6* of this procedure).

> *NOTE: During normal system operation, use the Data Base Store functions on the Disk Utilities menu to back-up the system data base. For more information about the Disk Utilities menu, refer to your* System Administrator's Guide.

To back-up the system data base, follow these steps.

1. Sign onto the system and access the Maintenance menu. (Refer to Figure 3.1)

```
                M A I N T E N A N C E    M E N U

          A)   Card Maintenance
          B)   Disk Utilities
          C)   Print/Display System Log File
          D)   Print/Display Trace File
          E)   Switch ACT System to SBY
          F)   Master Timing Link Selection
          G)   Card Alarm Display
          H)   System Alarm Display
          I)   Shutdown System
          J)   Voice Prompt Maintenance

                        Enter Selection:
```

Figure 3.1: Maintenance Menu

2. Remove any diskette in the diskette drive on the A-side and insert a high-density diskette.
3. Type **B** to access the Disk Utilities, and press the **Return** key.
   The Disk Utilities menu appears (Refer to Figure 3.2.)

```
                D I S K   U T I L I T I E S


          A) Show Directory
          B) Copy Files
          C) Delete Files
          D) Rename Files
          E) Database Store
          F) Database Retrieve
          G) Display File
          H) Show Free Space on Disk
          I) Format Disk
          J) Create Directory
          K) Delete Directory


          Enter Selection _
```

Figure 3.2: Disk Utilities Menu

4. a. To format the diskette, type **I** and press the **Return** key.
The following message appears:

F O R M A T D I S K

Format What Drive? ____
Disk Volume Label? _____
Do Bad Sector Scan During Format <Y/N>? ___

The cursor is in the first field waiting for your response.
Appropriate responses to the prompts are provided below:

Format What Drive?	Type **A:** then press the **Next Field** key.
Disk Volume Label?	This is optional. If you do not want to label the disk, press the **Next Field** key. If you want to label the disk, type in the label name and then press the **Next Field** key.
Do Bad Sector Scan During Format <Y/N>?	Type **Y.** This is optional. If you do not want to scan the disk for bad sectors, type **N**. *Note: This field is required and cannot be left blank.*

b. A message appears to confirm your responses.
For example:

F O R M A T D I S K

Format Drive:

A:

OKAY TO FORMAT DISK? <Y/N>? ___

Type **Y** and then press **Enter**.

5. When the formatting is complete the Disk Utilities menu appears.
   a. Type **E** for **Database Store** and press **Return**. The following message appears:

      Ok to Store Database From C: to A: <Y/N>?

   b. Type **Y** and press **Return**. A message at the bottom of the screen indicates the copying is taking place.
6. When the copy is complete, the message in Step 5 above reappears. Press **Exit** to return to the Disk Utilities menu.

7. Power down the system and continue to the next section.

   Note: If you use this backup diskette to restore the current data base after the upgrade, you will have to do a data base conversion after restoring. Refer to Performing a Data Base Conversion, *in section 3.8 on page 14. If you do not do the conversion after restoring from this diskette, the data base will not be compatible with the new version of software.*

3.6 REPLACING THE HARDWARE AND FIRMWARE

3.6.1 Replacing the NBC or NBC-3 card

Before you install the Generic software, you must install the NBC-3 card, Rev C0ER or later. If you install the software without replacing the NBC card with the new NBC-3 card, when the system is rebooted you will see a message that says the NBC is not available.

Replace the NBC or NBC-3 card whether you are upgrading from V3.3 or V4.0 FSR00.

You *cannot* replace the NBC card while the system is powered-on. However, you *can* replace the NBC-3 card while the system is powered-on. *Be certain that you are following the correct procedures for the type of NBC card you are replacing.*

If replacing an original NBC card (systems being upgraded from V3.3):
Follow the removal and replacement procedures in the *Technical Description: Network Bus Controller (NBC) Card* in the V3.3 documentation set. The technical description in the V3.3 documentation contains procedures for changing the card while the system is powered-off.

> **CAUTION: Do not remove the original NBC card while the system is running or you will damage the card. Make certain that the power to the system is turned off.**

If replacing an NBC-3 card (upgrading systems from V4.0 FSR00):
Follow the removal and replacement procedures in the *Technical Description: Network Bus Controller-3 (NBC-3) Card* in the V4.0 documentation set. The technical description in the V4.0 documentation contains procedures for changing the card while the system is powered-on.

Replacing the NBC-3 Boot PROM

After removing the NBC-3 card, replace the Boot PROM (U4 on the Rev C card, U1 on the Rev E card) with the V1.02 firmware supplied with this release.

3.6.2 Replacing the CPU PROMs

Replace the PROMs on the CPU board with the PROMs supplied with this release.

CAUTION: Before you remove the CPU card to install the PROMs, make certain that the power is turned off. In a redundant system, turn off power only on the side containing the card to be removed. Be sure to follow ESD procedures when replacing these PROMs.

- The PROM labelled EVEN goes into socket U1.
- The PROM labelled ODD goes into socket U15.

These two sockets are located next to the four LEDs on the CPU board and consist of 32-pin ICs. With the face plate towards you, these are the two left-most ICs of the four that are socketed on the board.

3.7 INSTALLING THE SOFTWARE

The following provides instructions for installing Generic V4.0 FSR02 on systems currently running V4.0 FSR00 or later and V3.3 FSR03 through V3.3 FSR05. Installation procedures for Ethernet and optional software follow the Generic installation.

Note: Call Summa Four at 1-800-978-6642 if you are running a Generic other than the above.

On Disk 1, the Incremental Install Basic System Software option installs the Generic software and downloads files onto the hard disk. This selection does not format the hard drive.

Note: Before continuing, make certain that you have completed STEP 1 and that the system database is backed-up.

The instructions in the following subsections assume that the system console is connected to the CPU-TM of the side being installed.

CAUTION: Do not install the MIB - Supplemental Disk software on the switch. The MIB software is installed on the Host computer. Refer to *Section 3.10*, ***Installing the MIB Software*****. Do this after completing the installation of the Generic software on the switch.**

3.7.1 Installing the Generic Software

With the new hardware and firmware is in place (*Section 3.6*), install the new Generic software on your system:

1. Insert Disk 1 into the floppy diskette drive (A-side if this is a non-redundant system, B-side if you are returning to this procedure to install software for that side).
2. Connect or switch the administration console to the A-side CPU-TM, or go to the A-side system console.
3. Power on the A-side.

4. After the system performs diagnostic tests, the Installation Utilities menu appears (*Figure 3.3*).

5. The cursor is located in the Enter Selection data entry field. Type **2**, (for Incremental Install of Basic System Software) then press **Return**.

   The following message appears:

   Do You Wish To Back-Up The System Data Base? (Y/N) =N?_

```
          I N S T A L L A T I O N   U T I L I T I E S


    1) Install/Configure Basic System Software
    2) Incremental Install of Basic System Software
    3) Disk Utilities
    4) Install Another Software Option
    5) Database Conversion
    6) License Configuration
    7) Terminate Installation


    Enter Selection __
```

Figure 3.3: Installation Utilities Menu

6. Press **Return** (this defaults to N).
   The database will not be backed up at this time. Make certain that the database was backed up previously, as described in *Section 3.5* of this installation procedure.

7. The following message appears:

   Insert disk 2 of Installation Set

   Press return to continue

   Remove the current diskette from the drive, insert Disk 2, and press **Return**. The system copies the files from Disk 2 to the C: drive in the /BOOT, /DBASE, /LOG and /TRACE directories.

8. When all the files from Disk 2 are copied, the following message appears:

   Insert disk 3 of Installation Set

   Press return to continue

   Remove the current diskette from the drive, insert Disk 3 then press **Return**. The system copies the files from Disk 3 onto the C: drive.

9. When all the files from Disk 3 are copied, the following message appears:

   Insert disk 4 of Installation Set

   Press return to continue

   Remove the current diskette from the drive, insert Disk 4 then press **Return**. When the installation is complete, the Installation Utilities menu appears (*Figure 3.3*).

10. a. If you have optional software packages to install, such as Telerouter, ISDN-NFAS or Ethernet, type **4**, Install Another Software Option, then press **Return**.

   The following message appears:

   Insert Another Install Disk

   Press Return To Continue

   Instructions for installing Ethernet for the Host and SNMP communications are contained in the next section, *Section 3.7.2*. If you are installing Ethernet, go to that section now. If you have other optional software to install after you have installed the Generic, see *Section 3.7.3* for generalized installation instructions. More information on optional software installation is provided in the appropriate product supplement.

   b. If there is no Ethernet or optional software to be installed, continue to *Section 3.8* to convert your database.

   NOTE: When you install a software option (such as TeleRouter, etc.) on a system, the installation process makes changes to the nonvolatile RAM (NVRAM) on the CPU. These changes make operation of software options specific to the CPU on which you installed the options. For this reason:

   - *Software options must be installed on both system controllers in a redundant system.*
   - *Software options must be reinstalled if the CPU is replaced. Although the data base information resides on the hard disk, a new CPU is unable to access this information.*

   Because of the reliability of the CPU, failures requiring replacement are very rare occurrences.

3.7.2 Installing Ethernet for Host and SNMP Communication

Do the following to install the software for SNMP trap message reporting and to set up the network parameters:

1. Insert the Ethernet diskette into the Side A drive and press the reset button. After the system loads the Ethernet files from the diskette, the Ethernet Installation Utilities menu appears with the cursor located in the Enter Selection field (see *Figure 3.4*).

```
                    I N S T A L L A T I O N   U T I L I T I E S


        1) Install/Configure Ethernet Optional Package
        2) Enable/Disable Ethernet Option
        3) Disk Utilities
        4) Install Another Software Option
        5) Database Conversion
        6) License Configuration
        7) Terminate Installation


        Enter Selection 1
```

Figure 3.4: Ethernet Installation Utilities Menu

2. Type **1** and press **Return**. The following message appears:

   Do You Wish to Back-Up the System Data Base (Y/N) =N?

   If you do not wish to back up the system data base, press **Return** and proceed to the next step.

   a. To back up the data base, type **Y** and press **Return**. Instructions for backing up the system data base are provided in *Section 3.5*.

   The Ethernet Configuration menu appears (see *Figure 3.5*).

```
            E T H E R N E T   C O N F I G U R A T I O N

        1) Install Ethernet Options
        2) Edit Ethernet Parameters
        3) Edit SNMP Management Station Parameters
        4) Edit NFS Parameters
        5) Edit Gateway Routing Table Parameters
        6) Exit Ethernet Configuration

         Enter Selection 1
```

Figure 3.5: Ethernet Configuration Menu

3. Type **1** and press **Return**. The following message appears:

   Copy A:/BOOT/ETHERNET.EXE

   1 files(s) copied

   Ethernet Option Enabled

4. To set the Ethernet Parameters, type **2** and press **Return**. The following message appears:

   System Internet Address = 107.3.254.98?

   Note: The Ethernet and Internet address numbers that you see in the screen messages in this section are only examples. In your system these numbers are replaced by numbers that represent your system addresses.

5. Set the Internet Address of this system and press **Return**.

   Set System Internet Address To 107.3.254.98 (Y/N) =Y?

6. If you change the address, you are prompted to confirm your new address. Type **Y** to confirm your selections. The following confirmation message appears:

   System Internet Address Configured

7. Set the System Subnet Mask, or press **Return** to accept the displayed value.

   After you complete this step, you can connect a remote console to your system via Telnet.

8. a. If you are *not* going to manage this system with SNMP, go to Step 14.

   b. If you *are* going to manage this system with SNMP, type **3** and press **Return** to set the SNMP Management Station Internet address. The following message appears:

      SNMP Management Internet Address = 0.0.0.0?

9. Set the Internet address to the address of the system that you are using as the NMS. Press **Return**. The following message appears:

   Set SNMP Management Internet Station Address To 189.7.107.44 (Y/N) =Y?

10. Type **Y** to confirm your selections. The following confirmation message appears:

    SNMP Management Station Internet Address Configured

    After you complete this step, the system will report SNMP trap messages to the NMS that you selected.

11. a. If you are not going to boot your system over the network, go to Step 14.
    b. If you are going to boot your system over the network, continue with Step 12.

12. Type **4** to set the Network File System (NFS) server parameters. The following selections appear one at a time. Enter the information for your system. Type **Y** and press **Return** after each selection.

    Enable NFS Access (Y/N) =Y?

    NFS Server Internet Address = 000.0.000.000?

    NFS Server Name =xxx?

    NFS Mount Directory Point #?

    Target System Name =

    Target System User Id =

    Target System Group Id =

    Target System Umask =

    Update NFS Configuration With Above Data (Y/N) =Y?

13. After you update the NFS configuration with the new data, the following message appears:

    NFS Configuration Updated

    You can now boot the system over the network from a remote disk or save the log files and database to a remote location.

14. Type **6** to exit and press **Return**. The Installation Utilities screen appears (see Figure 3.4).

15. To end the Ethernet installation, type **7** and press **Return**.

16. Remove the Ethernet diskette from drive A.

17. If you have additional optional software to install, *Section 3.7.3, Installing Optional Software,* which follows.

18. If there is no optional software to install, proceed to *Section 3.8, Performing a Data Base Conversion*.

3.7.3 Installing Optional Software

You can install optional software as part of the generic software installation or separately, on an active system. For complete installation instructions, refer to the supplement provided with the optional software.

The following section provides generalized instructions for installing an optional software package. It is assumed that this step is being completed as part of the overall install and is being done as a continuation of *Installing the Software*.

To install optional software, follow these steps:

1. Insert the optional software diskette and press the **Return** key.

   If you are installing optional software such as Telerouter or ISDN-NFAS, the installation utilities menu specific to the optional software appears in place of *Option Name* in choices 1 and 2 (*Figure 3.6*).

```
                INSTALLATION  UTILITIES


  1) Install/Configure Option Name Optional Package
  2) Enable/Disable Option Name Option
  3) Disk Utilities
  4) Install Another Software Option
  5) Database Conversion
  6) License Configuration
  7) Terminate Installation


  Enter Selection 1
```

Figure 3.6: Optional Software Installation Utilities Menu

2. To install and configure the optional software, type **1** and press **Return**. The following message appears:

   Do You Wish To Back-Up The System Data Base? (Y/N) =N?_

   Press **Return** (this defaults to N). You will not be backing up the data base at this time. Data base backup should have been done in *Section 3.5* of this installation.

3. The following messages appears for most options:

   Copying A:/*Option Filename*.EXE...

   1 file(s) copied

   Option Name Option Enabled

4. If you are installing additional software packages, press **4**, (Install Another Software Option) and repeat the steps above.
5. After you install the last optional software package, type **3** and press **Return**. Proceed to *Section 3.8*.

3.8 PERFORMING A DATA BASE CONVERSION

Since the data base tables have changed, it is mandatory that you do a data base conversion. To do this, select option **5** in the Installation Utilities menu.

Note: Japanese ISDN customers upgrading to V4.0 FSR02 will have their NTTPRI card entries replaced with PRI/N card entries. After completing the database conversion, re-enter PRI/N entries with the appropriate NTTPRI entries.

The conversion takes a few seconds. The following message is displayed on the screen:

Data base path for conversion: C:/dbase/

If the database does not need to be converted (i.e. it had previously been converted), no other messages are displayed. However, if you do convert the database, several other messages may be displayed. For example:

Converting the System Configuration table ...
(The message notes the version number being converted from and to.)

Converting the Inpulse Rule table ...
(The message notes the version number being converted from and to.)

The messages note the tables that are being converted. This will take just a few seconds.

If you are upgrading a non-redundant system or you have finished installing software on the B-side, the upgrade is complete. Type **7**, Terminate Installation (refer to *Figure 3.6*), reboot the system, and proceed to *Section 3.10, Installing the MIB Software.*

If you are upgrading a redundant system, you can boot the A-side of the system (the side you have just completed upgrading) at this time to process calls. This is optional and can be done later, after you upgrade the B-side. Continue to the next section to complete the upgrade by installing software on the B-side.

3.9 INSTALLING THE SOFTWARE ON THE B-SIDE

If you do not have a redundant system, proceed to *Section 3.10, Installing the MIB Software.*

1. Connect or switch the administration console to the B-side CPU-TM, or go to the B-side system console.
2. Insert Disk 1 into the B-side drive.
3. Power on the B-side.

4. After the system performs diagnostic tests, repeat *Section 3.7, Installing the Software*, starting with Step 4 on page 8, to install the Generic software and optional software, and then *Section 3.8, Performing a Data Base Conversion*, on the B-side.

   NOTE: Make certain that you place the Installation Disks into the B: drive during installation of the B-side.

5. After you have installed the software and converted the database on the B-side, type **7**, Terminate Installation (refer to *Figure 3.6)*. Reboot the system and proceed to the next section to verify file synchronization.

3.9.1 Verifying File Synchronization

For redundant systems, after you have installed the software on both sides and rebooted the system, you must verify that file synchronization has occurred. Check the messages at the bottom of the screen until you see:

ACT FILE SYNC COMPLETED

When file synchronization has been verified, the installation of system software is complete. Proceed to the next section to install the MIB software.

3.10 INSTALLING THE MIB SOFTWARE

Install the MIB software on your network management system. The MIB - Supplemental Disk contains four files:

vco.mib	This file defines the structure of the MIB in ASN.1 notation. It is used for your implementation of network management on a workstation, PC, or other computer system.
snmptalk	This is a UNIX executable file which provides the user with the ability to send and get information from the database tables.
mib.rt	This file, used by snmptalk, is a translation of the vco.mib file. Snmptalk needs it to understand the mnemonics used to query the database tables.
etc.ini	This is the initialization file for snmptalk.

To move the MIB software which is provided on the MIB - Supplemental Disk to a network management system:

1. Place the MIB - Supplemental Disk in the floppy drive of the Host computer.

   Note that snmptalk is a UNIX executable file and is only usable on UNIX computers. The three other files can be used on a non-UNIX platform.

2. Create a directory in which the MIB files are to reside. Define the location and name of the directory.
3. Move the files from the disk into the new directory created in Step 2.

   Note: All four files must reside in the same directory.

This completes the installation of V4.0 FSR02.

Section 4
KNOWN DESIGN CONSTRAINTS

4.1 INTRODUCTION

Summa Four, Inc. has identified and evaluated design constraints in Generic V4.0 FSR02 software, firmware, and hardware. This section provides explanations of, and where applicable, workarounds for, design constraints in the following areas:

- Upgrading to V4.0 FSR02 on SDS and VCO/80 Systems
- Simple Network Management Protocol (SNMP)
- System Configuration Utilities
- Systems Considerations
- Software Exceptions on System Controller
- Card Initialization
- DTG-2 Card Alarms
- T1 Trunk Card Support
- Digit Collection
- Inpulse Rule Processing
- Resource Group Processing
- Conferencing
- MVDC-T1
- Operational Constraints
- Connecting to Modems
- IP Addressing

4.2 UPGRADING TO V4.0 FRS02 ON SDS AND VCO/80 SYSTEMS

Upgrading to V4.0 FSR02 on an SDS-1000 or VCO/80 system with any card other than the NBC-3 configured in slot 2 of the Master Port Subrack, can cause the CPU to crash during the reboot after the data base conversion is performed. There is also a potential risk that the database cannot be converted back to its original state after the CPU crashes.

Resolution

To avoid this condition on redundant systems, verify that the redundant NBC-3 is correctly configured in slot 2 before you begin the upgrade. On non-redundant systems, verify that slot 2 is empty in the database before you begin the upgrade.

4.3 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

The SNMP agent is designed to send a trap message on all alarms that would be reported to a host. Informational messages that are displayed on the system console are not sent as trap messages to an NMS.

The clearing of alarms matches the system configuration that you have set on the System Features screen. The alarm occurrence count is reduced when the alarm clears. There are no separate trap messages for clearing or setting alarms. Alarms are returned with a severity code. It is up to the Network Management System (NMS) to interpret and display the alarms.

4.4 SYSTEM CONFIGURATION UTILITIES

The following information applies to system configuration changes performed via the system administration interface.

4.4.1 Peripheral Configuration Utility

The Peripheral Configuration utility allows you to define the communication parameters of the local and remote system administration interfaces. You must be careful to match the communication parameters (keyboard type, baud rate, etc.) to the requirements of the equipment you are using. If the configuration stored in the data base does not match these equipment or communication characteristics, the system cannot recognize keystrokes from the interface and system administration cannot be performed.

If this type of mismatch occurs, try the following steps:

- Modify the communication parameters at the interface end to match the configuration data stored in the system data base.
- Log into the system through another interface and modify the settings in the Peripheral Configuration screen. For example, if system administration is blocked on the Local TTY interface, log into the system remotely and change the settings.

If system administration access remains blocked on the interface, contact Summa Four Technical Support at 1-800-9SUMMA4.

4.4.2 U611120001: Cannot Blank Out NFS Server Name

It is not currently possible to blank out the NFS Server Name when NFS File access is disabled.

4.5 SYSTEMS CONSIDERATIONS

4.5.1 U702240001: Timeout Waiting for Console Access

This is normal when the system is trying to display messages under heavy load conditions. These are diagnostic messages that serve only to indicate that the system is too busy to update the display on the Console, such as when attempting to update the clock time.

4.5.2 U702250006: Switchovers Cause Card Alarms with DTG-2

When performing a switchover with redundant DTG2's, FRM113 T1/E1 Remote Alarms are set and then cleared for all the cards in the system. This occurs when the DTG2 from one NBC switches to the other DTG2.

4.6 SOFTWARE EXCEPTIONS ON SYSTEM CONTROLLER

When a software exception (such as a bus exception or address exception) occurs on the active system controller, the Alarm Arbiter Card remains unaware of the problem for up to 20 seconds before initiating a system switchover. During the 20 second delay:

- There may be a loss in the voice path.
- A system outage occurs before the switchover to the standby controller.
- Stable calls are not torn down and will be on the standby side.

The system recovers automatically (the controller reboots) unless the software exception was caused by a hardware failure. While a software exception on the active controller could greatly impair system performance, it is an extremely rare occurrence.

4.7 CARD INITIALIZATION

Cards request initialization from the NBC-3 by sending a signal. Under normal conditions, a card is initialized by the NBC-3, and then comes into service. If the NBC-3 cannot initialize the card, the card continues to request initialization from the NBC-3, and its green LED is lit. This may happen under one of the following conditions:

- A card connected to the backplane does not come into service (possible card failure). Remove any Out of Service cards from the backplane.
- A card is in a slot and connected to the backplane but is not defined in the system data base. Remove the card from the backplane or define that card in the system administration Card Maintenance screen.
- A card is in a slot and connected to the backplane but is defined as an incorrect card type in the data base. Remove the card and replace it with the correct type or update the card definition in the data base by using the system administration Card Maintenance screen.
- A card is marked as Out of Service in the Card Maintenance screen. Change the card status or remove the card.

The green LED is lit in NBC-3s, DTG/DTG-2s, and BRCs operating normally in Standby mode. It is good system practice to remove any Out of Service cards from the backplane to optimize system performance and further guard against the conditions described in this section.

For more information on the Card Maintenance screen, refer to the *System Administrator's Guide*. For more information on removing cards from the backplane, refer to the *System Maintenance Manual*.

4.8 DTG-2 CARD ALARMS

The information that follows applies to systems equipped with DTG-2 Cards.

4.8.1 Card Alarms for Missing DTG-2 Cards (U612120002)

All V4.0 systems that do not have DTG-2s installed on every NBC-3 will show a card alarm for the missing DTG-2s. The DTG-2 can not be deleted as a separate card from the NBC-3. Thus, these card alarms can not be eliminated when the switch doesn't have a DTG-2 installed on each NBC-2. The alarms do not hamper the switches' operation.

4.9 T1 TRUNK CARD SUPPORT

The information that follows applies to systems equipped with T1 cards.

4.9.1 Slip Conditions in T1-Channel Service Unit (CSU) Connections

T1 slips are known to occur if the T1 port is connected to a Channel Service Unit (CSU) and the current timing source is either internal or incoming. Slips should be less than 255 in a 24-hour period. If they exceed this threshold, a minor system alarm is set and a FRM114 message is sent to the printer and system logfile. The message identifies the location of the T1 card which has passed the slip limit. If this condition occurs, contact Summa Four Technical Support at 1-800-9SUMMA4. For information on setting the timing source, refer to the *System Administrator's Guide* for your system.

4.9.2 Slip Counts in Card Display Only Updated after 10 Seconds

Slip counts for T1 cards are updated every 10 seconds on the Card Display. When a T1 card is displayed, the slip count will not be accurate for the first 10 seconds. After the first 10 seconds, the fields are updated with the correct slip count and are maintained properly thereafter.

4.10 DIGIT COLLECTION

The following information applies to DTMF/MF digit collection. The type of collection (DTMF or MF) is specified where necessary.

4.10.1 Optimum DTMF Digit Timing (8-Port DTMF Cards Only)

DTMF receivers are optimized to detect digits with a 60ms on/off time (60ms of tone, followed by 60ms of quiet). As the digit on/off times decrease, digits within a collection string may be missed, resulting in erroneous digit collection reports. This condition applies to:

- DTMF Receiver Card (DRC) service circuits, eight port version only
- The on-board receivers on SLIC-2, DID-2, and UTC-2 interface cards

You should contact your network service provider(s) to determine the digit timing on circuits connected to the system.

4.10.2 Digit Collection Using Reenter/Clear Character (8-Port DTMF Cards Only)

When a one- or two-digit Reenter Character is used for DTMF digit collection with the 8-Port DTMF card, the first digit that follows that character must have an on/off time of at least 55ms. If the timer for this first digit is less than 55ms, it may not be detected by the system.

4.11 INPULSE RULE PROCESSING

The following information applies to values for Inpulse Rule tokens.

4.11.1 Timer Variations

All timers specified in seconds can vary in length up to ±1/2 second. This variation affects the Inpulse Rule tokens TIM FIELD, TIM FDIG, TIM INTER, and WAIT TIME in addition to all timers set in the DTMF Digit ($67) standard/enhanced and Speech Collection Control ($6E) commands and segments. This behavior is most pronounced when the timer is set to a value of 1 or 2 seconds.

4.11.2 TIM FDIG 15 On DRC-24/48

The DRC-24/48 does not support a first digit timeout of 15 seconds. (U412204829/TR 4829)

4.12 RESOURCE GROUP PROCESSING

4.12.1 Inserting a Port Into a Resource Group

Changes to resource group configurations during call processing are not recommended. Inserting a port into a group during call processing may temporarily prevent the system from hunting that group for ports. Commands that attempt to hunt from the group are returned with a $1F (no available port in resource group) Network Status byte until the system resets the port data pointers.

Resolution

If you must add ports to a group during call processing, you can avoid this condition by adding the ports to the end of the resource group and changing the group's hunt type setting to “Rotary” while the ports are added.

4.13 CONFERENCING

4.13.1 Conference Call Timing Delay

When adding a large number (300-400) of ports to a conference call at the same time, you may see the following message: CP_TX_Q QUEUE UNDER CONFERENCE LOAD.

Resolution

Add a 100 millisecond delay between each conference command to add each call, and this error should not occur.

4.14 MVDC-T1

4.14.1 RAM Diagnostics

The MVDC-T1 skips the RAM diagnostics after it powers-up and after subsequent resets from the NBC-3 card. This shortens the diagnostic checking period and is normal operation for the card. Do not remove and reinsert the card.

Resolution

When you want to rerun RAM diagnostics or reinstall a new download, leave the card out for approximately one minute. This will ensure that the card will rerun the diagnostics.

4.15 OPERATIONAL CONSTRAINTS

4.15.1 Activating Multiple Spans Simultaneously

Multi-span cards can sometimes get into an improper state if the entire card is OOS and the administrator attempts to activate multiple spans at the same time. This is caused by the time delay imposed by the on-card diagnostics.

Resolution

You can avoid this by starting a single span first. Always activate span one first for the 4xT1 and 4xE1. You can activate any span first for the MVDC. Once the first span is active, you can activate the others without any problem.

4.15.2 Adding Cards to End of Configured Data Base

Trying to add cards to the end of a configured data base may cause a problem. For example, if 1576 ports are assigned out of the 1776 that were licensed, and you try to add a 64-port IPRC, the following error message may occur: NO AVAILABLE PORT MEMORY. This is caused by port fragmentation, which means that there are enough total ports, but they are not contiguous.

Resolution

Rebuild the data base to reallocate the ports in a contiguous block.

4.16 CONNECTING TO MODEMS

When you connect a modem to the Modem/TTY port on the serial port 2/TTY01, the modem must be configured for 8 Data Bits/Char. If the modem is configured for 7 Data Bits/Char, the system cannot be accessed remotely.

Also, the configuration of the remote terminal must match the Modem/TTY baud rate, parity, and stop bit parameters displayed on the Peripheral Configuration screen.

Section 5
KNOWN FUNCTIONAL CONSTRAINTS

5.1 INTRODUCTION

Summa Four, Inc. has identified and evaluated functional constraints in Generic V4.0 FSR02 software, firmware, and hardware.

This section provides explanations and, where applicable, workarounds for functional constraints in the areas that follow:

- System Administration
- System Configuration Utilities
- Special Redundant Systems Considerations
- Disk Operations
- Digit Collection
- Inpulse/Outpulse Rule Processing
- Call Processing
- Command/Report Processing
- Initialization
- Network Bus Controller-3 (NBC-3)
- Digital Tone Generator (DTG) and Digital Tone Generator-2 (DTG-2)
- Four Span Cards
- Miscellaneous Card Issues
- Multiple Host Connections
- TeleRouter
- Simple Network Management Protocol (SNMP)
- Ethernet
- ISDN Issues
- International Issues
- Japanese ISDN

5.2 SYSTEM ADMINISTRATION

The constraints described in this subsection apply to system administration tasks performed from the System Administration console.

5.2.1 Functions Not Supported in SNMP

Not all system administration tasks are supported by SNMP. See *Section 5.17.1* for a list of the tasks not supported.

5.2.2 U507315154/TR 5154: Trace Files Do Not Close

Trace files do not close at the end of the calendar day unless you have disabled tracing. Therefore, if you enable tracing, and the date changes, the system continues to add trace data to the previous date's trace file.

5.2.3 U507315162/TR 5162: No Automatic Database Conversion

You may experience a problem if you inadvertently try to load a backup copy of an outdated database. The system does not detect the outdated database and does not automatically perform the database conversion.

5.2.4 U508295234/TR 5234: Adding Cards to End of Configured Data Base

If you try to add cards to the end of a configured data base, you may see the following message: NO AVAILABLE PORT MEMORY. This is caused by port fragmentation, which means that there are enough total ports, but they are not contiguous.

This could happen, for example, if 1576 ports are assigned out of the 1776 that were licensed, and you try to add a 64-port IPRC.

Resolution

Rebuild the data base to reallocate the ports in a contiguous block.

5.2.5 U512071001: Aux1 Alarm Not Set on System Alarms Display Screen

Aux1 alarms triggered by the hardware (i.e., power supply, fan unit, or ring voltage failure) are not displayed on the System Alarms Display screen. Therefore, remote users cannot determine if a major hardware alarm is set.

5.2.6 U604041001: IPRC Voice Prompt Maintenance

The following error message can occur when you add voice prompts for the IPRC card in the Voice Prompt Maintenance screen:

ERROR — Cannot Add Prompt Err = 780

You might have entered a bad directory path, or the file might not be in the location specified.

Resolution

Verify that you have specified the correct directory and path name.

5.2.7 U604100003/U607150013: Refresh Clears Log Display

(See also U604050005.) Pressing REDRAW while viewing the system log clears the log display.

Resolution:

Use the PREVIOUS and NEXT SCREEN keys to refresh the log display.

5.2.8 U605010004: Keyboard Type is Reset During System Reboots

The Administration Console intermittently gets re-initialized when the system reboots. This causes the keypad to reset to Numeric, instead of Application, which is required by the generic.

Resolution

To correct this condition on systems with VT220 consoles, complete the following steps:

1. From the login screen, press PF3. The Set-Up Directory menu appears.
2. Use the arrow keys to position the cursor in the General field and press ENTER. The General Set-Up Menu appears.
3. Use the arrow keys to position the cursor in the Keypad=Numeric field and press ENTER. The field toggles to Keypad=Application.
4. Press PF3 to save the setting and return to the login screen.

To correct this condition on systems with WYSE consoles, complete the following steps:

1. From the login screen, press PF3. The Set-Up Directory menu appears.
2. Press PF11 (Kbd2). The Keyboard2 Set-Up Menu appears with the cursor in the Keypad=Numeric field.
3. Press ENTER. The field toggles to Keypad=Application.
4. Press PF4 to save the setting and return to the login screen.

5.2.9 U607161001: Deleting Card with Master Timing Source

If you delete the card that contains the channel supplying the master timing source, the switch may fail.

Resolution:

Follow normal practice, which is to reconfigure the master timer to some other source (a channel on another port card or an external or internal source from the NBC-3) before deleting the card.

5.2.10 U610030003: FRM51 Error Reading Download

Occasionally a system boot displays “FRM51 Error Reading Download File-Code 0x7e Filename C:/boot/xxxx.dwn.” The download proceeds normally. There is no error.

5.2.11 U611260002: Abort Button

Pressing the ABORT button on the system controller has no effect if the Ethernet option has not been installed.

5.3 SYSTEM CONFIGURATION UTILITIES

The constraints described in this subsection apply to system configuration changes performed through the System Administration console.

5.3.1 U301063881/TR 3881: Selective Tracing Does Not Work

Selective tracing does not work properly in the System Trace Configuration screen. When **Selected** is enabled and you specify only one or two ports for a card, the system displays trace data for all the ports on the card.

5.3.2 U411304788/TR 4788: Viewing Software Configuration on Floppy Disks

Avoid using the Software/Firmware Configuration screen to view the contents of floppy diskettes (device A:). This screen does not produce consistent information.

Resolution

To view the contents of a floppy diskette, use the Disk Utilities Show Directory function.

5.4 SPECIAL REDUNDANT SYSTEMS CONSIDERATIONS

The constraints described in this subsection apply to redundant systems only.

5.4.1 U406284594/TR 4594: Lost Class of Service Results in Command Failure

The class-of-service of a phantom port in a stable call is incorrect. This results in command failure when the system tries to disconnect the call. The problem occurs when the active controller changes while the call is stable and the call was set up with one controller and torn down with the other.

5.4.2 U606190001: System Host Configuration Update Problem

On redundant systems, when you change the System Host configuration, you may get the error, “Standby DB Update Error - Bad Record Count.” When this error occurs, the changes made on the Active side do not get written to the Standby side.

5.4.3 U609170001: Prompt Libraries are Not Displayed on Redundant Systems

Prompt libraries added on the Active side of a redundant system are not displayed when you perform a walk through the database.

5.4.4 U701290006/U508191001: DVC $9 Timeout on Transfer to Standby

When you insert a DVC, it intermittently fails the download. A $9 timeout message is generated and also an FRM006 Transition From Standby To Active message. The system, however, does NOT change from Standby to Active.

Resolution

Reinsert the card or activate the card from the Card Maintenance screen.

5.5 DISK OPERATIONS

The constraints described in this subsection apply to actions involving the Disk Utilities.

5.5.1 U409224673/TR 4673: Database Utility Covers File Access Errors

If an error occurs in the disk operation when you use the Data Base Store or Data Base Retrieve commands (under File Utilities), no warning is displayed to indicate that all files may not have been copied correctly.

5.5.2 U505035026/TR 5026: Formatting a Floppy During Reboot

Attempting to format a floppy diskette while the system is downloading a card causes the system to reboot with the error "FRM506: Fatal Processing Error Due To - ALM002: Network Manager Failure (SA)."

Resolution

Wait until all cards are downloaded before formatting a floppy diskette.

5.5.3 U507055099/TR 5099: System Failure Dump Not Printing Completely

During a fatal alarm, the printer gets reset by the AAC, so that the last page of information going to the printer gets lost. A complete dump is available in the logfile.

5.5.4 U604121001: Mismatch between On-line and Diskette Disk Utilities

Files that are created with the diskette disk utilities and which have special characters in them, such as underscores, are not readable with the on-line generic disk utilities when the system is up and running.

5.6 DIGIT COLLECTION

The constraints described in this subsection apply to DTMF/MF digit collection. The type of collection (DTMF or MF) is specified where necessary.

5.6.1 TR 2274: Single Digit Collections (8-Port DTMF Cards Only)

Using single digit end flags while performing DTMF digit collection may result in misplaced or unreported digits. The receiver requires processing time to detect a digit string, report the string to the generic software, and then reset itself for another collection. Collecting single digits as start/end designators between larger strings can result in missed digits because the DTMF receiver does not have sufficient time to reset before the next digit is entered. This situation can be aggravated when the digit timing does not match the optimum timing of 60ms of tone followed by 60ms of quiet. DRC 24/48 port cards function properly.

Resolution

Collect and store incoming DTMF digits as a single digit string. Digit fields 1 through 4 can store up to 40 digits; the ANI field can store up to 20 digits. Digit strings are reported to the host in either a DTMF Digit ($D1) report or as a segment in an Inpulse Rule Complete ($DD) report. Using these reports, the host application can parse digit strings into their functional groups, as required.

5.6.2 U507315157/TR 5157: Garbled MF Digit Reports Not Sent to Host

MF Digit ($D0) reports indicating garbled digits are not sent to the host when the Inpulse Rule performing the collection contains the reporting control tokens REP EACH or REP NEXT. The system sends an Inpulse Rule Complete ($DD) report informing the host that the Inpulse Rule was aborted, but does not send a subsequent $D0 report. All other conditions that cause an Inpulse Rule to abort generate an additional report explaining the cause. If you use the reporting control token REP END in the Inpulse Rule, the $DD report correctly contains a $D0 segment indicating that the MF digits are garbled.

If an Inpulse Rule with a REP EACH or REP NEXT token aborts while performing MF digit collection without generating an additional report, assume that the digit collection is garbled.

5.6.3 U607030001: ASIST and 4th Column DTMF

The current version of ASIST (V3.11) does not support 4th column DTMF. ASIST does not convert the 0 digit to A.

5.6.4 U607290001: Reenter Character Disables DTMF Collection Timers

When a Reenter Character is entered as the first digit before the DTMF Collection Control ($67) command's prompts finish playing, a DTMF Digit ($D1) Report is not issued.

5.7 INPULSE/OUTPULSE RULE PROCESSING

The constraints described in this subsection apply to values for Inpulse Rule tokens.

5.7.1 U503234961/TR 4961: RELEASE Inpulse Rule Requires Resource Type

You must specify a resource type when you use the Inpulse rule token RELEASE. If you do not specify a resource (IPRC, MRC, DRC, DTG, or CPA), the RELEASE token has no effect.

5.7.2 U608140005: RELEASE DTG Token Does Not Work

The RELEASE Outpulse rule token does not release the DTG/DTG-2 and causes the system to log an error during Inpulse rule execution.

5.7.3 U608090004: Outpulsing without OPC (Out Pulse Channel)

An FRM error message (Outpulsing without OPC) is generated by MVDC-T1 and Four Span T1/E1 cards while Outpulsing MF strings. An Outpulsing without OPC indicates that the port was found not to be linked to an Outpulse channel. This results in lost calls.

5.7.4 U511211001/TR 5009: Limited Support for RETAIN and RELEASE Token

The RETAIN token is supported for only the IPRC and DRC in the Inpulse rules, and only partially supported in the Outpulse rules.

The RELEASE token is supported in the screen manager for the resource types IPRC, MRC, DRC, DTG, and CPA, but not fully supported in the run time processing. There is also an inconsistency in that the resources DTG and CPA, are not relevant to the IP rules but are supported for the RELEASE token. Resources IPRC, MRC, and DRC are not relevant to OP rules, but are supported for the RELEASE token. It is not possible to add a resource type for only an IP or OP rule.

5.8 CALL PROCESSING

The constraints described in this subsection apply to call processing.

5.8.1 U407064606/TR 4606: DASS Ports Stuck in MAINT-NE State

DASS ports may become stuck in a MAINT_NE state.

Resolution

Clear a port by deactivating it and then activating it with the Port control function of the Card Maintenance submenu. Or, take the card out of service and then reactivate it.

5.8.2 U410264726/TR 4726: After Switchover, SLIC OGT Keeps Ringing

If a SLIC ICT (Incoming Trunk) is telerouted to SLIC OGT (Outgoing Trunk), and the SLIC OGT is ringing during a switchover, the SLIC OGT does not stop ringing when the SLIC ICT goes back on hook.

5.8.3 U412014797/TR 4797: DASS Ports Getting Stuck in CP_GUARD

When there are two inbound DASS2 pipes (30 ports each with the first 15 in and the second 15 out), the ports on the second pipe may become stuck in CP_GARD. The system uses the second 15 ports when all 15 ports in the first pipe are busy. If this condition persists and the CO tears down layer 3, the ports become unusable and no inbound calls are sent.

Resolution

Clear a port by deactivating it and then activating it with the Port control function of the Card Maintenance submenu. Or, take the card out of service and then reactivate it.

5.8.4 U503064939/TR 4939: Ringing a Port that is Off Hook

This condition involves SLIC ports (when class of service is A2) that go on-hook after every call. On an incoming call, a $72 command is sent to seize and ring the port. Subsequently, a $69 command is sent with Outpulse Rule 0 to connect the port to the incoming call. However, these two commands cause the port's ringer toggle bit to become out of synch (i.e., the $69 command toggles the bit in an attempt to ring the port), which is already ringing as a result of the $72 command. As a result, the ports ring when they should not, and do not ring when they should.

5.8.5 U503284968/TR 4968: Disconnect Fails Unless Port Goes Through Stable

A voice path must be established between incoming and outgoing ports (both ports are CP_STAB) in order for those ports to successfully disconnect.

5.8.6 U505085035/TR 5035: Multiple Host and High Load Causes System Failure

Using an Ethernet system /Host interface with up to four hosts and high loads may cause the system to fail. Higher loads may support even fewer host connections.

5.8.7 U505115041/TR 5041: Interval between Seizure and Wink

One of the fields in Trunk Timing configuration is the Wink Send. For E1, this is the time period of the delayed dial signal. Tests have shown that this is about 60ms as opposed to the 30ms stated in the specifications.

5.9 COMMAND/REPORT PROCESSING

The constraints described in this subsection apply to all host-issued commands and received reports.

5.9.1 U406284589/TR 4589: ADLC Polling Protocol Errors Corrupt Messages

ADLC polling protocol errors can corrupt messages during poll timeout times. The messages are not retransmitted.

5.9.2 U505105037/TR 5037: SIT Tone Detection Failure

The SIT tone for the North American DTG and CPA is not reported correctly. The SIT tone (4C8) is reported as Dial Tone in the $DA reports.

5.9.3 U507315159/TR 5159: Appending Digits via the $67 Command

When appending an odd number of digits to a field, which already contains an odd number of digits, the last digit of the first string and the first digit of the last string are lost. Two zeros are added to the end of the string to provide the correct number of digits.

Resolution

To avoid this condition, use two digit fields for digit storage instead of appending digits to an existing field.

5.9.4 U507315160/TR 5160: Number of Digits to Collect ($67 Command)

You can use the $67 command to collect up to 40 digits. Specify the number of digits that you want to collect in the Digit Collection Control (byte offset 9) byte. Command processing does not currently check this value to verify that the number is less than 40. If you specify a number

greater than 40, the system still attempts to collect only 40 digits. The command is not rejected with a Network Status byte value of $2C, as would be expected.

Resolution

Specify 40 or less in the Digit Collection Control byte.

5.9.5 U507315161/TR 5161: Inpulse Rule Complete ($DD) Report Processing

A $DD generated when an Inpulse Rule aborts due to a CPA exhaust condition, does not correctly specify the cause for the abort. The report indicates that the rule aborted because no Outpulse channels were available (T = 1 in the Inpulse Rule/DVC Port byte offset 10). However, the CPA exhaust condition is identified, by a Resource Allocation ($D6) report, which specifies a resource limitation for the CPA resource group.

5.9.6 U508175187/TR 5187: $67 Command and Inpulse Rule—Digit Collection

When the caller enters digits, it appears that a combination of the $67 command and Inpulse rule is being processed. The digits that are reported are the first three digits that the caller input. Those digits are reported in a $DD report and are also stored in field 1.

A second collection command (via the Inpulse rule specified in the $6A command) does not completely override the first collection command (in the $67 command). The DRC collects only 3 digits and reports them to the host, per the $67 command, but then stores those digits in field 1 per the Inpulse rule.

Resolution

Have the application remove the receiver attached with the $67 command when the outgoing hangs up. Then send the $6C, and then the $6A to start the Inpulse rule.

5.9.7 U603210001: NSB 02 Returned for $65 and $49 Commands

A Network Status Byte of 02 (Invalid command function ID) is returned by the Subrate Path Control ($65) Command when the $65 command contains 82 destinations. The ISDN Port Control ($49) Command also returns a Network Status Byte of 02 if the $49 command contains between 258 and 261 bytes.

5.10 INITIALIZATION

The constraints described in this subsection apply to system initialization.

5.10.1 U311104202/TR 4202: System Sends $DC Report too Early

After a warm start, the system sends a ($DC) report to start call processing before IPRC prompt downloading is complete.

Resolution

You can use the feature flag and not start call processing until the system receives a command from the host ($C0 04) to send that command when the IPRC changes from Maintenance to Active.

5.10.2 U701090002: $9 Timeouts on Cold Boot Download

On cold boots with various cards in the database the system receives $9 timeouts during broadcast downloads on various cards.

Resolution

Recovers automatically with directed download.

5.11 NBC-3

The constraints described in this subsection apply to the NBC-3 card.

5.11.1 U704090001: Loss of External BITs Clock Does Not Cause Alarm

If the system is using an external BITs clock, and the clock is lost, the system selects internal timing and generates the error “FRM020 (NBC External Reference Signal not Present),” instead of the error “FRM023 (NBC Cannot Sync on External Reference).” Also, a major alarm is not generated.

If the external BITs clock is restored, you must re-select “External Clock” through the System Administration console or through SNMP.

5.11.2 U704140001: Cards Not Downloading After DID

If the error message FRM341: NBC error - Comm Bus Interf- DID err is received, cards in the system may fail to come into service. This usually occurs because a card is in a slot that is not defined for that card. When this is the case, other cards, even if properly defined, may also fail to come into service because device polling is discontinued.

Resolution

Cards can be activated through the Card Maintenance screen, or polling can be reactivated by re-booting the system with the offending card removed.

Normally, a Device Identification (DID) signal is asserted on the Communications Bus by a card to request initialization from the NBC. The card is then initialized by the NBC and comes into active service. If the card fails to initialize, it continues to assert DID on the Communications Bus and its green LED is lit. This condition occurs when one of the scenarios below is true. The corrective action is listed for each case.

- A card in the backplane does not come into service (possible card failure). Remove any Out of Service cards from the backplane.
- A card is inserted into a slot that does not have a card defined for it in the system data base. Remove the card or define that card from the system administration Card Maintenance utility.

- A card is inserted into a slot and connected to the backplane, but is defined as an incorrect card type in the data base. Remove the card and replace it with the correct type or update the card definition in the data base from the system administration Card Maintenance utility.
- A card is marked a Out of Service in the Card Maintenance Utility. Change the card status or remove the card.

It is good system practice to remove any Out of Service card from the backplane to optimize system performance and further guard against the conditions above.

When NBCs, DTGs, and BRCs are in Standby mode, their green LED is lit.

5.12 DTG AND DTG-2

The constraints described in this subsection apply to the DTG and DTG-2 card.

5.12.1 U608140004: Problems with Tone Ports during Switchovers

If the fuse is blown on the DTG-2 and there are no active tone cards in the system during switchover, the following conditions occur:

- On VCO/20 systems, the Standby side fails when the system attempts to remove tone ports from call chains.
- On VCO/80 systems, the system hangs during file synchronization and you cannot access screens from the Standby side.

5.12.2 U610020003: DTG/DTG-2 Add/Delete during Outpulsing

If you add or delete a tone generator card while another tone generator is outpulsing, the switch may be unable to do further outpulsing and may even fail.

Resolution

Do not add or delete tone generator cards while the switch is processing calls.

5.13 FOUR SPAN CARDS

The constraints described in this subsection apply to the MVDC-T1 and Four Span T1/E1 cards.

5.13.1 U507201007: Processing WINK Command

When the Four Span T1 is configured as FX0-LX, the card processes a WINK command after it seizes out.

Resolution

Do not use a WINK in an Outpulse rule when Four Span T1 cards are configured as FX0-LX.

5.13.2 U603151001: Inconsistent Handling of Channels on Four Span E1

With Four Span E1 cards, resource groups can include channel 17, depending on whether the card spans are provisioned for CCS/31B or CAS. In CCS/31B mode, channel 17 is a bearer channel and can be added to a resource group. In CAS mode, channel 17 is used as the D-channel, and therefore, cannot be in a resource group.

After a Four Span E1 card is added and configured, you can change the mode from the Resource Group Configuration screen. However, the system does not automatically remove channel 17 from the resource group when the mode is changed from CCS/31B to CAS, or automatically add channel 17 to the resource group when the mode is changed from CAS to CCS/31B. When the span is changed from CCS/31B to CAS, all call attempts on channel 17 fail, because channel 17 is no longer a bearer channel. When a span is changed from CAS to CCS/31B mode, bandwidth is wasted.

Resolution

Verify that resource groups properly reflect the nature of channel 17 when changing the mode of a Four Span E 1 card span between CCS and CAS.

NOTE: The System Administration console and SNMP do not prevent users from configuring bearer-channel signaling and timing parameters for channels that are not truly bearer channels. This applies to channel 17 for CAS mode and channel 1 for both modes. (Channel 1 is used for framing.) Users may find this misleading, but it is harmless.

5.13.3 U604260001: Testing Patterns from TTS-3 Analyzer Causes Errors

MVDC-T1 and Four Span T1/E1 cards perceive the test patterns from a TTS-3 Analyzer as incoming seizures and generate FRM373 and FRM102 errors.

Resolution

Remove the test boxes before connecting the system to the network and processing calls.

5.13.4 U606101001: MVDC-T1s/Four Span T1s Generate FRM90 before Download

Multiple iterations of the FRM090 message (Card restored, card alarm cleared) are generated while MVDC-T1 and Four Span T1 cards are downloading, coming into service, and going active.

5.13.5 U606241001: Four Span T1/E1 Internal Errors During Boot

During the broadcast download cycle, Four Span T1 and Four Span E1 cards intermittently generate an internal error code 1. The broadcast download fails, but the system recovers and successfully performs a direct download to each card.

Resolution

None. This problem does not affect service.

5.13.6 U610160001: PRI failures from MVDCT1

During boot up the generic intermittently reports an alarm for D-Channel failures on the MVCD-T1, even though the switch does not have PRI, PRI/N or NFAS installed. This problem does not affect service.

5.13.7 U611140005: Problem with Four Span T1 on Switchover

If you change the mode on a Four Span T1 card from active to maintenance, and then to out of service, from the Active side of the system, the changes also occur on the Standby side. However, if you change the mode back to active from the Active side, the card stays in maintenance mode on the Standby side. If the switch changes over while this condition exists, calls are lost.

Resolution

From the Active side of the switch, change the mode back to out of service, to active, to maintenance, and then back to active. This causes the Standby side to change from maintenance to active mode.

5.13.8 U611250003: FRM523 Queue Overflow

The messages “FRM523 Queue Overflow, Data Lost” and “Data lost on Screen_Msg Queue” may appear when the system broadcasts a download to a large number (such as 16) of MVDCs.

5.13.9 U611260001: Rotary Resource Group

If the outgoing Four Span T1 trunk resource groups are set to ROTARY search, the ports in the resource group get stuck in CP_WTFSUP.

Resolution

Use CYCLIC search.

5.13.10 U704140004: Display ACTIVE while Downloading

Following a warm reset, the 4xE1 cards display ACTIVE while downloading.

5.14 MISCELLANEOUS CARD ISSUES

The constraints described in this subsection are miscellaneous card issues.

5.14.1 U409124662/TR 4662: UTC Firmware Causing T1 INIT Code F Error

The UTC firmware does not initialize the serial port in order to disable it. This might cause T1 INIT CODE F errors. Summa Four recommends that all firmware be checked to make sure that the serial port is disabled.

5.14.2 U505105038/TR 5038: Reorder Tone is Not Reported/Detected (UK)

The Call Progress Analyzer (CPA) in use in the UK does not detect the Reorder Tone from the Dial Tone Generator (DTG).

5.14.3 U507195126/TR 5126: A2 SLIC Stuck in CP_OUTPULSE

A SLIC permanently goes into a CP_OUTPULSE if an A2 SLIC goes on-hook, even momentarily, before a call is routed to it. Subsequently, no hook flashes are reported for the SLIC.

5.14.4 U603021003: IPRC Load Problems with more than 22 Seizures

Load seize on Inpulse rules with record and speak tokens at 22 seizures cause IPRC cards to go OOS.

5.14.5 U604040002: IPRC Load Problem

If sixteen simultaneous seizures occur while the IPRC is recording and playing temporary prompts, on systems configured withMFCR2 and Four Span E1 cards, which use Call Associated Signaling (CAS) with CRC4 set to ON, the IPRC card goes out of service and causes the system to fail.

The IPRC also goes out of service and causes the system to dump and reboot when an Inpulse rule, used to collect DTMF or MFCR2 digits, is followed by an Inpulse rule, used to record a prompt with the GOTO RULE or DO IRULE token.

5.14.6 U608090005: Erroneous Minor Alarms on Four Span E1

Occasionally, the minor alarm LED (yellow) stays illuminated after the alarms are cleared on all spans of the Four Span E1 card. The Card Display screen correctly displays the alarms as cleared.

5.14.7 U608140002: Remote Alarm Problems with DPNSS Ports

When a remote alarm occurs during a DPNSS to DPNSS call, the generic keeps the call in a stable state and while clearing the alarm, the port gets stuck.

5.14.8 U610110003: Subrate Switch Card Download Broadcast

Subrate Switch cards do not simultaneously download when you cold boot the system.

5.15 MULTIPLE HOST CONNECTIONS

The constraints described in this subsection apply to SDS/VCO systems connected to multiple hosts.

5.15.1 U605091001: Major Alarm Not Set on Loss of Hosts

The system does not generate the following alarm when all external host connections are lost and TeleRouter has been enabled:

ALM011: No Hosts Available

If TeleRouter is disabled after being enabled, the alarm is still not generated unless a new Ethernet host is configured and all host connections are then lost.

5.16 TELEROUTER

The constraints described in this subsection apply to systems with the Telerouter option.

5.16.1 U606041001: TeleRouter $D5 (Routing Action) Reports

Telerouter $D5 (Routing Action) Reports do not appear in the system trace file, but they are sent to the host.

5.16.2 U606030001: Access of TeleRouter Routes

When a Routing screen is displayed, which shows all of the routes in a table, you cannot access the last two routes. The “D” and “C” commands will give an “Invalid Route” error. The “T” command will find “NO MATCH” even though the screen displays the route and pattern.

Resolution

Add the patterns “FFFE” and “FFFF” to the end of the route table.

5.17 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

The constraints described in this subsection apply to SNMP operation.

5.17.1 Functions Not Supported

The Management Information Base (MIB) does not support the functions on the following System Administration screens.

- Disk Utilities Menu
- Print/Display System Log File Submenu
- Print/Display System Trace File Submenu
- Set Up Path Submenu
- Conference Display Screen
- Service Circuit Test Utility Screen
- Test Port Card Screen
- Call Generation Ports Display Screen
- Call Progress Tone Monitor Screen
- System Trace Configuration Screen

In addition, the MIB does not support the Routing Statistics Display function on the TeleRouter screen.

5.17.2 U601301007: Host Fails to Establish TCP/IP Connection

If the Ethernet host is configured with the SNMP hostEntry object, the host cannot establish a TCP/IP connection.

Resolution:

Configure the Ethernet host through the System Administration console screen.

5.17.3 U602200001: SNMP Causes Queue Overflows

The SNMP agent causes several queues to overflow when you add or modify an MVDC-T1 or Four Span T1/E1. The overflows occur during card table and port table updates.

Resolution

Add and modify MVDC-T1 or Four Span T1/E1 cards from the System Administration console.

5.17.4 U604241001: Card Activate Errors Not Returned in SNMP

You can activate a card through the System Administration console or through SNMP. In either case, when a card is activated and the card type does not match what's in the database, an error message appears on the System Administration console and in the log, but not in SNMP. This is because the MIB variable for the error status is not updated.

5.17.5 U606051001: Zero Value for hostRemotePort Not Accepted

If you assign the value of zero to the object host Remote Port, in SNMP, it will fail. This should not happen because zero is a valid value.

Resolution

Set the remote port field in the Host Configuration screen to zero on the System Administration console.

5.17.6 U606051002: Zero Value for hostType Not Accepted

Assigning the value of zero to the object hostType in SNMP causes the following error message:

hostType.2 Number: unused(1) = 'bad value'

Assigning the value of zero should clear all of the objects of the host configuration entry.

Resolution

Use the Select key on the system console to toggle through the hostType options and clear the fields on the screen.

5.17.7 U606061002: Adding Same Card in Resource Group Twice

If you inadvertently add the same card twice into a resource group through SNMP, and then delete it through the system console, the data base is corrupted.

Resolution

Never add the same card into a resource group twice.

5.17.8 U606201001: Configuring Hosts

When a new host is added to the host table through SNMP, the Host Alarm State is incorrectly set to OFF. This creates a problem because the switch does not allow a host to connect when the alarm state is OFF.

Resolution

Configure new host settings through the System Administration console.

NOTE: SNMP can update existing host configurations successfully.

5.17.9 U606201002: Committing Changes to the Data Base

Changes to MIB objects accumulate in the system until the appropriate EntryStatus object is set to VALID. There is a limit on the maximum number of outstanding changes, and when the limit is exceeded, changes are discarded, and the following error messages appear on the System Administration console:

```
FRM340: CODE Error – adm_api.c, 516:    cannot grow queue: 416
FRM340: CODE Error – adm_card.c, 795:   cannot buffer attr: 21
```

The limit is not easily quantifiable.

Resolution

Make changes to tables by periodically setting the EntryStatus to VALID (for example, every five to eight rows), depending on the number of attributes changed.

5.17.10 U606211001: Modifying TimingCard Objects

If masTimingSource has been defined as internal or external, SNMP incorrectly allows the user to modify masPrimaryTimingCardPhyAddr and masSecondaryTimingCardPhyAddr. A subsequent GET on masPrimaryTimingCardPhyAddr or masSecondaryTimingCardPhyAddr returns the value zero. (Zero is returned whether you modify the object or not.)

Resolution

Do not modify masPrimaryTimingCardPhyAddr or masSecondaryTimingCardPhyAddr when masTimingSource is internal or external.

5.17.11 U608130005: SNMP Resource Group Configuration Problem

If you use SNMP to configure resource groups on redundant systems, the port.tbl file gets corrupted and ports are missing from resource group.

5.17.12 U609250016/U609250017: SNMP Modification Tables

(See also U609250018.) The following SNMP tables do not get updated:

- dtgCardTableLastModified, when you added or deleted an NBC-3 card
- nbcTableLastModified, when you deleted a DTG-2 card

5.18 ETHERNET

The constraints described in this subsection apply to Ethernet.

5.18.1 U608080006: Problem with Ethernet Install

If you attempt to update the gateway routing tables before Ethernet is installed and enabled, the gateway routing tables get corrupted.

Resolution:

Install and enable Ethernet before you attempt to update the routing tables.

5.19 ISDN ISSUES

The constraints described in this subsection apply to PRI and PRI/N ISDN configurations.

5.19.1 U401054297/TR 4297: ISDN Ports Remain in DISC_REQ State

If phantom-to-DASS port calls are set up and torn down periodically for all the ports on a card, the DASS ports may become stuck in a CP_GARD, NORMAL, DISC_REQ state. If this happens to only a few ports on a card (some ports remain idle), incoming call attempts from the PSTN fail and no indication of the call is received. Outgoing calls from the SLIC connect but the DASS ports remain in a CP_WTSUP, O_INITED state.

5.19.2 U707300003: ISDN Message Type SETUPACK is Missing

ISDN message templates selection does not allow you to select SETUPACK, which is required for Overlap Sending and Receiving responses.

5.20 INTERNATIONAL ISSUES

Note: In future releases, issues of this nature will be documented in a new International Release Notes *document.*

5.20.1 U505125048/TR 5048 Chile CPA Does Not Detect any Tones

The Chile Call Progress Analyzer (CPA 8.51) used with the Dial Tone Generator (DTG 1.02) does not detect Dial, Busy, Ring, and Congestion tones, and reports CPA Internal Errors (Code 44).

5.20.2 U505155052/TR 5052: Finland CPA Does Not Detect Tones

The Finland Feature Package (CPA 8.70 with DTG FW V1.00) does not detect tones. All tones are detected as Voice Detect and Voice Cessation.

5.20.3 U505165056/TR 5056: Colombia DTG Does Not Outpulse Digits

The Colombia Dial Tone Generator (DTG V1.00) used with Call Progress Analyzer (CPA V8.70) does not outpulse digits.

5.20.4 U505255069/TR 5069/TR 5068: Colombia CPA Tone Detection Problems

The Colombia CPA (V19.02) detects the SIT (04D4) tone intermittently. SIT tone is detected as PAGER CUE, VOICE, and VOICE CESSATION tones. RING tone is detected only 60% of the time; REORDER tone 40% of the time. SPECIAL REORDER tone is not detected at all.

5.20.5 U508075168/TR 5168: Multiple MFCR2 Cards with Colombia V19.02

When you add more than one MFCR2 board to a system, running Colombia V19.02, some of the calls might fail to seize ports. Occasionally, the boards fail and need to be reset before they start working again.

5.21 JAPANESE ISDN

5.21.1 U704040003: ISDN Disconnect Control Fails

The ISDN disconnect control byte in the $49 command has no effect. All disconnects are reported to hosts.

Appendix A
REPLACING PROMS AND PLDS

A.1 INTRODUCTION

This appendix describes the procedures for installing new firmware and programmable logic in circuit cards. Firmware is shipped in the form of programmable read only memory (PROMs), dual in-line packages (DIPs), integrated circuits (ICs) for through-hole mounting, and plastic leaded chip carriers (PLCC) for surface mount.

Programmable logic is shipped in the form of programmable logic devices (PLDs), DIPs for through-hole mounting, and PLCCs for surface mount.

PROMs are labelled with configuration data which should be checked, prior to installation, against the firmware requirements contained in *Section 2*. PLDs are labelled with their LP identification number.

Instructions for removing and replacing through-hole and surface-mount PROMs and PLDs are in the following sections.

A.2 REMOVING AND REPLACING THROUGH-HOLE PROMs and PLDs

The following sections provide information about removing and replacing through-hole PROMs and PLDs. Refer to the appropriate technical description for the physical locations of the PROMs and PLDs on each circuit card.

A.2.1 Removing Through-Hole PROMs and PLDs

To remove a through-hole PROM or PLD, follow these steps.

1. If the circuit card is currently installed in the system, follow the removal and replacement procedures in the appropriate technical description. Be sure to also locate affected circuit cards kept as spares.

   CAUTION: Observe antistatic precautions near circuit cards. Wear a ground strap connected to the equipment frame whenever servicing or cleaning circuit cards (ground points are indicated by labels on the system front).

2. Remove the PROM to be replaced from the circuit card. Use a PROM removal tool to grasp the integrated circuit and pull it straight up and away from the socket.

   CAUTION: Avoid using devices, such as screwdrivers, to remove PROMs. These devices can damage PROM pins and scratch the circuit card.

3. Remove the PROM chip from the shipping package. Refer to *Section 2* to verify that the label on the chip matches the software requirements.

A.2.2 Replacing Through-Hole PROMs and PLDs

To replace a through-hole PROM or PLD, follow these steps.

1. Before installing the new chip, verify that its pins are all evenly spaced and vertically aligned. If necessary, align the IC pins properly prior to installation. To align the pins, you can either use a commercially available pin-straightener tool, sized for a 28-pin DIP device, or you can lay the PROM or PLD on its side and gently press the top edge, being careful not to press on the pins (Figure A.1). Repeat this procedure for the other row of pins.

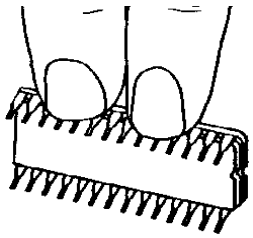


Figure A.1: Aligning PROM or PLD Pins

2. Orient the PROM or PLD chip so that the notch in the chip (Figure A.2) faces the notch on the circuit card.

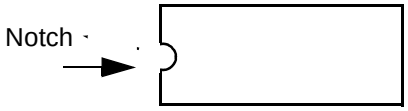


Figure A.2: Notch Orientation for Integrated Circuit

3. Carefully insert the pins on one side of the PROM or PLD chip into holes on the correct side of the socket (see Figure A.3).

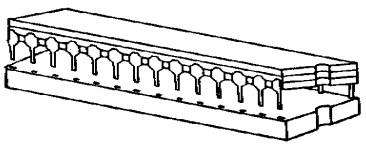


Figure A.3: Inserting Pins in One Side of Socket

4. Insert the pins on the other side of the PROM or PLD chip into holes on that side of the socket (see Figure A.4).

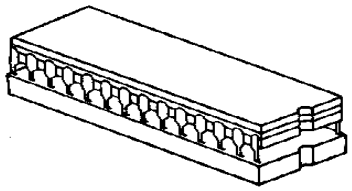


Figure A.4: Inserting Pins in Other Side of Socket

NOTE: If the pins are not aligned with the socket holes, remove the PROM or PLD chip and straighten the pins (see Step 1). After realigning the pins, repeat Step 2 through Step 4.

5. Carefully examine all the pins on the PROM or PLD chip. Be sure that none of the pins are bent or touching one another.
6. With all of the pins inserted into the socket holes, apply gentle and even pressure to the top of the chip until it is fully seated in the socket.
7. Re-install the circuit card in the system or return the card to spares stock.

A.3 REMOVING AND REPLACING SURFACE-MOUNT PROMs and PLDs

The following sections provide information about removing and replacing surface-mount PROMs and PLDs. Refer to the appropriate technical description for the physical locations of the PROMs and PLDs on each circuit card.

CAUTION: Make sure you use the proper tool to remove surface mount PROMs and PLDs, or you may damage the board.

A.3.1 Removing Surface-Mount PROMs and PLDs

To remove a surface-mount PROM or PLD, follow these steps.

1. If the circuit card is currently installed in the system, follow the removal and replacement procedures contained in the appropriate technical description. Be sure to also locate affected circuit cards kept as spares.

   CAUTION: Observe antistatic precautions near circuit cards. Wear a ground strap connected to the equipment frame whenever servicing or cleaning circuit cards (ground points are indicated by labels on the system front).

2. Use the surface-mount chip removal tool, provided by Summa Four, Inc. to remove the PROM or PLD that is to be replaced on the circuit card. To remove the PROM or PLD chip:
   a. Spread or compress the tool legs so the tongs fit into the slots of the chip carrier socket.

b. Insert the tool tongs into the slots of the socket, and push firmly so that the tool butts on the socket.

c. Place the thumb and forefinger on the tool's grip. Squeeze the thumb and forefinger together to remove the chip from the socket.

3. Remove the PROM or PLD chip from the shipping package. Refer to *Section 2* to verify that the label on the chip matches the software requirements.

A.3.2 Replacing Surface-Mount PROMs and PLDs

To replace a surface-mount PROM or PLD, follow these steps.

1. Before installing the new PLD, verify that the pins are all evenly spaced and properly aligned. If necessary, use tweezers to carefully align the IC pins prior to installation.
2. Align the notch or chamfered edge on the PLD to the silkscreened dot on the circuit card (see Figure A.5).

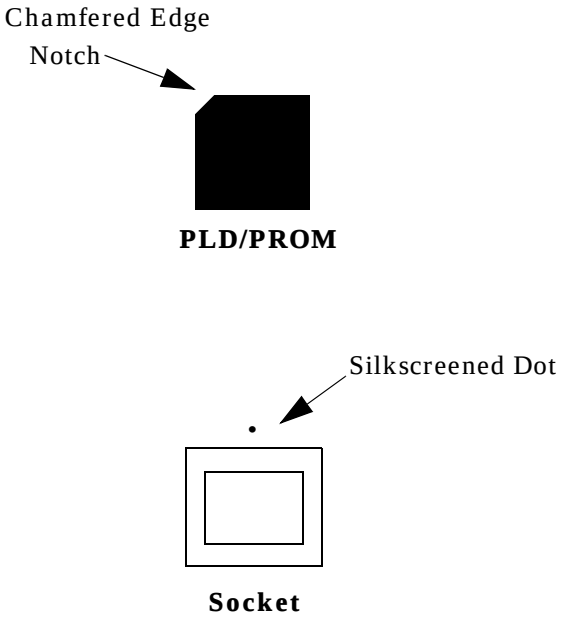


Figure A.5: PLD Alignment

3. With all pins aligned to the pins of the socket, apply gentle, even finger pressure to the top of the chip until it is fully seated in its socket. This completes the installation of the surface mount chip.
4. Reinstall the circuit card in the system or return the card to spares stock.

Appendix B
RE-INSTALLING V4.0 FSR02

B.1 INTRODUCTION

This section describes the procedures for installing Generic V4.0 FSR02 or V4.0 FSR02 PUN22 on systems previously running V4.0 FSR02. This is provided for users who want to re-build their system.

If you are upgrading an earlier system see *Section 3***.**

CAUTION: This section provides detailed installation procedures for loading system software. Review the material in this section prior to installing the software. If you encounter any problems during the installation, contact Summa Four.

B.2 REFERENCE

Before you install the software, make sure you read all the material contained in this section. You may also want to refer to the following documents:

- SDS and VCO *Installation Manual*
- Technical Description: *Network Bus Controller 3 (NBC3) Card*
- Product supplements for optional software, including
  - *VCO V4.0 Management Information Base (MIB) Reference Guide*
  - *VCO V4.0 Management Information Base (MIB) User's Guide*
  - *TeleRouter Reference Guide*
  - *ISDN Supplement*
  - *ISDN NET5 Supplement*
  - *Ethernet Supplement*
  - *DPNSS Supplement*
  - *DASS2 Supplement*
  - *IPRC Supplement*
  - *Japanese ISDN Supplement*
  - *NET5 Supplement*
  - *NTDASS2 Supplement*
  - Applicable Country Supplements

B.3 OVERVIEW OF THE INSTALLATION STEPS

The following provides a brief overview of the procedure to install the Generic V4.0 FSR02 software on your system. The steps are explained in detail in *Section B.5* through *Section B.10*.

Installing the Software

1. The V4.0 FSR02 Generic software is installed on the A-side. Refer to *Section B.5*.
2. After the Generic is installed, SNMP Software (Ethernet), and optional software is installed. Refer to *Section B.6* and *Section B.7*.
3. If installing on a redundant system: after installing the software on the A-side, the software is installed on the B-side. The procedure is the same as the A-side installation. Refer to *Section B.8*
4. If you have purchased additional time-slots, the Time-Slot Allocation License must be updated so that the system recognizes the additional time-slots. Refer to *Section B.8*.
5. The MIB files are installed on the host computer. Refer to *Section B.10*.

CAUTION: Do not install the MIB–Supplemental Disk software on the switch. The MIB software is for installation on a network management station (NMS). Refer to the section The MIB–Supplemental Disk Files, for information on moving the MIB software on your NMS. Do this after completing the installation of V4.0 Generic software on the switch.

B.4 WHAT YOU NEED

You need the following software to do the generic software installation. Make certain you have:

- Four diskettes labeled as follows:

  VCO SYSTEMS V4.0 FSR02 PUN22
  GENERIC
  DISK *x* OF 4

  Note: The *x* is a number from 1 to 4. The number indicates the sequence in which the diskettes must be loaded when you install the generic software.

- Diskettes containing the installation utilities for any optional software packages, for example, TeleRouter, ISDN-NFAS and/or Ethernet.
- A system printer with paper, that is powered on, so you have a printed record of the installation process.
- Time-Slot Allocation License for additional time-slots (optional).
- Diskette labeled: MIB - Supplemental Disk Files (optional).

For redundant systems, be sure you can connect a system console to both system controllers. Depending on your equipment's arrangement, you can:

- Set up a separate system console for each controller (A- and B-side).
- Use an A/B transfer switch wired to both system controller CPU-TM front panels to switch access.
- Physically remove and reconnect the system console cable from one CPU-TM front panel to the other.

B.5 INSTALLING THE SOFTWARE

The following is the procedure for installing the Generic V4.0 FSR02 on new systems.

CAUTION: This procedure reformats the C: drive. If this is not a new system install, refer to *Section 3*.

On Disk 1, the Install/Configure Basic System Software option installs the generic software and downloads files onto the hard disk.

Note: Verify that the CPU firmware is Version 4.02 before you proceed with the installation.

The instructions in the following steps assume that the system console is connected to the CPU-TM of the side being installed.

To install the generic software on your system, do the following:

1. Move the AAC switch to the A position.
2. Insert Disk 1 into the A-side floppy diskette drive.
3. Connect or switch the administration console to the A side CPU-TM, or go to the A-side system console.
4. Power on the A-side.
   After the system performs diagnostic tests, the Installation Utilities menu appears (Figure B.1), with the cursor located in the Enter Selection data entry field.

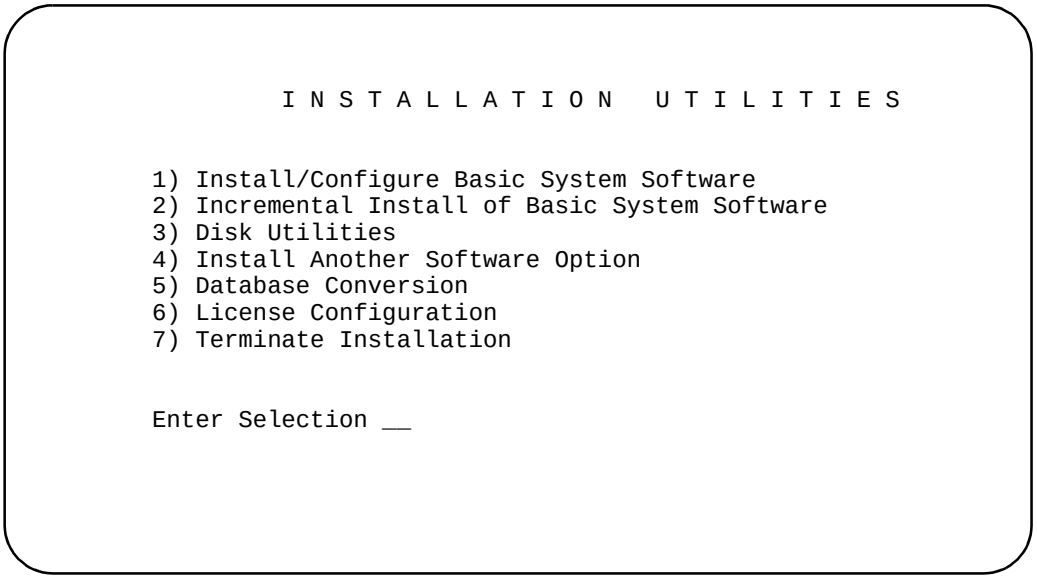


Figure B.1: Installation Utilities Menu

5. Do you want to reformat the hard drive?
   a. If you do not want to reformat the hard drive, Type **2**. This will take you to Step 7, below.

      Note: Only Disk 1 contains the installation utilities. Booting the system with Disk 2 automatically loads the generic software into the system memory, but does not load the software onto the hard drive. You would probably choose to boot from disk 2 if you had a drive failure or other reason not to use the hard drive.

   b. If you want to reformat the hard drive, Type **1** (for Install/Configure Basic System Software), then press the **Return** key.

      The following message appears:

      Do You Wish To Back-Up The System Data Base? (Y/N) =N?_

6. Press the **Return** key (this defaults to N).

   The following verification message appears:

   The installation process reformats the device C:

   All information will be erased

   Press return to continue

   Press the **Return** key to continue. The following message appears:

   Formatting device C:

When complete, the following message appears:

Insert disk 2 of Installation Set

Press return to continue

Remove the current diskette from the drive.

7. Insert Disk 2 and press the **Return** key. The system copies the files from Disk 2 to the C: drive in the /BOOT, /DBASE, /LOG and /TRACE directories.
8. When all the files from disk 2 are copied, the following message appears:

   Insert disk 3 of Installation Set

   Press return to continue

   Remove Disk 2 from the drive, insert Disk 3 and press the **Return** key. The system copies the files from Disk 3 onto the C: drive.
9. When all the files from disk 3 are copied, the following message appears:

   Insert disk 4 of Installation Set

   Press return to continue

   Remove Disk 3 from the drive, insert Disk 4 and press the **Return** key. When the installation is complete, the Installation Utilities menu appears (Figure B.1).
10. Remove Disk 4 from the drive.
11. a.) If you are *not* installing optional software, proceed to *Section B.8* to install the software on the B-side.

    b.) If you have optional software packages to install, such as Telerouter, ISDN-NFAS, or Ethernet, type **4**, Install Another Software Option, then press the **Return** key.

    The following message appears:

    Insert Another Install Disk

    Press Return To Continue

    Instructions for installing optional software after you have installed the Generic are provided in *Section B.6*, installing Ethernet, and *Section B.7*, installing optional software. The product supplement also contains installation information. Proceed to the appropriate section.

    NOTE: When you install a software option (such as TeleRouter, etc.) on a system, the installation process makes changes to the nonvolatile RAM (NVRAM) on the CPU. These changes make operation of software options specific to the CPU on which you installed the options. For this reason:

    - *Software options must be installed on both system controllers in a redundant system.*
    - *Software options must be reinstalled if the CPU is replaced. Although the data base information resides on the hard disk, a new CPU is unable to access this information.*

    Because of the reliability of the CPU, failures requiring replacement are very rare occurrences.

B.6 INSTALLING ETHERNET SOFTWARE FOR HOST AND SNMP COMMUNICATION

Install the software for SNMP trap message reporting and set up the network parameters by performing the following steps:

1. Insert the Ethernet diskette into the Side A drive and press the Reset button. After the system loads the Ethernet files from the diskette, the Ethernet Installation Utilities menu appears with the cursor located in the Enter Selection field (see Figure B.2).

```
                    I N S T A L L A T I O N   U T I L I T I E S


        1) Install/Configure Ethernet Optional Package
        2) Enable/Disable Ethernet Option
        3) Disk Utilities
        4) Install Another Software Option
        5) Database Conversion
        6) License Configuration
        7) Terminate Installation


        Enter Selection 1
```

Figure B.2: Ethernet Installation Utilities Menu

2. Type **1** and press **Return**. The following message appears:

   Do You Wish to Back-Up the System Data Base (Y/N) =N?

3. Press the **Return** key (there is no data base to back up) and proceed to Step 4.

   The Ethernet Configuration screen appears (see Figure B.3).

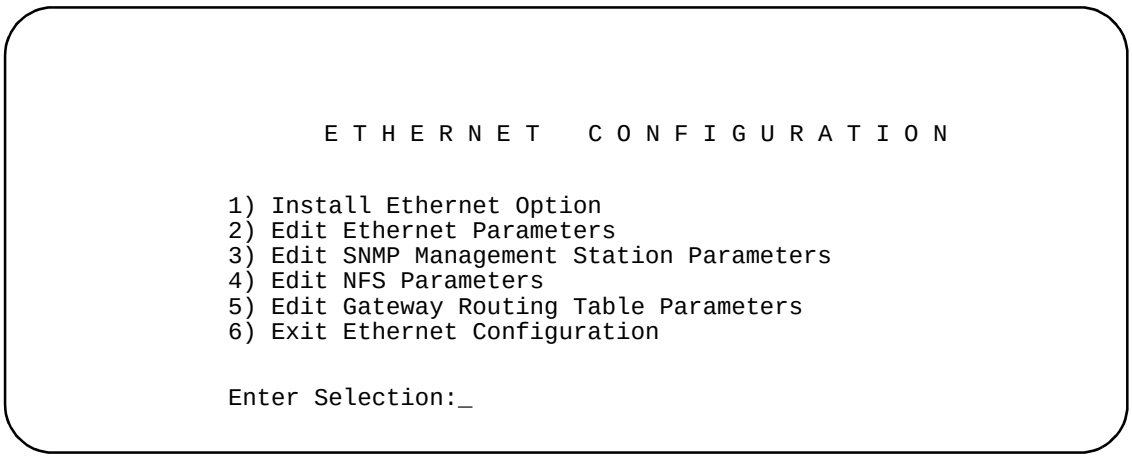


Figure B.3: Ethernet Configuration Menu

4. Type **1** and press **Return**. The following message appears:

   Copy A:/BOOT/ETHERNET.EXE

   1 files(s) copied

   Ethernet Option Enabled

5. To set the Ethernet Parameters, type **2** and press **Return**. The following message appears:

   System Internet Address = 107.3.254.98?

   IMPORTANT NOTE: The Ethernet and Internet address numbers that you see in the screen messages in this section are only examples. In your system these numbers are replaced by numbers that represent your system addresses.

6. Set the Internet Address of this system and press **Return**.

   Set System Internet Address To 107.3.254.98 (Y/N) =Y?

7. If you change the address, you are prompted to confirm your new address. Type **Y** to confirm your selections. The following confirmation message appears:

   System Internet Address Configured

8. Set the System Subnet Mask, or press **Return** to accept the displayed value.

   After you complete this step you can connect a remote console to your system via Telnet.

9. a. If you are not going to manage this system with SNMP, go to Step 15.

   b. If you are going to manage this system with SNMP, type **3** and press **Return** to set the SNMP Management Station Internet address. The following message appears:

      SNMP Management Internet Address = 0.0.0.0?

10. Set the Internet address to the address of the system that you are using as the NMS. Press **Return**. The following message appears:

    Set SNMP Management Internet Station Address To 189.7.107.44 (Y/N) =Y?

11. Type **Y** to confirm your selections. The following confirmation message appears:

    SNMP Management Station Internet Address Configured

    After you complete this step, the system will report SNMP trap messages to the NMS that you selected.

12. a. If you are not going to boot your system over the network, go to Step 15.

    b. If you are going to boot your system over the network, go to Step 13

13. Type **4** to set the Network File System (NFS) server parameters. The following selections appear one at a time. Enter the information for your system. Type **Y** and press **Return** after each selection.

    Enable NFS Access (Y/N) =Y?

    NFS Server Internet Address = 000.0.000.000?

    NFS Server Name =xxx?

    NFS Mount Directory Point #?

    Target System Name =

    Target System User Id =

    Target System Group Id =

    Target System Umask =

    Update NFS Configuration With Above Data (Y/N) =Y?

14. After you update the NFS configuration with the new data, the following message appears:

    NFS Configuration Updated

    The log files and database can now be saved to a remote location.

15. Type **6** to exit and press **Return**. The Installation Utilities screen appears (see Figure B.4).

16. To end the Ethernet installation, type **7** and press **Return**.

17. Remove the Ethernet diskette from drive A.

18. If you have more optional software packages to install, proceed to *Section B.7*.

19. If this is the last optional software package and you have a redundant system, the V4.0 software must be installed on the B-side, refer to *Section B.8, Installing Software on the B-Side*.

B.7 INSTALLING OPTIONAL SOFTWARE

The following section provides generalized instructions for installing an optional software package. For complete installation instructions refer to the supplement provided with the optional software.

To install optional software:

1. Insert the optional software diskette and press the **Return** key.

   If you are installing optional software such as Telerouter or ISDN-NFAS, the Installation Utilities menu specific to the optional software appears in place of *Option Name* in choices 1 and 2 (Figure B.4).

```
                    I N S T A L L A T I O N   U T I L I T I E S


        1) Install/Configure Option Name Optional Package
        2) Enable/Disable Option Name Option
        3) Disk Utilities
        4) Install Another Software Option
        5) Database Conversion
        6) License Configuration
        7) Terminate Installation


        Enter Selection 1
```

Figure B.4: Optional Software Installation Utilities Menu

2. To install and configure the optional software, type **1** and press the **Return** key. The following message appears:

   Do You Wish To Back-Up The System Data Base? (Y/N) =N?_

   Press the **Return** key (this defaults to N.) There should be no data base to be backed up at this time.

   The following messages appears for most options other than Ethernet:

   Copying A:/*Option Filename*.EXE...

   1 file(s) copied

   Option Name Option Enabled

3. If you are installing additional software packages, press **4** (to Install Another Software Option), and repeat the steps in this section.
4. After you install the last optional software package, type **7** and press the **Return** key. If you have a redundant system, the V4.0 software must be installed on the B-side, refer to *Section B.8, Installing Software on the B-Side.*
5. If you have purchased additional time-slots, refer to *Section B.9* and to the *System Administration Guide,* for information about updating the license.

B.8 INSTALLING THE SOFTWARE ON THE B-SIDE

If you are installing the software on a redundant system, you must also install the software on the B-side. If you do not have a redundant system, skip this section and continue to the next section.

To install the software on the B-side:

1. Power down the system.
2. Move the AAC switch to the B position.
3. Connect or switch the administration console to the B-side CPU-TM, or go to the B-side system console.
4. Insert Disk 1 into the B-side drive.

   NOTE: Make certain that you place the Installation Disks into the B: drive during installation of the B-side.
5. Power on the B-side.
6. After the system performs diagnostic tests, repeat the steps in *Section B.5, Installing the Software* starting with Step 5 and, if needed, *Section B.7, Installing Optional Software.*
7. After the software has been installed on the B-side, power down the system, switch the AAC to Auto, and reboot the system.

B.9 TIME-SLOT ALLOCATION LICENSE

If you have purchased additional time-slots, you must update the time-slot allocation license. Refer to the *System Administration Guide* for information about updating the license.

If no additional time slots were purchased, proceed to the next section, installing the MIB.

B.10 THE MIB - SUPPLEMENTAL DISK FILES

Install the MIB software on your network management system. The MIB - Supplemental Disk contains four files:

vco.mib	This file defines the structure of the MIB in ASN.1 notation. It is used for your implementation of network management on a workstation, PC, or other computer system.
snmptalk	This is a UNIX executable file which provides the user with the ability to send and get information from the database tables.
mib.rt	This file, used by snmptalk, is a translation of the vco.mib file. Snmptalk needs it to understand the mnemonics used to query the database tables.
etc.ini	This is the initialization file for snmptalk.

To move the MIB software which is provided on the MIB - Supplemental Disk to a network management system:

1. Place the MIB - Supplemental Disk in the floppy drive of the Host computer.

   Note that snmptalk is a UNIX executable file and is only usable on UNIX computers. The three other files can be used on a non-UNIX platform.

2. Create a directory in which the MIB files are to reside. Define the location and name of the directory.
3. Move the files from the disk into the new directory created in Step 2.

   Note: All four files must reside in the same directory.

Appendix C
CONFIGURING THE MIB

C.1 INTRODUCTION

This appendix describes the procedures for installing the MIB files that are on the Supplemental disk. The disk contains a copy of the MIB (vco.mib) and the snmptalk® application. This application enables you to send basic SNMP requests to the VCO for testing purposes and to demonstrate the basic structure of the SNMP agent.

The snmptalk application is designed to be invoked on a Sun workstation using SunOS. The program uses files etc.ini and mib.rt. The file etc.ini contains configuration information, and the file mib.rt contains information that enables you to enter symbolic information instead of numbers.

All three files (vco.mib, etc.ini, and mib.rt) must be located in the same directory as the snmptalk application.

C.2 SETTING UP snmptalk

Once you invoke the snmptalk program, you need to enter the following set-up information so it will communicate with your system. Prior to doing the set-up, you need to know the Internet Protocol (IP) address of your system.

Table C.1: snmptalk Setup Commands

Command	Meaning
v 1	Selects the SNMP Version 1 mode
write-comm public	Sets write community to “public”
dest ###.###.###.###	Enters the IP address of the VCO
?	Provides a list of the commands available
get sysUpTime.0	Example of get command
tset sysLocation.0 string here	Example of set command
quit	Exit program

NOTE: This program does not recognize white space or quotes, so you must enter commands without spaces. This is a limitation of the basic test program.

C.2.1 MIB File

The vco.mib file is the ASN.1 notation MIB for the V4.0 system. This file can be compiled by a SNMP Network Management Station and used to provide the management station with information on the VCO MIB structure. The information in this file is also listed in the *VCO V4.0 Management Information Base (MIB) Reference Guide*.

C.2.2 Public Access

The community names for read and write access must be set to “public” for a NMS to properly access the Summa Four Enterprise MIB.

Appendix D
DATABASE CARD CONFIGURATION

D.1 INTRODUCTION

This is an overview of the steps you must follow to add and configure the cards in your system. Refer to the *System Administration Guide* for details on the steps outlined below.

D.2 DATABASE CARD INSTALLATION

To add and configure the cards, do the following for the cards installed in your system.

D.2.1 Add Cards to the Database

The first step when adding cards to the database, is to take a survey of the cards in your system. Note the physical location (in which slot) each card resides. The card location survey worksheets, included at the end of this appendix, may be used to complete this step.

If you want to change the location of the cards, do so before completing the survey and adding the cards to the database.

Table D.1: Card Placement

Card	VCO/20		SDS and VCO/80	
	Redundant	**Non-redundant**	**Redundant**	**Non-redundant**
NBC-3/ DTG-2	Resides in slots 1 and 2	Resides in slot 1[a]	Resides in slots 1 and 2 of the Master Port Subrack	Resides in slot 1 of the Master Port Subrack[b]
Combined Controller	Resides in slots 3-4, and 5-6	Resides in slots 3-4[a]	(none)	
BRC	(none)		In the Master Port Subrack: it is suggested that it reside in slot 3 In Expansion racks: resides in slots1 and 2	In the Master Port Subrack: it is suggested that it reside in slot 3[b] In Expansion racks: resides in slot 1
All other cards	Start in slot 7		In Master Port subrack: start in slot 5 In Expansion racks: start in slot 3	In Master Port subrack: start in slot 4[b] In Expansion racks: start in slot 3

[a] Slots 2, 5, and 6 must remain empty in non-redundant VCO/20 systems.
[b] Slot 2 of the Master Port Subrack must remain empty in non-redundant SDS or VCO/80.

When you have a written survey of where the cards reside, do the following.

- Log on to the system, and from the Maintenance Menu screen, access the Card Maintenance screen.
- The NBC-3/DTG-2 cards are the only cards that should display for rack 1 level 1. Add all other cards to the database.

  Note: When a card is added, it is out-of-service (OOS).

You will activate the cards in the last step in this procedure.

Refer to the *System Administration Guide, Section 4,* for information on how to access the Maintenance screens, and for instructions on adding cards.

D.2.2 Configure the Cards in the Database

From the Data Base Administration screen, access the Card Summary screen. Tab to the DISP CARD field for the card you want to configure. Enter any character, then press the Enter key. A new screen appears for the selected card.

Enter the data on a per port basis:

- port name (if needed)
- hardware type (trunk cards only)
- inpulse rule to be executed as a default
- class of service (per port)

Refer to the *System Administration Guide, Section 2,* for information on how to access the Card Summary screen, and for instructions on configuring cards.

D.2.3 Assign the Ports to a Resource Group

From the Data Base Administration screen, access the Resource Group Summary screen. *This step is mandatory for service circuit cards.*

- Define the resource groups.
- Tab to the DISP field for the resource group to which you want to assign ports. Enter any character, then press the Enter key. A new screen appears for the selected resource group.

Refer to the *System Administration Guide, Section 2,* for information on how to access the Resource Group Summary screen, and for instructions on assigning ports.

D.2.4 Activate the Cards

Access the Card Maintenance screen and change the status of the card to *Active.*

Refer to the *System Administration Guide, Section 4,* for information on how to access the Card Maintenance screen, and for instructions on activating cards.

Table D.2: Card Location Survey—VCO/20

Card	Location rack/level/slot (R/L/S)	Other—Configuration and/or Resource Group Notes
NBC-3/DTG-2	1-1-1	
NBC-3/DTG-2	1-1-2 *(redundant systems only)*[a]	
Combined Controller	1-1-3 1-1-4	
Combined Controller	1-1-5 1-1-6 *(redundant systems only)*[a]	
	1-1-7	
	1-1-8	
	1-1-9	
	1-1-10	
	1-1-11	
	1-1-12	
	1-1-13	
	1-1-14	
	1-1-15	
	1-1-16	
	1-1-17	
	1-1-18	
	1-1-19	
	1-1-20	
	1-1-21	

[a] Slots 2, 5, and 6 must remain empty in non-redundant VCO/20 systems.

Table D.3: Card Location Survey—SDS or VCO/80 Master Port Subrack

Card	Location rack/level/slot (R/L/S) Master Port Subrack	Other—Configuration and/or Resource Group Notes
NBC-3/DTG-2	1-1-1	
NBC-3/DTG-2	1-1-2[b] *(redundant systems only)*	
BRC	1-1-3	
	1-1-4	
	1-1-5	
	1-1-6	
	1-1-7	
	1-1-8	
	1-1-9	
	1-1-10	
	1-1-11	
	1-1-12	
	1-1-13	
	1-1-14	
	1-1-15	
	1-1-16	
	1-1-17	
	1-1-18	
	1-1-19	
	1-1-20	
	1-1-21	

[b] Slot 2 of the Master Port Subrack must remain empty in non-redundant SDS or VCO/80 systems.

Table D.4: Card Location Survey—SDS or VCO/80 Expansion Rack (R1-L2)

Card	Location rack/level/slot (R/L/S) Expansion Subrack	Other—Configuration and/or Resource Group Notes
BRC	1-2-1	
BRC	1-2-2 *(redundant systems)*	
	1-2-2 *(available in non-redundant systems)*	
	1-2-3	
	1-2-4	
	1-2-5	
	1-2-6	
	1-2-7	
	1-2-8	
	1-2-9	
	1-2-10	
	1-2-11	
	1-2-12	
	1-2-13	
	1-2-14	
	1-2-15	
	1-2-16	
	1-2-17	
	1-2-18	
	1-2-19	
	1-2-20	
	1-2-21	

Table D.5: Card Location Survey—SDS or VCO/80 Expansion Rack (R2-L0)

Card	Location rack/level/slot (R/L/S) Expansion Subrack	Other—Configuration and/or Resource Group Notes
BRC	2-0-1	
BRC	2-0-2 *(redundant systems)*	
	2-0-2 *(available in non-redundant systems)*	
	2-0-3	
	2-0-4	
	2-0-5	
	2-0-6	
	2-0-7	
	2-0-8	
	2-0-9	
	2-0-10	
	2-0-11	
	2-0-12	
	2-0-13	
	2-0-14	
	2-0-15	
	2-0-16	
	2-0-17	
	2-0-18	
	2-0-19	
	2-0-20	
	2-0-21	

Table D.6: Card Location Survey—SDS or VCO/80 Expansion Rack (R2-L1)

Card	Location rack/level/slot (R/L/S) Expansion Subrack	Other—Configuration and/or Resource Group Notes
BRC	2-1-1	
BRC	2-1-2 *(redundant systems)*	
	2-1-2 *(available in non-redundant systems)*	
	2-1-3	
	2-1-4	
	2-1-5	
	2-1-6	
	2-1-7	
	2-1-8	
	2-1-9	
	2-1-10	
	2-1-11	
	2-1-12	
	2-1-13	
	2-1-14	
	2-1-15	
	2-1-16	
	2-1-17	
	2-1-18	
	2-1-19	
	2-1-20	
	2-1-21	

Table D.7: Card Location Survey—SDS or VCO/80 Expansion Rack (R2-L2)

Card	Location rack/level/slot (R/L/S) Expansion Subrack	Other—Configuration and/or Resource Group Notes
BRC	2-2-1	
BRC	2-2-2 *(redundant systems)*	
	2-2-2 *(available in non-redundant systems)*	
	2-2-3	
	2-2-4	
	2-2-5	
	2-2-6	
	2-2-7	
	2-2-8	
	2-2-9	
	2-2-10	
	2-2-11	
	2-2-12	
	2-2-13	
	2-2-14	
	2-2-15	
	2-2-16	
	2-2-17	
	2-2-18	
	2-2-19	
	2-2-20	
	2-2-21	

Table D.8: Card Location Survey—SDS or VCO/80 Expansion Rack

Card	Location rack/level/slot (R/L/S) Expansion Subrack	Other—Configuration and/or Resource Group Notes