Dialogic® SS7G2x Signaling Server

SGW Mode User Manual

www.dialogic.com

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Corporation or its subsidiaries (“Dialogic”). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic’s legal department at 9800 Cavendish Blvd., Montreal, Quebec, Canada H4M 2V9. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.**

Dialogic is a registered trademark of Dialogic Corporation. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic’s legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic’s trademarks requires proper acknowledgement.

Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries. Other names of actual companies and products mentioned herein are the trademarks of their respective owners.

Publication Date: September 2007

Document Number: 05-2304-004

Contents

Figures

Tables

Revision History

Date	Part Number	Issue	Description of Changes
September 2007	05-2304-004	4	Updates for brand changes, web sites, and other minor corrections.
December 2005	05-2304-003	3	Updates to include support for resilient IP connectivity, additional measurement and status commands (STSYP, MSSYP and MSEPP) and other minor enhancements and corrections.
May 2005	05-2304-001	2	Supports the first production release.
March 2005	05-2304-001-01	1	Field Trial release.

Note: The latest released issue of this guide can be found at: http://www.dialogic.com/support/helpweb/signaling

Chapter 1: Overview

1.1 General Description

The Dialogic® SS7G21 and SS7G22 Signaling Servers, (hereinafter sometimes referred to collectively as "the SS7G21 and SS7G22 products," individually as "SS7G21" and "SS7G22," respectively, or individually or interchangeably as "SS7G2x"), with the Dialogic® SS7SBG20SGW SGW Mode software license installed and enabled, operate as SIGTRAN Signaling Gateways (hereinafter sometimes referred to as "Signaling Gateway"). They provide an interface between SS7 and IP networks, allowing SS7 information to be carried over IP to either IP resident signaling points and applications (for example, a soft switch) or to another Signaling Gateway. IETF SIGTRAN protocols are used to ensure interoperability with third party equipment.

The Signaling Server may be purchased as one of two equipment types; SS7G21 and SS7G22. Each equipment type uses the same chassis and operates with the same software, but uses different signaling boards. See Section 1.4, “Hardware Overview” on page 9 for a fuller description of the Signaling Server hardware.

The Signaling Gateway uses the SIGTRAN M3UA protocol to "backhaul" SS7 signaling messages to IP resident Application Servers, removing the need for Application Hosts to have dedicated SS7 MTP services or hardware. Application Servers using the Signalling Gateway may be part of a single point code or multiple point codes.

The Signaling Gateway M3UA architecture uses open standards interfaces, providing flexibility, scalability and resilience. It is easy to add or reconfigure M3UA Application Servers and Signaling Gateways to meet demands for new services or increased capacity.

The Signaling Gateway also supports SIGTRAN M2PA protocol to talk to other Point Codes over IP links, rather than TDM. M2PA may be used to connect within the central office, or for longhaul links over IP.

The SIGTRAN Signaling Gateway (SGW) functionality is provided as a software option on the SS7G21 and SS7G22 Signaling Servers. To enable this functionality, order and install the SS7SBG20SGW software license. A unit with the SGW Mode license installed and enabled is referred to as a “Signaling Gateway” throughout this manual.

When the software license is either not installed or deactivated, the SS7G21 and SS7G22 act as SS7 Signaling Interface Units (SIUs), providing an interface to SS7 networks for a number of distributed application platforms via TCP/IP LAN. In this mode, the units implement the SS7 Message Transfer Part (MTP) and a number of User Parts (ISUP, SCCP, TCAP, MAP, IS41 and INAP). See the *SS7G2x SIU Mode User Manual* for a detailed description of this mode of operation.

The SS7G21 and SS7G22, when fitted with the DSC Mode software license, operate as a protocol converter. It provides protocol interworking between any pair of telephony protocols for both network protocols and access protocols. Description and use of the system acting as a protocol converter is outside the scope of this manual. See the *SS7G2x DSC Mode User Manual* for a detailed description of this mode of operation.

The SS7G21 and SS7G22 are shipped without the SGW Mode Software License installed and therefore start up initially as SS7 Signaling Interface Units (SIUs). The procedures for the purchase and installation of the SGW and other software options are described in Section 4.14, “System Licenses” on page 27. The procedures required to configure a unit for SGW operation as well as those for initial system configuration are described in Chapter 3, “Installation and Initial Configuration”.

1.2 Related Information

This user manual, together with the *Dialogic® SS7G21 and SS7G22 Hardware Manual* forms the documentation set for the SGW mode of operation of an SS7G2x. The *Dialogic® SS7G21 and SS7G22 Hardware Manual* addresses the hardware-specific aspects of the product including: hardware variants, installation, specification, module replacement and a full description of the hardware modules. This user manual describes the user interface together with all parameters and configuration commands.

The full title of the hardware manual is:

- *Dialogic®*SS7G21 and SS7G22 Signaling Servers Hardware Manual –
(05-2300-xxx)

The latest software and documentation supporting SS7G2x products is available on the web at http://www.dialogic.com/support/helpweb/signaling.

The product data sheet is available at http://www.dialogic.com/support/helpweb/signaling.

For more information on Dialogic® SS7 products and solutions, visit http://www.dialogic.com/support/helpweb/signaling.

When used for M3UA backhaul operation, the Signaling Gateway may operate with an ASP operating either an Dialogic M3UA Application Server or an Application Server provided by a third party vendor. See the *Dialogic® SS7 Protocols Programmer's Manual for SIGTRAN Host Software* for documentation on the configuration and use of a Dialogic M3UA Application Server.

1.3 Applicability

This manual is applicable to SS7G2x units with software V3.02 and later installed. This manual is not applicable when operating as a Signaling Interface Unit (SIU) or as a DSC Protocol Converter (DSC). See the *Dialogic® SS7G2x SIU Mode User Manual* and the *Dialogic® SS7G2x DSC Mode User Manual* for descriptions use of these modes of operation.

1.4 Hardware Overview

The Signaling Gateway may be purchased as one of two equipment types; SS7G21 and SS7G22. Each equipment type uses the same chassis and operates with the same software, but differ in the type of pre-installed SS7 Signaling boards. This provides options in the numbers and types of links and ports available.

An SS7G21 may be purchased with one, two, or three SPCI2S boards (where each board provides four SS7 links, two T1/E1 interfaces and two V.11 serial ports per board) or one, two or three SPCI4 boards (where each board provides four SS7 links and four T1/E1 interfaces per board).

An SS7G22 may be purchased with one, two or three SS7HDP boards (where each board provides 64 SS7 links and four T1/E1 interfaces per board) with a system maximum of 128 SS7 links.

When T1 or E1 is selected, the Signaling Gateway may be configured to pass the bearer channels from one PCM port to another, effectively “dropping out” the signaling in line.

See Chapter 2, “Specification” for a full definition of the capabilities of the system.

1.4.1 Part Numbers

See the *Dialogic® SS7G21 and SS7G22 Hardware Manual* for a full list of the ordering codes and definitions of all of the hardware variants of the two equipment types.

1.5 Connectivity

TDM SS7 signaling can interface to the Signaling Gateway using balanced 1544 kbit/sec (T1) balanced connections in accordance with G.733 or 2048 kbit/sec (E1) connections in accordance with G.703. SS7 signaling can also be presented on a V.11 (56/64 kbit/sec) synchronous serial interface.

MP2A signaling used for communication between paired Signaling Gateways can be received at the conveter using 4 x 1 Gbit/sec RJ45 Ethernet™ interfaces.

1.6 User Interface

The Signaling Gateway provides serial port and telnet connections for configuration and management. All ports provide identical functionality and operate using text-based MML (Man Machine Language) commands in accordance with CCITT recommendations.

The serial and telnet ports allow the user to configure the Signaling Gateway for operation and to carry out subsequent modifications to the configuration. They allow the user to read the current status of the various signaling entities and to view the current active alarms and a history of past alarm events.

The Signaling Gateway provides SNMP V1 support to allow the reporting of alarms to an SNMP manager. See Chapter 10, “SS7G2x SNMP MIB” for more information.

The Signaling Gateway has alarm indicators on the front panel and alarm relays for connection to an integrated management system.

1.7 Configuration and Program Storage

All configuration data is stored on hard disk and is automatically recovered after system restart. Configuration data may optionally be backed up to a remote computer, previously backed-up configurations can be reloaded.

All operating software is stored on hard disk and is automatically initiated after system restart. The operating software can be updated either by reading a new software release from CD ROM or by FTP transfer from a remote computer. In both cases, software update is initiated by MML command. See Section 4.11, “Updating System Software” on page 24 for details. Following a software update, the Signaling Gateway automatically uses the saved configuration data so that there is no need to reenter the configuration parameters.

1.8 IP Security

The Signaling Gateway offers a number of security features to protect it from unwarranted access on its IP interface. It is recommended that the user always enable the optional password protection on the management interface port and on the FTP server port (if used).

For additional security, the Signaling Gateway is also equipped to support telnet and FTP access using a Secure Shell (SSH).

Unused ports are disabled to increase security against unintentional or malicious interference.

Additional security may be gained by separating management and signaling IP traffic. This can be achieved by configuring specific Ethernet ports for traffic and utilizing other Ethernet ports for system management.

It should be understood that while the Signaling Gateway has been designed with security in mind, it is recommended that Signaling Gateway accessibility over IP is restricted to as small a network as possible. If the unit is accessible by third parties, the use of a third-party firewall should be considered.

1.9 Functional Summary

The functional summary is described in the following topics:

- Signaling
- Configuration Model
- Cross Connections
- Monitoring
- Remote Data Centres
- Alarm Log
- M3UA Backhaul Operation
- M2PA Longhaul Operation
- Dual Operation
- Default Routing

1.9.1 Signaling

The Signaling Gateway supports the Message Transfer Part (MTP) in accordance with ITU Recommendations Q.700, Q.704 and Q.707 and ANSI operation in accordance with ANSI T1.111.

When a link set contains two or more signaling links, the Signaling Gateway supports load sharing and the full changeover and changeback procedures in accordance with ITU-T Q.704.

The Signaling Gateway supports up to 128 TDM SS7 signaling links allowing the Signaling Gateway to interface over TDM to a maximum of 64 other signaling points.

If required, each signaling link in a link set can be terminated on a separate signaling board providing additional resilience.

The Signaling Gateway can have a presence in up to four separate IP subnets.

The Signaling Gateway supports up to 32 M2PA SS7 signaling links, allowing the Signaling Gateway to interface over IP to a maximum of 32 other signaling points.

M2PA is supported in accordance with the IETF SS7 MTP2-User Peer-to-Peer Adaptation Layer specification.

SCTP is supported in accordance with IETF RFC 2960 and RFC 3309 Stream Control Transmission Protocol.

The Signaling Gateway supports communication with up to 200 Application Servers Processes (ASPs) for backhaul operation over M3UA.

M3UA is supported in accordance with the IETF RFC 3332 SS7 MTP3 User Adaptation Layer.

1.9.2 Configuration Model

MTP data messages are considered to arrive at either an MTP3 **link set** or an M3UA **SIGTRAN link**. The link set or M3UA SIGTRAN link identifies the network and SS7 format of the message. MTP3 link sets can exist above a TDM MTP2 signaling link or a signaling link utilizing a M2PA SIGTRAN link for communication over IP.

The decision as to how to process the data message is performed by the incoming route. The **incoming route** is identified by the network and domain (either MTP or IP) that a message arrives from.

The incoming route then determines whether the message requires further analysis of the data prior to destination selection by looking up a **routing key** table or whether a **destination** can immediately be selected.

If the Signaling Gateway determines that a routing key table be looked up, the data from the data message is compared with routing keys in a routing key table. If a match is found, and the destination for that routing key is in service, that destination is used. Otherwise, if the incoming route also has a destination associated with it, that default destination is used. If no routing key table is associated with it, the default destination is used.

A destination can route a data message to either an **Application Server** (AS) or to MTP (MTP over MTP2 or MTP over M2PA). Selection of whether MTP or IP routing is used is determined by the availability of the data messages point code in the MTP or IP domain and whether MTP or IP has priority.

If MTP routing is selected, the data message is sent out on an MTP **SS7 route** that matches the point code of the data message. It is possible to configure MTP3 with a default route for use when it is undesirable to preconfigure all routes that are used.

See Chapter 7, "Configuration Overview" for a more detailed configuration discussion and Chapter 11, "Worked Configuration Examples" for some examples.

1.9.3 Cross Connections

The Signaling Gateway allows the user to set up cross connections (semi-permanent connections) between an incoming timeslot on one PCM port and an outgoing timeslot on any PCM port. These connections can either be simplex or duplex.

1.9.4 Monitoring

The Signaling Gateway allows the user to monitor TDM signaling links by dropping a copy of the signaling to a spare PCM port. This allows for a protocol analyzer to be left connected to one PCM port and gives the user the ability to control remotely which signaling links are monitored. Each monitored signaling link requires two timeslots on the spare PCM port, one to monitor the send direction and the other for the receive direction.

1.9.5 Remote Data Centres

The Signaling Gateway supports the transfer of software updates, configuration files, alarm reports and periodic measurements over Ethernet to/from a remote location, the Remote Data Centre (RDC).

Multiple RDCs can be configured by specifying an IP address and a user name and password for the Signaling Gateway to use to "logon" to the RDC.

Data transfer to the RDC uses the File Transfer Protocol (FTP).

Measurement reports are made on a configurable periodic basis.

Optionally, since it can be configured as an FTP server, the Signaling Gateway itself can be configured to act as an RDC, thus allowing RDC operation to be performed locally on the Signaling Gateway itself.

See Chapter 9, "Remote Data Centre Operation" for a more detailed description of the capabilities and configuration of an RDC.

1.9.6 Alarm Log

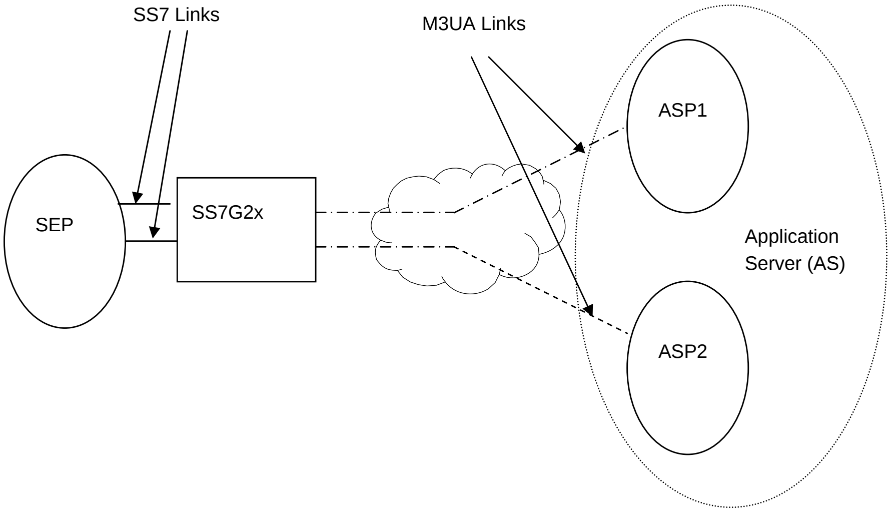
The Dialogic® SS7G2x product is able to detect a number of events or alarm conditions relating to either the hardware or the operation of the protocols. Each alarm condition is assigned a severity/class (3 = Critical, 2 = Major, 1 = Minor) and a category and ID, which give more detail about the alarm. There are a number of mechanisms described below, by which these conditions can be communicated to management systems, and ultimately to the system operator (see Chapter 8, "Alarm Fault Code Listing" for a full list of alarm types, and their reporting parameters):

- Active alarms are indicated on the front panel of the unit by three LEDs showing the severity; CRT, MJR and MNR. See the *Dialogic® SS7G21 and SS7G22 Hardware Manual* for information on the location of these indicators.
- Active alarms may be indicated remotely from the unit, by connecting to relay outputs provided by the SS7G2x. There are contacts for each severity; Critical, Major and Minor. See the *SS7G21 and SS7G22 Hardware Manual* for information on the location, pinout and rating of the Alarms connector.
- Alarm events (class, category and ID) may be reported to an SNMP manager. Activation of SNMP V1 support and the SNMP MIB are described in Chapter 10, "SS7G2x SNMP MIB".
- A system operator can obtain a listing of the current alarm status (ID, class, fault title, occurrence time and title) using the ALLIP management terminal command described in Section 6.4.4, "ALLIP" on page 44.
- A system operator can access a log of the current and previous alarms using the ALLOP management terminal command described in Section 6.4.5, "ALLOP" on page 45. The Alarm Log has the capacity for up to 200 entries, each entry detailing the ID, title, alarm class, fault title, occurrence time, status (active or cleared), and cleared time (if appropriate). If a new fault occurs when the log is full, the oldest entry that is either cleared, of lower class, or equal class is overwritten, in that order of preference. The operator may request a display of the log at any time and may remove entries that have cleared status.
- The alarm log may also be reported to a Remote Data Centre (RDC). See Section 9, "Remote Data Centre Operation" on page 151 for the configuration and operation of an RDC and for the format of the alarm log records.

1.9.7 M3UA Backhaul Operation

The Signaling Gateway can use the SIGTRAN protocol M3UA to "backhaul" SS7 information to an IP resident Application Server (AS) operating on one or more Application Server Processes (ASPs). Examples of Application Servers are Media Gateway Controllers or IP resident databases. In both cases, the Application Server can operate as a Signaling End Point (SEP), where SS7 User Part Protocols, such as SCCP or ISUP, operate above a M3UA layer on the host.

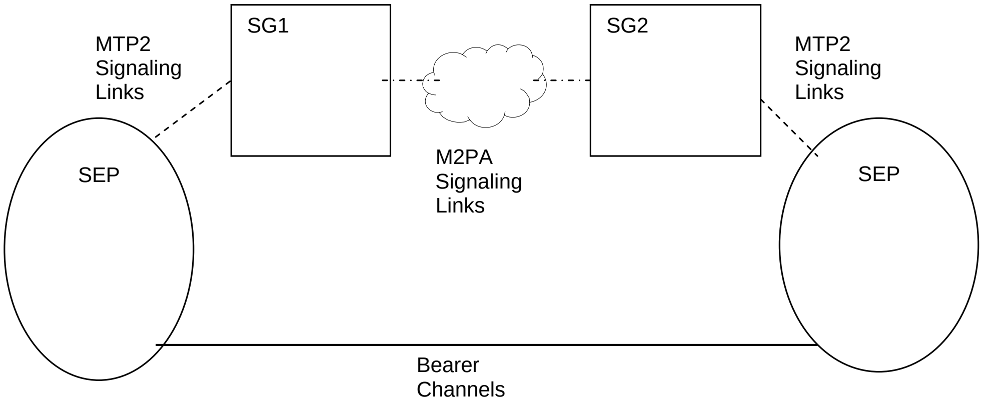
Figure 1. M3UA Backhaul Configuration



1.9.8 M2PA Longhaul Operation

The Signaling Gateway is capable of replacing TDM SS7 links with signaling links operating over IP providing the equivalent functionality to MTP Layer 2 by using the SIGTRAN M2PA protocol. One use of M2PA signaling links would be for the low cost longhaul of signaling traffic possibly involving SS7/SS7 protocol conversion. Two Signaling Gateways would be required, one either side of the IP connection translating between M2PA <-< MTP2. See Chapter 11, “Worked Configuration Examples” for an M2PA Longhaul configuration example.

Figure 2. M2PA Longhaul Configuration



1.9.9 Default Routing

The Signaling Gateway may be configured to use default routing. This is designed to allow greater routing flexibility. See Section 6.5, “Configuration Commands” on page 48 for further information regarding default routing.

1.9.10 Resilience

1.9.10.1 IP Resilience

The Signaling Gateway has four IP ports. These ports may be configured with IP addresses in separate IP networks to allow greater IP resilience on the Signaling Gateway. IP addresses are configured using the CNSYS command. The CNSYS command also allows the user to configure the default IP gateway for the unit, while the IPGWI command allows the user to configure additional IP gateways.

As the Signaling Gateway supports static, rather than dynamic IP routing, the Signaling Gateway may not be configured with different IP addresses within the same IP network. Instead, resilience between two IP ports within the same network can be achieved by using IP port bonding, which allows two physical IP ports to be bonded together in an active/standby configuration under a single IP address. See Section 7.6.1, "IP Port Bonding" on page 142 for more information.

1.9.10.2 Dual Operation

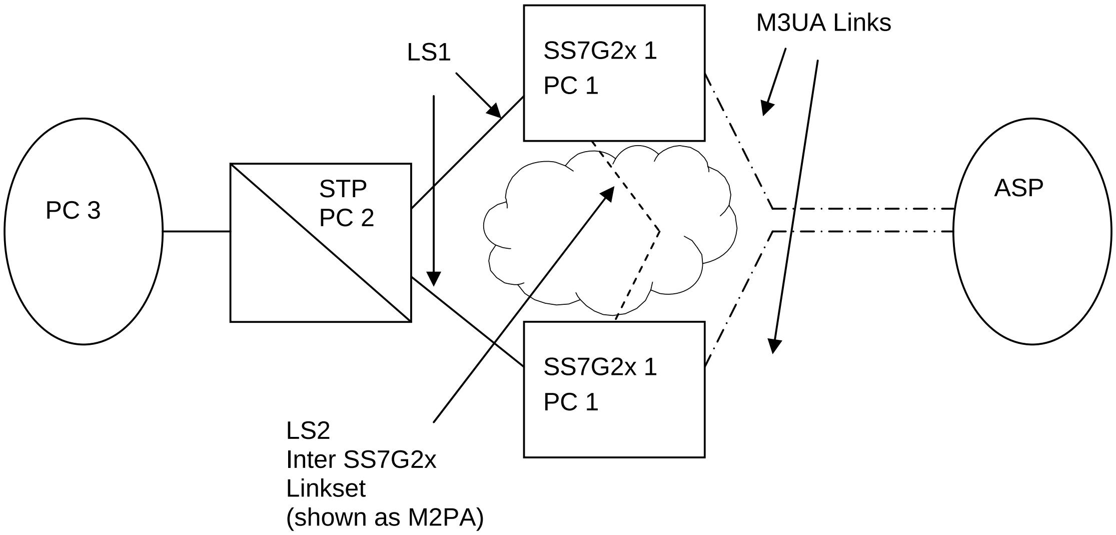
The Signaling Gateway may be configured as part of a Dual-Resilient pair; that is, two SS7G2x units appearing to the network as a single point code. If the SS7 network loses accessibility of one unit, the point code status remains unaffected.

Figure 3 shows a dual resilient system with two Dialogic® SS7G2xs products connected to an STP in the SS7 network and an M3UA ASP. To achieve this configuration, the following additions to the normal configuration must be made:

1. The configuration of an inter-SS7G2x link set. This has the same DPC and OPC. This link set may consist of MTP2 links, M2PA links or a combination of both.
2. Each C7Route must be configured to use a preferred link set LS1 and a backup link set LS2.
3. Each SS7G2x must be configured with a C7Route to the other SS7G2x using only LS2.

Note: Since both SS7G2xs have C7Links that are part of the same link set (from the perspective of the adjacent point code), care must be taken in the assignment of SLCs.

Figure 3. Dual Resilient Configuration



See Chapter 7, "Configuration Overview" for a more in depth discussion of Dual Resilient configuration.

Chapter 2: Specification

2.1 Hardware Specification

Full details of the Signaling Gateway hardware specification are given in the *Dialogic® SS7G21 and SS7G22 Hardware Manual*.

2.2 System Capacity

The maximum capacity is dependent on the number and type of signaling boards installed. The numbers given in this section are for a single unit. Use of Signaling Gateways in dual pairs or in clusters proportionally increases the capacity of the overall system while still acting as a single SS7 point code.

2.3 System Capabilities

- Maximum number of signaling boards: 3
- Number of 10/100/1000 Mbit/sec Ethernet interfaces: 4

2.4 Signaling Capabilities (Per System)

- Maximum number of SS7 Signaling Links (including M2PA): 128
- Maximum number of M2PA Signaling Links: 32

Note: A system supports up to 128 SS7 links, where each link can be used for either M2PA or MTP2. The number of SS7 links used for M2PA reduces the number of links available for MTP2 and vice-versa. For example, if 32 SS7 links are used for M2PA, 96 links are available for MTP2.

- Maximum number of SS7 link sets: 64
- Maximum number of SS7 routes: 128 per network
- Maximum number of Networks: 4
- Maximum number of Application Servers: 200
- Maximum number of Application Servers: 200
- Maximum number of M3UA routes: 200
- Maximum number of Network Contexts: 4

2.5 Physical Interfaces (Per Signaling Board)

- SPCI2S T1/E1 PCM interfaces: 2
- SPCI2S SS7 V.11 serial interfaces: 2
- SPCI4 T1/E1 PCM interfaces: 4
- SS7HDP T1/E1 PCM interfaces: 4

2.6 TDM Signaling Capabilities (Per Signaling Board)

- Maximum number of SS7 Signaling Links (SPCI4 / SPCI2S): 4
- Maximum number of SS7 Signaling Links (SS7HDP): 64

Note: The system limit for a Signaling Gateway is still 128 SS7 Signaling Links even when three SS7HDP boards are installed.

Chapter 3: Installation and Initial Configuration

3.1 Installation

Note: The Signaling Gateway should only be installed by suitably qualified service personnel. Important safety and technical details, required for installation, are given in the *Dialogic® SS7G21 and SS7G22 Hardware Manual*.

In order to complete the installation of the Signaling Gateway unit, follow the steps below:

1. Connect a VT100 terminal to the unit (see Section 3.2).
2. Check whether a software download and upgrade is required (see Section 3.3).
3. Install any additional software option licenses that may have been purchased (see Section 4.14.2, “Installing System Licenses” on page 28).
4. Change the system type to act as a SIGTRAN Signaling Gateway (see Section 3.4).
5. Set the IP addresses of the unit (see Section 3.4).
6. Apply the configuration to the unit (see Section 3.5).

3.2 Connecting a VT100 Terminal

A VT100 compatible terminal can be connected, using a DKL29 cable, to the serial port (COM2) on the rear of the unit. After pressing the carriage return (Enter) key, the Signaling Gateway interface prompt is displayed. Default serial port settings are 9600 baud, 8 data bits, 1 stop bits and no parity bits.

The output on the VT100 screen is one of the following:

```
SS7G20(SIU) logged on at 2004-01-20 14:52:29
<
```

to indicate SIU operation

OR

```
SS7G20(SGW) logged on at 2004-01-20 14:52:29
<
```

to indicate SGW operation

OR

```
SS7G20(DSC) logged on at 2004-01-20 14:52:29
<
```

to indicate DSC operation.

3.3 Software Download

Up-to-date information and software downloads for the Dialogic® SS7G2x products can be found at the following URL:
http://www.dialogic.com/support/helpweb/signaling

The product leaves the factory with fully-functional software installed. We recommend you check the above URL for any recent revisions, and install them before putting the product into service.

Since it is possible to source units from multiple supply channels, we recommend that each is verified to ensure that all units in a delivery are at the same software revision.

Follow the steps below:

1. Check the current software version running in the system using the CNSWP command.
2. Check the latest distribution file from the “SS7G2x Signaling Gateway” section on the SS7 Products download web site:
http://www.dialogic.com/support/helpweb/signaling

3. If a download is required, store the distribution file in an empty directory on the hard drive of the downloading machine.
4. Follow the steps detailed in Section 4.11, “Updating System Software” on page 24 in order to carry out the update of the system software.

3.4 Initial Configuration

By default, the Signaling Gateway is shipped configured to operate in SIU mode. Once an SGW license has been applied, the system must be restarted using the MNRSI MML command requesting that the unit operate in SGW mode. Connect a VT100 terminal to identify the mode of operation (See Section 3.2, “Connecting a VT100 Terminal” on page 16).

The MNRSI restart command should be used to restart the system in a different mode. MNRSI should be used together with the mode in which the Signaling Gateway is expected to operate in after restart. For SGW operation this is:

```
MNRSI:SYSTYPE=SGW;
```

The Signaling Gateway is configured with a default IP address of 192.168.0.1. If this address is not unique, or not suitable for the existing network configuration, it is necessary to change this value to a unique IP address in the Ethernet network to which it is connected. Instructions for making this change are given below.

Using the VT100-compatible terminal, the IP address is set by entering the system configuration command, CNSYS. For example, to set the IP address to 123.124.125.126, the following command should be entered:

```
CNSYS:IPADDR=123.124.125.126;
```

It is also possible to configure a subnet mask if the unit is a member of a subnet. The default subnet mask is 255.255.255.0. To set the subnet mask to a different value, the following command should be used (the example here sets a subnet mask of 255.255.255.192):

```
CNSYS:SUBNET=255.255.255.192;
```

The management interface also allows an IP gateway address to be specified using the GATEWAY parameter. This is set by default to 0.0.0.0, indicating that no gateway is present. For example, to set the gateway address to 123.124.125.250, the following command is used:

```
CNSYS:GATEWAY=123.124.124.250;
```

The current settings can be displayed by entering the CNSYP command.

```
CNSYP;
```

The configuration is displayed in the format shown below:

```
System Configuration
UNITID:     0004238734ef
SYSID:
SYSREF:     0
PASSWORD:   ********
FTPPWD:     N
FTPSER:     Y
SECURE:     N
PER:        0
IPADDR:     172.28.148.99
SUBNET:     255.255.255.0
IPADDR2:    170.28.148.100
SUBNET2:    255.255.255.0
IPADDR3:    170.28.148.101
SUBNET3:    255.255.255.0
IPADDR4:    0.0.0.0
SUBNET4:    255.255.255.0
GATEWAY:    172.28.148.1
SNMP:       N
SGW:        Y
DSC:        N
SIU:        N
EXECUTED
```

Note: The protocol and mode parameters are only present if licensed. When a protocol or mode is active, the parameter shows the value “Y”, and when inactive, the parameter shows the value “N”.

The new IP address parameters is initialized *with immediate effect*. If the IP address used to login to the unit for the telnet session is changed, the user is automatically logged out of the session. However, the user can log in again without delay using the new IP address.

The Ethernet connection should be verified by attempting to “ping” the SGW from a computer connected to the same Ethernet network, using the following command:

```
ping 123.124.125.126
```

If the Signaling Gateway has been configured correctly, it responds to the ping and the host machine displays a message confirming communication with the Signaling Gateway (the exact format and response of this message is operating system dependant).

If ping fails, the user should check that the IP address was entered correctly and that there is no fault with the cabling to the Signaling Gateway.

Once the ping command shows that the Ethernet connection is valid, it should be possible to access the management interface previously used on the VT100 compatible terminal via telnet. This is achieved by establishing a telnet session to port 8100 or 8101.

Note: It is not possible to telnet to the standard telnet port 23.

For example, on a typical host console, the following command starts a telnet session to a Signaling Gateway with an IP address of 123.124.125.126:

```
telnet 123.124.125.126 8100
```

The telnet terminal displays the MML interface prompt:

```
SS7G20(SGW) logged on at 2004-01-20 14:52:29

<
```

An optional password can be set to control remote access to the MML. This is also done using the CNSYS command:

```
CNSYS:PASSWORD=password,CONFIRM=password;
```

If set, a user opening a telnet session to the MML is prompted to enter a password, for example:

```
SS7G20(SGW) logged on at 2004-01-20 14:52:29

password:
```

Password access can be removed by specifying “null” values for the PASSWORD and CONFIRM parameters, that is:

```
CNSYS:PASSWORD=,CONFIRM=;
```

For additional security, the units support the use of Secure Shell (SSH) tunnelling for telnet and secure FTP operation. The user should use the CNSYS command to restrict telnet access to "telnet via SSH tunnelling" only. For example:

```
CNSYS:SECURE=Y;
```

Note: The unit does not provide a Secure Shell session connection. Your SSH client may need additional configuration to allow SSH tunnelling without a session connection.

Once activated, a future user is required to set up an SSH tunnel prior to telnet access. For a client on a Linux® or Solaris™ like operating system, login for telnet using the ssh application. The ssh application should be invoked using a shellscript of the following form:

```
#!/bin/sh
ssh -l siuftp -C -f $1 -L 2323:$1:8101 sleep 5
telnet localhost 2323
```

3.5 Configuration Procedure

Once the system architecture and protocol configuration is known, it is necessary to set this configuration within the Signaling Gateway. Configuration is achieved using MML commands as described in Chapter 6, “Command Definitions”. An overview of configuration is provided in Chapter 7, “Configuration Overview” and example configurations are described in Chapter 11, “Worked Configuration Examples”.

Chapter 4: Operation

4.1 General

The Signaling Gateway can be configured by the user from either serial port 2 (COM2, on the rear panel) or by using telnet over the Ethernet interface. The serial port can be configured over a range of baud rates and parity. The default configuration for the port is 9600 bits/s, 8 data bits, 1 stop bit, and no parity. Serial port 1 (COM1, on the front panel) is not supported on the SS7G2x. Flow control can be set to either NONE or XON/XOFF on the terminal used to communicate with the serial interface of the SS7G2x.

The commands that make up the Signaling Gateway Man-Machine Interface Language (MML) are based on the CCITT blue book recommendations Z.311 to Z.317.

In the following description, input text, numerals and characters that the user is expected to enter are shown in **bold text** and responses displayed on the screen are shown in fixed width text. Syntax elements that are further defined are shown in angle brackets, for example, <time of day>.

4.2 Log On/Off Procedure

To initiate a dialog with the Signaling Gateway, the operator must “log on” to one of the MML interfaces.

To log on to the serial port when it is configured to use DTR/DSR, the connected terminal should assert DSR. The Signaling Gateway asserts DTR in response and the user can then enter into a dialog with the Signaling Gateway. The session is ended by operator command to the Signaling Gateway, or by the terminal deasserting DSR or at the expiry of an auto log off timer. The Signaling Gateway deasserts DTR in response to any one of these three. To log on again, DSR must first be deasserted.

To log on to the serial port when it is not configured to use DTR/DSR, the carriage return key should be entered. The session is ended by operator command to the Signaling Gateway or at the expiry of an auto log off timer.

The two telnet connections provided are accessed using a standard telnet utility. Only ports 8100 and 8101 can be used. The default port 23 should **not** be used.

If a password is specified for the system, when logging on, the password is required before being allowed to continue. If an incorrect password is entered, the system again prompts for a password. If an incorrect password is entered three times, the port is disconnected. For safety, the password is never required on the serial port.

When the connection is established, a message consisting of the system identity followed by:

```
logged on at <calendar date> <time of day>
```

is displayed, followed by the command prompt, which is the less than symbol (<). The logon session is ended either by operator command or at the end of an auto log off time out.

The system maintains two timers during the log on session: an “auto log off warning” timer and a “auto log off” timer. Both are restarted each time a new command is input. When the auto log off warning time out expires, an auto log off warning message is output to the terminal and any partially entered command is discarded. The system then outputs a command prompt to the terminal. If no command is input before the auto log off time out expires, the log on session is ended. The duration of both these timers is user-configurable and can even be disabled completely.

When log off is initiated, a message consisting of the system identity followed by:

```
logged off at <calendar date> <time of day>
```

is output to the operator’s terminal. The Signaling Gateway then initiates the appropriate procedure to end the connection to the operator’s terminal.

4.3 Command Character Set and Syntax

The only characters used for commands and parameters are:

- The letters **A** to **Z** and **a** to **z**, referred to as <letter>. The case of characters in command names and parameter names is not significant.
- The digits **0** to **9**, referred to as <digit>
- - (hyphen), CR (FE5), SP (space), **$**(dollar), **&** (ampersand), ***** (asterisk), **:** (colon), **;** (semicolon) **/** (solidus), **.** (full stop/period) and **=** (equals sign)
- The DEL (Delete) character or the BS (Backspace) character is used to delete characters on the current line.
- The CAN character (Ctrl X) is used as an abort character.

It is possible to indicate several simple values for the same parameter by grouping parameter arguments using the operators **&** or **&&**. For example, **3&6** indicates the simple parameter arguments 3 and 6. A sequence of consecutive simple parameter arguments is indicated by writing the lower and upper simple parameter arguments separated by **&&**, hence **4&&8** indicates the simple parameter arguments 4, 5, 6, 7 and 8.

Comments are allowed in command input, and can appear in any position on the command line. A comment is defined as a character string enclosed between the separators **/*** (solidus asterisk) and ***/** (asterisk solidus), where the character string can contain any characters except the format effector characters (HT – Horizontal Tab, LF – Line Feed, VT – Vertical Tab, FF – Form Feed and CR – Carriage Return) and the sequence ***/**.

4.4 Command Formats

To allow easy command recognition and familiarization, all the commands share a common five character format:

```
XXYYZ
```

where:

- XX = Command group
- YY = Function within group
- Z = Operation code

The following operation codes are used:

- **C** = Change
- **E** = End
- **I** = Initiate
- **P** = Print
- **S** = Set

Note: The term “print” refers to output to the serial port in use for the dialog procedure.

4.5 Command Entry

Each character entered is echoed to the operator’s terminal. The BS (backspace) or DEL (delete) character can be used to delete characters entered within the current line. This causes the Signaling Gateway to output the sequence BS space BS. On a visual display terminal, this has the effect of deleting the last character entered from the display.

Commands can be entered whenever the command prompt has been output. Commands are terminated by a semicolon (;) followed by CR. Commands may exceed one line on the terminal, but may not exceed 100 characters.

If a command takes parameters, a colon is used to separate the command from the parameters. A comma (,) is used to separate multiple parameters.

To ensure correct operation of the character deletion, the maximum number of characters entered on a single command line should be no greater than the number of characters that can be displayed on a single line of the terminal (to prevent text “wrap around”). If a command is longer than one line, each line before the last should be terminated with a complete parameter value followed by a comma and CR. The command can then continue on the next line. If the user wishes to specify more parameters than can be entered on a single initiate command, they should use the initiate command to enter mandatory parameters, then use a change command to specify additional parameters.

A partially entered command can be aborted using the CAN character. The system outputs an indication that the command has been aborted, followed by a prompt for new command input. The CAN character can also be used to abort an output listing on the operators terminal.

4.6 Dangerous Commands

Commands that affect the Signaling Gateway operation are considered DANGEROUS commands. When a DANGEROUS command is entered the Signaling Gateway outputs the following on a new line:

```
Are you sure? [Y/N]
```

The operator must enter **Y** followed by CR to continue the execution of the command. Any other valid input character apart from SP or CR, followed by CR, causes the command to be aborted.

4.7 Changing Configuration Data

Many configuration commands require that certain other commands have been entered first (for example to block a link before removing a boards configuration). These rules are described on a per-command basis as prerequisites.

4.8 Command Responses

The Signaling Gateway does not, in general, produce output unless in response to an operator command. The only exception to this is the auto log off warning message and the log off message (when log off is initiated automatically).

The auto log off warning message is as follows:

```
WARNING: Auto log off imminent!
```

When a syntactically correct command has been issued to the Signaling Gateway, acceptance is indicated by the Command Executed output as follows:

```
EXECUTED
```

An invalid command is not acted upon. The Signaling Gateway indicates command rejection by issuing one of the responses in Table 1. Only the first error detected in a command is indicated.

Table 1. Command Rejection Responses

Response	Reason for Rejection
UNACCEPTABLE COMMAND	The command is valid but not in the current state of the equipment (for example, changing a signaling link configuration without blocking).
UNKNOWN COMMAND	The command is not recognized.
NO SYSTEM RESOURCES	The requested command cannot be executed due to unavailable system resources.
INVALID PARAMETER NAME	A parameter name has been entered that is not valid for this command.
EXTRA PARAMETERS	Too many parameters have been entered.
MISSING PARAMETER	A required parameter has not been input.
INCONSISTENT PARAMETER	The parameters input are not valid together for the command.
MISSING DATA	A parameter has no data.
INCONSISTENT DATA	The values of parameters are inconsistent with each other or with data already entered into the system.
RANGE ERROR	The value assigned to a numeric parameter is outside the valid range.

Table 1. Command Rejection Responses (Continued)

Response	Reason for Rejection
INVALID INFORMATION GROUPING	The type of information grouping used in the input of the parameter value is not valid.
INVALID INDICATOR	This command contains a ‘format character’ (‘:’, ‘;’, etc.) that is not valid for this command.
GENERAL ERROR	Command unable to execute due to an external error (for example, a missing or write-protected CDROM).
INTERNAL ERROR	Command failed to complete due to internal error.
INVALID INFORMATION UNIT	The value entered for a parameter is not valid for that parameter.
UNKNOWN SEPARATOR	The character used to separate two parameters is not recognized.

4.9 FTP Access

The Signaling Gateway supports FTP server operation allowing the user to perform maintenance operations, such as software, license and configuration update without the use of MML as well as providing access to locally stored continuous records and periodic reports.

An FTP session should be established between the remote machine and the Signaling Gateway by entering the appropriate command on the remote machine's keyboard, for example:

```
ftp 123.124.125.125
```

The FTP server can be activated or deactivated using the FTPSER parameter on the CNSYS command.

The appropriate user name and password to use depends on whether the FTPPWD option has been set to Y using the CNSYS MML command.

When FTPPWD = Y, FTP access must use the fixed user name “siuftp” in conjunction with the normal MML access password as configured by setting the CNSYS parameter PASSWORD.

Access to the Signaling Gateway using other user accounts except “siuftp” is denied. Note also that access is denied if FTPPWD = Y, but there is no MML password.

When FTPPWD=N, no FTP access is permitted. Access with “siuftp” or any other user account is disabled. Therefore, the user is strongly advised to activate FTP password security.

The state of FTPPWD can be viewed using the CNSYP command.

For additional security, the Signaling Gateway supports the use of Secure Shell (SSH) access for FTP operation. The user should use the CNSYS command to allow only secure FTP access to the unit, for example:

```
CNSYS:SECURE=Y;
```

For a client on a UNIX operating system, the command sequence to log in for FTP access using the sftp application is:

```
sftp -l ftp@<IP Address>
```

The user is also prompted to enter the password for the siuftp login account.

The secure connection to a unit can also be established from Windows® operating system using the appropriate SSH software.

4.10 Backing Up System Software

The user can backup a binary copy of the Signaling Gateway software for restoration later.

4.10.1 Software Backup to a Remote Data Centre

The procedure to perform a software backup to an Remote Data Center (RDC) is as follows:

1. The user should enter:

```
CNBUI: RDC=<rdc id>, DTYPE=SOFTWARE,
       DIRECTORY=<subdirectory>,FILE=<filename>;
```

   to request that the software be backed up to an RDC where the software file <filename.tgz> is stored in a subdirectory in the ftproot.

   Note: The user should **not** use a filename of “sgw” when backing up to the local RDC.

   The unit indicates that the configuration has been successfully backed up by displaying the “EXECUTED” response to the CNBUI command.

4.11 Updating System Software

The configuration data, stored in non-volatile memory, is not affected by a software update.

Normal operation of the software update procedure uses MML to update the software. While a software update can take place while phone calls are in progress, the new software is not activated until the system is restarted.

On completion of the software update, the user must perform a system restart. MML commands are restricted to the following “safe” mode commands CNSYS, CNUPI and STRDP commands, as well as the alarm log and configuration print commands.

If the user aborts the software update or the software update process fails, the system alarm “SW mismatch” is activated and the user is restricted to “safe” mode commands. If the user restarts the system in this state, the system restarts in “safe” mode running limited configuration only software.

Note: Prior to performing a system upgrade, it is recommended that the user makes a backup of the system configuration using the procedures specified in Section 4.12, “Backing Up Configuration Data” on page 25.

4.11.1 Software Update from a Remote Data Centre

The procedure to perform a software update from a Remote Data Center (RDC) is as follows:

1. The user should enter:

```
CNUPI:DTYPE=SOFTWARE,RDC=<rdc id>,
      DIRECTORY=<subdirectory>,FILE=<filename>;
```

   to request that the software be updated from a RDC where the software update files are stored in a subdirectory in the ftproot.

   Note: The directory and filename are optional and when not used the system looks for the file sgw.tgz in the ftproot directory. If <filename> is specified, it should be specified without an extension.

2. Once the user has confirmed that the software should be upgraded, the distribution file is transferred to the Signaling Gateway without further interaction with the user. The unit indicates that the file has been successfully transferred by displaying the “EXECUTED” response to the CNUPI command.
3. On completion, the user should restart the system by executing the MNRSI command.

4.11.2 Software Update from CD-ROM

The following procedure assumes that a CD-ROM with the updated software has already been created. Perform the software update as follows:

1. Insert the CD in the CD ROM drive.
2. Enter the following command:

```
CNUPI:DTYPE=SOFTWARE,DIRECTORY=<subdirectory>,FILE=<filename>;
```

to request that the software be updated from CD ROM.

Note: The directory and filename are optional and when not used the system looks for the file sgw.tgz in the CR ROM root directory.

3. Prompts are displayed asking first if the user is certain that they wish to upgrade the software and then to put the first software update disk in the CD ROM drive.

   The software is uploaded from the distribution CD to the Signaling Gateway.

   The unit indicates that all files have been successfully transferred by displaying the "EXECUTED" response to the CNUPI command.
4. The user should restart the system by entering the MML command MNRSI.

4.11.3 Software Update from Startup

The user is also able to update the software from system start. Installation of software from system start is not normal operating procedure and should only be used if the user is unable to install software via MML. A failed installation of software from system start can result in the system failing to operate. The procedure to install software from system start using either FTP or CD is as follows:

Software Update from Startup Using FTP

1. Rename the software distribution to sgw.tgz.
2. Establish an FTP session (see Section 4.9, "FTP Access" on page 23).
3. Set the FTP transfer mode to "Binary", since the software file is a binary file.
4. Transfer the software to the Signaling Gateway by typing the command "put sgw.tgz sgw.tgz".

   Note: The Signaling Gateway uses a case-sensitive file system. Therefore, it is necessary to specify sgw.tgz in lowercase.
5. Terminate the FTP session by entering "quit" or "bye".
6. Establish an MML session and restart the unit by typing the MNRSI command.

   The machine then boots and completes the upgrade. Once the upgrade is complete, the machine is accessible via the MML.
7. Check the software version using the CNSWP command.

Software Update from Startup Using a CD

1. Place the CD containing the file sgw.tgz in the CD ROM drive.
2. Restart the system.

   The new software is installed and started automatically.

4.12 Backing Up Configuration Data

The user can backup a binary copy of the Signaling Gateway configuration for restoration later.

4.12.1 Configuration Backup to Remote Data Centre

The procedure to perform a configuration backup to an RDC is as follows:

1. The user should enter:

```
CNBUI:RDC=<rdc id>, DTYPE=CONFIG,
       DIRECTORY=<subdirectory>,FILE=<filename>;
```

to request that the configuration be backed up to an RDC where the configuration file <filename.CF3> is stored in a subdirectory in the ftproot.

Note: The user should **not** use a filename of "SDC" when backing up to the local RDC.

The unit indicates that the configuration has been successfully backed up by displaying the "EXECUTED" response to the CNBUI command.

4.13 Updating Configuration Data

Valid configuration data can be stored by the Signaling Gateway at a Remote Data Center (RDC) using the CNBUI command (see Section 4.12), on CD ROM or on a remote machine accessible via FTP. This configuration data can then be restored as described in the following subsections.

4.13.1 Configuration Update from a Remote Data Centre

The procedure to perform a configuration update from a Remote Data Center (RDC) is as follows:

1. The user should enter:

```
CNUPI:DTYPE=CONFIG,RDC=<rdc id>,
       DIRECTORY=<subdirectory>,FILE=<filename>;
```

   to request that the configuration be updated from a RDC where the configuration update file <filename.CF3> is stored in a subdirectory in the ftproot.

   Note: The directory and filename are optional and when not used the system looks for the SDC.CF3 file in the ftproot directory.

   The unit indicates that the configuration has been successfully transferred by displaying the “EXECUTED” response to the CNUPI command.

2. The user should then restart the system by entering the MML command MNRSI.

4.13.2 Configuration Update from CD ROM

The procedure for a configuration update from CD ROM using MML is as follows:

1. The user should enter:

```
CNUPI:DTYPE=CONFIG, DIRECTORY=<subdirectory>,FILE=<filename>;
```

   to request that the configuration file be updated from CD ROM.

   Note: The directory and filename are optional and when not used the system looks for the SDC.CF3 file in the CD ROM root directory.

   The configuration file is uploaded from CD ROM. The unit indicates that the configuration has been successfully updated by displaying the “EXECUTED” response to the CNUPI command.

2. The user should then restart the system by entering the MML command MNRSI.

4.13.3 Configuration Update from Startup

The user is also able to install a previously backed-up system configuration from system start.

Note: Installation of configuration from system start is not normal operating procedure and should only be used if the user is unable to install configuration via MML. A failed installation of configuration from system start can result in the complete loss of system configuration.

The procedures to install configuration from system start using either FTP or CD are described below.

Configuration Update from Startup using FTP

1. Rename the software distribution to SDC.CF3.
2. Establish an FTP session (see Section 4.9, “FTP Access” on page 23).
3. Set the FTP transfer mode to “Binary”, since the software file is a binary file.
4. Transfer the configuration to the Signaling Gateway by entering the command “put SDC.CF3 SDC.CF3”.

   Note: The Signaling Gateway uses a case-sensitive file system. Therefore, it is necessary to specify SDC.CF3 in uppercase.

5. Terminate the FTP session by entering “quit” or “bye”.
6. Establish an MML session and restart the unit by typing the MNRSI command.

   The machine then boots and completes the upgrade. Once the upgrade is complete, the machine is accessible via the MML.

Software Update from Startup using a CD

1. Place the CD containing the sgw.tgz file in the CD ROM drive.
2. Restart the system.
   The new configuration is installed and started automatically.

4.14 System Licenses

Each mode of operation (SIU, DSC or SGW) supports a number of different protocol and software options. This section describes how additional licenses are purchased and installed on a system.

4.14.1 Purchasing System Licenses

The user should place an order using their normal sales channel quoting the *item market name* for the software option required. The supported item market names are:

For the SIU Mode of operation, the following protocols may be run on the unit by purchasing the licenses:

- SS7SBG20ISUP
- SS7SBG20SCCPCL (connectionless SCCP)
- SS7SBG20SCCPCO (connection-orientated SCCP)
- SS7SBG20TCAP
- SS7SBG20MAP
- SS7SBG20IS41
- SS7SBG20INAP

For the SGW Mode of operation, which incorporates the protocols MTP2, MTP3, M3UA and M2PA (inter-links), the user needs to purchase the license:

- SS7SBG20SGW

If the user also requires to use M2PA Network facing links, this will require purchase of the license:

- SS7SBG20M2PA

For the DSC Mode of operation, which incorporates the protocols MTP2, MTP3, ISUP, ISDN, DPNSS and M2PA (inter-links), the user needs to purchase the license:

- SS7SBG20DSC

If the user also requires to use M2PA Network facing links, this will require purchase of the license:

- SS7SBG20M2PA

At this point in the process, there is no need to know details of the specific Dialogic® SS7G2x product on which the option is to be installed (the target SS7G2x).

The order ships through the normal supply channels and the user receives a paper *Licence Certificate*. The certificate contains the full licence terms for using the SS7G20 software option and a unique *Licence ID* that is needed to activate the licence.

When the Licence Certificate is received, the user should first read the full terms of the software licence:

- If the user does not agree with the software licence terms, they must contact their sales channel for a refund and must not activate the software licence.
- If the user agrees the software licence terms, they can continue with the process following.

The next stage is to identify the SS7G2x on which the software option is to be activated. To do this, it is necessary to obtain the UNIT ID for the SS7G2x, which is obtained by executing the CNSYP MML command on the target SS7G2x.

Once the user has the Licence ID and the UNIT ID, the licence can be activated on the Dialogic® SS7G2x products. *Licence Activation* is the process of submitting the License ID and UNIT ID so that a *Licence File* can be generated and sent for installation on the target SS7G2x.

The Licence Activation process is web-based and the Licence File is sent by email.
The user performs License Activation by visiting the web site:
http://membersresource.dialogic.com/ss7/license/license.asp (or an alternative URL if listed on the Licence Certificate).

The user is asked to provide the following basic information:

- Name
- Company
- Country
- Email address (this is used to send the Licence File)

The user is then asked for the following information about the SS7G2x:

- Operating System - Enter “Systems Product”.
- Host ID - Enter the UNIT ID.
- User Machine Identification (a string, typically the Signaling Gateway name, used by the user to identify the SS7G2x).

The user must list the Licence ID (taken from the Licence Certificate) for each protocol that is to be licensed on the target SS7G2x.

Once all this information has been entered, the form should be submitted. The user receives confirmation that their request has been submitted. Subsequently, they receive their Licence File by email.

For installing system licenses, see Section 4.14.2, “Installing System Licenses” on page 28.

4.14.2 Installing System Licenses

This section describes how additional licenses are installed on an SS7G2x. Each SS7G2x is licensed to run specific components of the protocol stack. The CNSYP command provides a printout that shows which components are licensed on a particular unit. Each unit is uniquely identified by a unit identity value, which is displayed as the UNITID parameter in the CNSYP command output.

The License File, purchased as described in Chapter 3, “System Licenses”, is a simple text file. The contents of the file are similar to the following:

```
FEATURE SGW_G20 INTEL 1.000 permanent uncounted \
HOSTID=00d0b8a1aba1 SIGN=1E48C256bb1a
```

Normal operation of the license update procedure uses MML to update the system’s purchasable licenses with the file taken directly from a Remote Data Centre (RDC).

Note: If the licensing upgrade fails, the unit restores the previous licensing level.

4.14.3 License Update from Remote Data Centre

The procedure to perform a license update from the a Remote Data Center (RDC) is as follows:

1. The user should enter:

   ```
   CNUPI:DTYPE=LICENSE,RDC=<rdc id>,DIRECTORY=<subdirectory>;
   ```
   to request that the license be updated from a RDC where the license file is stored in a subdirectory in the ftproot.
2. Once the user has confirmed that the license should be updated, the license file is transferred to the Signaling Gateway without further interaction with the user. The unit indicates that the file has been successfully transferred by displaying the “EXECUTED” response to the CNUPI command.

4.14.4 License Update by FTP

The user is also able to install licenses from system start.

> **Note:** Installation of licenses from system start is not normal operating procedure and should only be used if the user is unable to install licenses via MML.

The procedure to install licenses from system start is as follows:

1. Rename the purchased license file to sgw.lic.
2. Establish an FTP session (see Section 4.9, "FTP Access" on page 23).
3. Set the FTP transfer mode to "ASCII", since the license file is a text file.
4. Transfer the software license to the Signaling Gateway by typing the command "put sgw.lic sgw.lic".

   > **Note:** The Signaling Gateway uses a case-sensitive file system. Therefore, it is necessary to specify sgw.lic in lowercase.

5. Terminate the FTP session by entering "quit" or "bye".
6. Establish an MML session and restart the unit by typing the MNRSI command.

   The machine then boots and completes the upgrade. Once the upgrade is complete, the machine is accessible via MML.

7. Check the licenses using the CNSYP command.

Chapter 5: Parameter Definitions

5.1 Parameter Table

Table 2 lists all parameters and details the possible values.

All numeric parameters are entered and output in decimal notation.

<text character> is either <lower case letter>, <upper case letter>, <digit>, $, or -. The use of quotation marks to delimit text strings is not required.

Table 2. Parameter Definitions

Name	Description	Range	Notes
ALP	Sequential reference number of an entry in the Alarm Log	1 to 9999	
AS	Logical reference for a SIGTRAN Application Server	1 to 200	
BCIC	The circuit identification code of an SS7 circuit that is the base CIC of a CIC Range	0 to 4095	
BPOS	Board position number (for signaling boards)	1 to 3	
BRDTYPE	Board type descriptor, in the format: xxxxxx-y-z where: • xxxxxx = board type • y = number of signaling links configured on the board • z = number of PCM ports on the board See Section 5.4, “Board Types” on page 39.	One of the following: • SPCI2S-4-2 • SPCI2S-8-2 • SPCI4-4-4 • SPCI4-8-4 • SS7HDP-64-4	
BUILDOUT	The buildout type: • 0 - Setting for E1 devices. • 1 - T1 short haul 0 - 110 ft. • 2 - T1 short haul 0 - 110 ft. • 3 - T1 short haul 110 - 220 ft. • 4 - T1 short haul 220 - 330 ft. • 5 - T1 short haul 330 - 440 ft. • 6 - T1 short haul 440 - 550 ft. • 7 - T1 short haul 550 - 660 ft. • 8 - T1 long haul LB0 (-0dB) • 9 - T1 long haul LB0 (-7.5dB) • 10 - T1 long haul LB0 (-15dB) • 11 - T1 long haul LB0 (0dB TR62411)	0 to 11	Default = • 0 for E1 • 1 for T1
C7LINK	Logical reference for an SS7 signaling link	1 to 128	
C7RT	Logical reference of an SS7 route	1 to 128	
CLA	Alarm class number. One of: • 0 = Unreported (the alarm is logged, but it does not trigger an alarm relay and is not included in SNMP output. • 1 = Minor (triggering the MNR alarm LED and relay) • 2 = Major (triggering the MJR alarm LED and relay) • 3 = Critical (triggering the CRT alarm LED and relay)	0 to 3	
CODE	Fault code of a system alarm	1 to 256	
CONFIRM	Confirmation of a password used to provide password control access to MML	0 to 12 <text character>	
CRTYPE	The type of continuous record: • ALARM – alarms that have been reported to the alarm log	ALARM	

Table 2. Parameter Definitions (Continued)

Name	Description	Range	Notes
DATE	Calendar date, in the format: xxxx-yy-zz where: • xxxx – 4 digit year • yy – 2 digit month • zz – 2 digit day	xxxx – 1990 to 2037 yy – 01 to 12 zz – 01 to 31	
DBITS	Number of data bits on V.24 port	7 or 8	Default = 8
DEST	Signaling Gateway Destination Point ID	1 to 512	
DIRECTORY	Directory name on a remote data centre.	0 to 12 <text character>	
DISCARD	Whether data can be discarded	Y or N	Default = N
DOMAIN	Domain	One of: • IP • MTP	
DPC	SS7 destination point code	0 to 16777215	
DTYPE	The type of saving/loading operation to be performed from a remote data centre. See Section 5.2, “Remote Operations” on page 37.	One of: • SOFTWARE • CONFIG • LICENSE	
DUPLEX	Specifies whether a connection is duplex (Y) or simplex (N).	Y or N	Default = N
END	Specifies whether the Signaling Gateway's end of the SIGTRAN link is acting as either a client (C) or a server (S).	C or S	
EQU	Signaling processor hardware identifier in the format: x-y where: • x = board position (BPOS) • y = signaling link within the board. **NOTE:** V.11 links can only use processors 1 and 2.	x – 1 to 3 y – 1 to 64	
ETH	Ethernet port number in the range 1 to 4, where: • ETH=1 corresponds to physical port ENET 1 • ETH=2 corresponds to physical port ENET 2 • ETH=3 corresponds to physical port ENET LNK A • ETH=4 corresponds to physical port ENET LNK B	1 to 4	
FF	PCM frame format: • G704 – Normal E1 format described in G.704 • CRC4 – Normal E1 format with CRC4 checksum generation • CRC4C – Normal E1 format with CRC4 checksum generation. Compatible with non-CRC4 operation. • SF – 12 frame multiframe (D3/D4) • ESF – 24-frame multiframe • CRC6 – ESF format with CRC6 checksum generation • CRC4G706 – CRC4 G.706 compatible mode **NOTE:** Out of CRC4-multiframe, E-Bits are transmitted as zeroes.	One of: • G704 • CRC4 • CRC4C • SF • ESF • CRC6 • CRC4G706	Default = • G704 for E1 • SF for T1
FILE	File name on a Remote Data Centre (RDC)	0 to 12 <text character>	

Table 2. Parameter Definitions (Continued)

Name	Description	Range	Notes
FTPPWD	FTP Password enabled parameter. Set to Y to enable ftp password protection, or N to disable password protection.	Y or N	Default = Y
FTPSER	Indicates whether the Signaling Gateway can act as a ftp server or not. Set to Y to enable the ftp server, or N to disable the ftp server.	Y or N	Default = Y
GATEWAY	An IP gateway used to reach other networks when the destination is not on the local subnet. Specified using dot notation, that is, www.xxx.yyy.zzz	www – 0 to 255 xxx – 0 to 255 yyy – 0 to 255 zzz – 0 to 255	Default = 0.0.0.0
HPORT	Host SCTP port	1 to 65535	2905 for M3UA SNLINKs. 3565 for M2PA SNLINKs.
INHIBIT	Invoke/revoke MTP3 management inhibiting of an SS7 signaling link	Y or N	Default = N
IPADDR	Internet Protocol (IP) address of the Signaling Gateway Ethernet port 1 specified using dot notation, that is, www.xxx.yyy.zzz	www – 0 to 255 xxx – 0 to 255 yyy – 0 to 255 zzz – 0 to 255	Default = 0.0.0.0
IPADDR2	Internet Protocol (IP) address of the Signaling Gateway Ethernet port 2 specified using dot notation, that is, www.xxx.yyy.zzz	www – 0 to 255 xxx – 0 to 255 yyy – 0 to 255 zzz – 0 to 255	Default = 0.0.0.0
IPADDR3	Internet Protocol (IP) address of the Signaling Gateway LNKA port specified using dot notation, that is, www.xxx.yyy.zzz	www – 0 to 255 xxx – 0 to 255 yyy – 0 to 255 zzz – 0 to 255	Default = 0.0.0.0
IPADDR4	Internet Protocol (IP) address of the Signaling Gateway LNKB port specified using dot notation: www.xxx.yyy.zzz	www – 0 to 255 xxx – 0 to 255 yyy – 0 to 255 zzz – 0 to 255	Default = 0.0.0.0
IPGW	Logical reference for an Internet Protocol Gateway	1 to 31	
IPNW	IP network identifier specified using dot notation, that is, www.xxx.yyy.zzz	www – 0 to 255 xxx – 0 to 255 yyy – 0 to 255 zzz – 0 to 255	Default = 0.0.0.0
IR	Logical reference for a incoming route	1 to 32	
ITS	The input timeslot in a cross connection (in the case of a duplex cross connection, this is also the output timeslot for the reverse direction). The format is: xx-y-zz where: • xx = board position (BPOS) • y = PCM within a board • zz = timeslot	xx – 1 to 3 y – 1 to 4 zz – 1 to 31	
LABEL	Text label.	0 to 12 <text character>	
LC	PCM line coding	One of: • HDB3 • AMI • B8ZS	Default = • HDB3 for E1 • B8ZS for T1
LINES	Number of MML lines per page	10 to 99	Default = 25
LSH	Load share across link sets	Y to N	Default = N
LS	Logical reference of an SS7 link set, which can contain a number of signaling links	1 to 64	

Table 2. Parameter Definitions (Continued)

Name	Description	Range	Notes
LS1	Primary link set associated with an SS7 route	1 to 64	
LS2	Secondary linkset associated with an SS7 route	1 to 64	
LSSIZE	Maximum number of SS7 links allowed in the link set. The link set size is used to determine the load sharing algorithm used across the link set.	1 to 16	
M56K	56kbits signaling mode: • 0 - 64 kbits/s used • 1 - 56kbits/s enabled (bit 8 not used) • 2 - 48kbits/s enabled (bits 7 and 8 not used) • 3 - Recover clock from V.11 interface • 4 - Transmit clock to V.11 interface	0 to 4	Default = 0 M56K modes 3 and 4 can only be set on boards with SIGTYPE = SS7
MASK	IP network mask specified using dot notation, that is, www.xxx.yyy.zzz	www – 0 to 255 xxx – 0 to 255 yyy – 0 to 255 zzz – 0 to 255	
MINREC	The minimum number of records held by the Signaling Gateway before transfer	100 to 200	
NA	Network appearance	0 to 2147483647	
NASP	Number of ASP required in load sharing mode	0 to 32	Default = 0
NC	Signaling Gateway SS7 network context	1 to 4	
NI	Network Indicator for an SS7 link set	0 to 3	
OPC	SS7 Originating Point Code	0 to 16777215	
OTS	The output timeslot in a cross connection (in the case of a duplex cross connection, this is also the input timeslot for the reverse direction). The format is: xx-y-zz where: • xx = board position (BPOS) • y = PCM within a board • zz = Timeslot	xx – 1 to 3 y – 1 to 4 zz – 1 to 31	
PAGE	The page of data to be printed	1 to 10	Default = 1
PARITY	Parity option on V.24 port. Affects transmit parity only, parity is ignored on receive.	One of: • ODD • EVEN • NONE	Default = NONE
PASSWORD	Used to specify the password for either remote login access or to provide password control for Signaling Gateway MML	0 to 12 <text character>	
PCM	PCM interface on a board in the format: xx-y where: • xx = board position (BPOS) • y = PCM within a board	xx – 1 to 3 y – 1 to 4	
PCMD	Application Server Point Code mode: • ANY – If any Application Server is in service then the Point Code the Application Server exists within is considered to be up. • ALL – Only when all the Application Servers within a Point Code are in service will the Point Code they exist within be considered to be up.	One of: • ANY • ALL	

Table 2. Parameter Definitions (Continued)

Name	Description	Range	Notes
PCMTYPE	The type of PCM in use	One of: • T1 • E1	
PCR	Preventive Cyclic Retransmission	Y or N	Default = N
PER	Personality configuration	0 to 255	Default = 0
PERIOD	A period of time in the format: xx:yy:zz where: • xx = 2 digit hour • yy = 2 digit minute • zz = 2 digit second	xx – 00 to 23 yy – 00 to 59 (yy must be 00, when xx is 23) zz – 00 to 59 (zz must be 00, when xx is 23)	
PORT	V24 port identifier **NOTE:** Port 1 is not physically accessible.	1 to 4	
PPORT	The SCTP port associated with the peer on a SIGTRAN link	1 to 65535	2905 for M3UA SNLINKs 3565 for M2PA SNLINKs
PRTYPE	The type of periodic report: • MSC7 – periodic reporting of traffic measurements for CCS SS7 links. • MSPCM – periodic reporting of traffic measurements for PCMs. • MSSL – periodic reporting of traffic measurements for SIGTRAN links. • MSEP – periodic reporting of Ethernet port measurements. • MSSY – periodic reporting of System measurements.	One of: • MSC7 • MSSL • MSPCM • MSEP • MSSY	
PTMODE	Mode for serial port	One of: • NONE • DTRDSR • TELNET	Default = • DTRDSR for ports 1 and 2 • TELNET for ports 3 and 4
RANGE	CIC range	0 to 4095	
RC	The routing context of a SIGTRAN link within an Application Server	0 to 2147483647	
RDC	Remote Data Centre (RDC) identifier	1 to 4	
RDC1	First choice RDC for a continuous record or periodic report	1 to 4	
RDC2	Second choice RDC for a continuous record or periodic report. Zero indicates no RDC is assigned.	0 to 4	Default = 0
RECORD	The identifier for a continuous data collection record	1 to 6	
REPORT	The identifier for a periodic data collection report	1 to 5	
RESET	Performs a reset operation	Y or N	Default = N

Table 2. Parameter Definitions (Continued)

Name	Description	Range	Notes
RESTART	Specifies the type of restart operation, which can be one of the following: • NORMAL - The system undergoes a full system restart, resetting the hardware, operating system and SIU software. This is the default behavior. NORMAL resets should be used for software upgrade or for maintenance events. • SOFT - The system restarts the application software. Prior to a soft restart, the Signaling boards are reset. SOFT resets may be used for a more rapid system restart after updating the system configuration or licenses. However, if a new software distribution is to be installed, the system performs a NORMAL restart. • HALT - The system shuts down without a subsequent restart. **Caution: Once the system has been halted, the only way to restart the unit is by physically pressing the Power switch on the front panel of the chassis.**	One of: • NORMAL • SOFT • HALT	
RKI	Routing Key Index An identifier for either a complete routing key or part of a routing key.	1 to 512	
RKTAB	Routing Key Table A table of particular routing keys.	1 to 8	
RTPRI	Destination route priority	One of: • NONE • MTP	Default = NONE
RTS	A timeslot within a PCM interface on a board used for monitoring information received by the monitored object. The format is: xx-y-zz where: • xx = board position (BPOS) • y = PCM within a board • zz = timeslot	xx – 1 to 3 y – 1 to 4 zz – 1 to 31	
SBITS	Number of stop bits on V.24 port	1 to 2	Default = 1
SECURE	Secure operation. When active offers a higher level of security. The use of the parameter is command specific. See the CNSYS and SNSLI command descriptions for more information.	Y or N	Default = N
SEQ	Sequence number	1 to 32	
SG	Reserved		
SI	Reserved		
SIGTYPE	Type of software loaded onto signaling board	SS7	
SLC	Signaling link code uniquely identifying a signaling link within a link set	0 to 15	
SNMP	Whether SNMP should be active on the system	Y or N	Default = N
SNRT	Reserved		
SNTYPE	The type of operation of the SIGTRAN link	One of: • SGM3UA • M2PA	
SNLINK	Logical reference for a SIGTRAN link	1 to 200	

Table 2. Parameter Definitions (Continued)

Name	Description	Range	Notes
SPEED	The speed of an Ethernet port. The values 10, 100, 100 select 10 MHz, 100 MHz and 1 GHz respectively. An "H" appended to the value indicates half-duplex operation; values without the appended "H" are full-duplex operation.	One of: • AUTO • 10 • 100 • 1000 • 10H • 100H • 1000H	Default = AUTO
SRTX	Number of times a packet of SIGTRAN information can be retransmitted before determining that the SIGTRAN link has gone out of service	2 to 10	
SS7MD	SS7 signaling mode: • ITU14 – ITU operation with 14 bit Point Code • ITU16 – ITU operation with 16 bit Point Code • ITU24 – ITU operation with 24 bit Point Code • ANSI – ANSI operation with 24 bit Point Code	One of: • ITU14 • ITU16 • ITU24 • ANSI	
STS	A timeslot within a PCM interface on a board used for monitoring information sent by the monitored object. The format is: xx-y-zz where: • xx = board position (BPOS) • y = PCM within a board • zz = timeslot	xx – 1 to 3 y – 1 to 4 zz – 1 to 31	
SUBNET	Subnet mask for the network to which the Signaling Gateway is connected specified using dot notation, that is, www.xxx.yyy.zzz	www – 0 to 255 xxx – 0 to 255 yyy – 0 to 255 zzz – 0 to 255	Default = 255.255.255.0
SUBNET2	2nd Subnet mask for the network to which the Signaling Gateway is connected specified using dot notation, that is, www.xxx.yyy.zzz	www – 0 to 255 xxx – 0 to 255 yyy – 0 to 255 zzz – 0 to 255	Default = 255.255.255.0
SUBNET3	3rd Subnet mask for the network to which the Signaling Gateway is connected specified using dot notation, that is, www.xxx.yyy.zzz	www – 0 to 255 xxx – 0 to 255 yyy – 0 to 255 zzz – 0 to 255	Default = 255.255.255.0
SUBNET4	4th Subnet mask for the network to which the Signaling Gateway is connected specified using dot notation, that is, www.xxx.yyy.zzz	www – 0 to 255 xxx – 0 to 255 yyy – 0 to 255 zzz – 0 to 255	Default = 255.255.255.0
SYNCPRI	The priority the PCM is given to provide clock synchronization: • 0 – Indicates never provide clock synchronization • 1 – Highest priority that PCM should provide clock synchronization • 32 – Lowest priority, that is, other PCMs have precedence	0 to 32	Default = 0
SYSID	System identity	0 to 12 <text character>	
SYSREF	The system reference number	0 to 999	Default = 0
SYSTYPE	The type of system to be run	One of: • SGW • DSC • SIU	

Table 2. Parameter Definitions (Continued)

Name	Description	Range	Notes
TIME	Time of day in the format: xx:yy:zz where: • xx – 2 digit hour • yy – 2 digit minute • zz – 2 digit second	xx – 00 to 23 yy – 00 to 59 zz – 00 to 59	
TLO	Auto log off time (in minutes)	1 to 60	Default = 30
TLOW	Log off warning time (in minutes)	0 to 60	Default = 25
TMSEC	Timer values in milliseconds associated with a timer number (resolution is 100ms)	100 to 10000 (in integer multiples of 100)	
TO	Signaling system dependent timer number. As specified in the particular signaling system's list of timers.	1 to 999	
TS	A timeslot within a PCM interface on a board in the format: xx-y-zz where: • xx = board position (BPOS) • y = PCM within a board • zz= Timeslot	xx – 1 to 3 y – 1 to 4 zz – 1 to 31	
TSEC	Timer values in seconds associated with a timer number	1 to 3000	
TTYPE	Timer Type See Section 5.3, "Signaling Gateway Timers" on page 38 for definitions of Signaling Gateway "CONV" specific timers.	One of: • MTP3 • MTP3A • SCTP • CONV	
USER	User name	0 to 12 <text character>	

5.2 Remote Operations

Table 3 gives the possible remote operation types.

Table 3. Remote Operation Types

DTYPE	Description
SOFTWARE	Selecting this operation allows the user to upload a new software version.
CONFIG	Selecting this operation allows the user to upload a previously backed up version of the configuration.
LICENSE	Selecting this operation allows the user to upload new software licenses.

5.3 Signaling Gateway Timers

5.3.1 Signaling Gateway-Specific Timers

Table 4 shows the Signaling Gateway specific timers. Timers for specific protocols are given in subsequent tables in this section.

Table 4. Signaling Gateway Specific Timers

T0	Range (seconds)	Default (seconds)	Description
5	5 to 20	7	Wait for board response guard timer. This timer starts when internal messages are sent to a signaling board and stopped when an acknowledgement is received. On timer expiry, it reports an error. If the internal message sent to a board related to setting up a speech path for a call, then the call is released using internal token 135.
7	2 to 10	3	MML wait for maintenance confirmation timer. The timer is started when a MML maintenance request is performed. It is stopped when a confirmation from the remote site to the maintenance request is received. On timer expiry, a confirmation to the request is internally generated allowing further MML commands to be entered.

5.3.2 MTP3-Specific Timers

MTP3 ITU timers are given in Table 5.

Table 5. MTP3 ITU Timers

TO	Range (milliseconds)	Default (milliseconds)	Description
1	500 to 1200	1000	Delay to avoid message mis-sequencing on changeover
2	700 to 2000	1500	Waiting for changeover acknowledgement
3	500 to 1200	1000	Time controlled diversion-delay to avoid mis-sequencing on changeback
4	500 to 1200	1000	Waiting for changeback acknowledgement (first attempt)
5	500 to 1200	1000	Waiting for changeback acknowledgement (second attempt)
6	500 to 1200	1000	Delay to avoid message mis-sequencing on controlled rerouting
10	30 to 60 sec.	45 sec.	Waiting to repeat signaling route set test message
12	800 to 1500	1200	Waiting for uninhibit acknowledgement
13	800 to 1500	1200	Waiting for force uninhibit
14	2000 to 3000	3000	Waiting to start signaling route set congestion test
17	800 to 1500	1000	Delay to avoid oscillation of initial alignment failure and link restart
22	180 to 360 sec.	270 sec.	Local inhibit test timer
23	180 to 360 sec.	270 sec.	Remote inhibit test timer
24	N/A	N/A	Reserved

MTP3 ANSI timers are given in Table 6.

Table 6. MTP3 ANSI Timers

TO	Range (milli-seconds)	Default (milliseconds)	Description
1	500 to 1200	1000	Delay to avoid message mis-sequencing on changeover
2	700 to 2000	1500	Waiting for changeover acknowledgement
3	500 to 1200	1000	Time controlled diversion-delay to avoid mis-sequencing on changeback
4	500 to 1200	1000	Waiting for changeback acknowledgement (first attempt)
5	500 to 1200	1000	Waiting for changeback acknowledgement (second attempt)

Table 6. MTP3 ANSI Timers (Continued)

TO	Range (milli-seconds)	Default (milliseconds)	Description
6	500 to 1200	1000	Delay to avoid message mis-sequencing on controlled rerouting
10	30 to 60secs	45 sec.	Waiting to repeat signaling route set test message
12	800 to 1500	1200	Waiting for uninhibit acknowledgement
13	800 to 1500	1200	Waiting for force uninhibit
14	2000 to 3000	3000	Waiting to start signaling route set congestion test
17	800 to 1500	1000	Delay to avoid oscillation of initial alignment failure and link restart
21	N/A	N/A	Reserved
22	180 to 360 sec.	270 sec.	Local inhibit test timer **NOTE:** This timer is referred to as timer T20 in the ANSI specification.
23	180 to 360 sec.	270 sec.	Remote inhibit test timer **NOTE:** This timer is referred to as timer T21 in the ANSI specification.
24	N/A	N/A	Reserved

5.3.3 SCTP-Specific Timers

SCTP-specific timers are given in Table 7.

Table 7. SCTP-Specific Timers

TO	Range (milliseconds)	Default (milliseconds)	Description
1	100 to 500	500	Minimum retransmission timeout (RTO)
2	100 to 60000	2000	Maximum retransmission timeout (RTO)
3	T1 to T2	1000	Retransmission timeout RTO initial value
4	100 to 3000	1000	SCTP Heartbeat timer

5.4 Board Types

Table 8 shows the signaling board types.

Table 8. Board Types

BRDTYPE	Description
SPCI2S-4-2	SS7G2x(DSC) Signaling board with 4 signaling links configured and 2 PCMs. Used when configuring signaling boards with a SIGTYPE of SS7.
SPCI4-4-4	SS7G2x(DSC) Signaling board with 4 signaling links configured and 4 PCMs. Used when configuring signaling boards with a SIGTYPE of SS7.
SS7HDP-64-4	SS7G2x(DSC) Signaling board with 64 signaling links configured and 4 PCMs. Used when configuring signaling boards with a SIGTYPE SS7.

Chapter 6: Command Definitions

6.1 Command Groups

The commands are broken down into a number of command groups as follows:

- Alarm Commands
- Configuration Commands
- SS7 Signaling Commands
- IP Commands
- MML Commands
- Maintenance Commands
- Measurement Commands
- Remote Data Centre Commands
- Signaling Gateway Commands
- SIGTRAN Commands
- Status Commands

6.2 Command Notation

The following conventions are used in the command definitions:

- Items in square brackets [ ] are optional.
- Items separated by a vertical bar | are alternatives, only one of which can be used.
- Curly brackets { } are used to designate a group of optional items of which at least one must be selected.
- The sequence of three dots ... is used to indicate that a number of values can be entered, linked by the **&** or **&&** operator.

6.3 Command Attributes

The following symbols are used to indicate command attributes:

- **CONFIG -** The command affects configuration data.
- **PROMPT -** A “DANGEROUS” command, which must be confirmed by the operator.

6.4 Alarm Commands

The alarm commands include:

- ALCLS - Alarm Class Set
- ALCLP - Alarm Class Print
- ALFCP - Alarm Fault Code Print
- ALLIP - Alarm List Print
- ALLOP - Alarm Log Print
- ALREI - Alarm Reset Initiate
- ALTEI - Alarm Test Initiate
- ALTEE - Alarm Test End

6.4.1 ALCLS – Alarm Class Set

Synopsis

This command assigns an alarm class value to a specified fault code(s).

The alarm class (CLA) is used to determine whether the alarm is classed as Minor, Major or Critical and in turn governs the alarm LED, relay and SNMP alarm that are activated when the condition exists.

Each alarm code (CODE) has a factory-set default class. See Chapter 8, “Alarm Fault Code Listing” for the factory default for each alarm code.

Syntax

```
ALCLS:CLA=,CODE=…;
```

Prerequisites

None

Attributes

CONFIG

Examples

```
ALCLS:CLA=1,CODE=20;
```

6.4.2 ALCLP – Alarm Class Print

Synopsis

This command gives a printout of the fault codes belonging to a particular alarm class. If the CLA parameter is omitted, all fault codes are printed out.

Syntax

```
ALCLP[:CLA=];
```

Prerequisites

None

Attributes

None

Examples

```
ALCLP;
ALCLP:CLA=2;
```

Output Format

```
Alarm Fault Codes
CODE  CLA  TITLE
11    2    Processor1 fail
EXECUTED
```

6.4.3 ALFCP – Alarm Fault Code Print

Synopsis

This command gives a printout of the alarm class of the specified fault code(s).

The alarm class (CLA) is used to determine whether the alarm is classed as Minor, Major or Critical and in turn governs the alarm LED, relay and SNMP alarm that are activated when the condition exists.

Each alarm code (CODE) has a factory-set default class. See Chapter 8, “Alarm Fault Code Listing” for the factory default for each alarm code.

Syntax

```
ALFCP[:CODE=…];
```

Prerequisites

None

Attributes

None

Examples

```
ALFCP;
ALFCP:CODE=8;
```

Output Format

```
Alarm Fault Codes
CODE        CLA       TITLE
8           2         In-band AIS
EXECUTED
```

6.4.4 ALLIP – Alarm List Print

Synopsis

This command gives a printout of all ACTIVE fault codes stored in the system's alarm log.

Each fault code (CODE) is associated with an alarm class (CLA) which may be Minor, Major or Critical. The alarm class in turn governs which alarm LED, relay or SNMP alarm is activated when the condition exists.

The command provides an indication of the time that the alarm occurred (OCCURRED), the alarm class (CLA indicating either a System, PCM or signaling failure) as well as an alarm code specific identifier (ID) and diagnostic field (DIAG).

See Chapter 8, "Alarm Fault Code Listing" for the definitions of the alarm code specific parameters.

> ***Note:*** The meaning of the ID field depends on the alarm code and is described in Chapter 8, "Alarm Fault Code Listing".

Syntax

```
ALLIP;
```

Prerequisites

None

Attributes

None

Examples

```
ALLIP;
```

Output Format

```
SYSTEMIDENT1 Alarm List (active alarms) 1996-12-01 00:00:54
ALP  CODE ID  DIAG CLA OCCURRED            CLEARED            TITLE
107     1 103    0 1 A 2001-10-30 10:54:48                    PCM loss
 74     1 104    0 2 A 2001-10-30 10:54:27                    PCM loss
EXECUTED
```

6.4.5 ALLOP – Alarm Log Print

Synopsis

This command gives a printout of the alarm log. If no code or class is entered, the whole log is output.

Each fault code (CODE) is associated with an alarm class (CLA) which may be Minor, Major or Critical. The alarm class in turn governs which alarm LED, relay or SNMP alarm that is activated when the condition exists.

The command provides and indication of the time the alarm occurred (OCCURRED) and, if it has done so, the time the alarm cleared (CLEARED). The output from the command indicates, the alarm class (CLA indicating either a System, PCM or signaling failure) as well as an alarm code specific identifier (ID) and a diagnostic field (DIAG). The C or A character in the CLA field indicates the current status as either A (active) or C (cleared).

See Chapter 8, “Alarm Fault Code Listing” for definitions of the alarm code specific parameters.

Syntax

```
ALLOP[:CODE=…];
ALLOP[:CLA=…];
```

Prerequisites

None

Attributes

None

Examples

```
ALLOP:CODE=20;
ALLOP:CLA=1&&2;
ALLOP;
```

Output Format

```
SYSTEMIDENT1 Alarm Log 1996-12-01 00:00:54
ALP  CODE ID  DIAG CLA OCCURRED            CLEARED             TITLE
107     1 103    0 1 A 2001-10-30 10:54:48 2001-10-30 10:54:53 PCM loss
 74     1 104    0 2 A 2001-10-30 10:54:27 2001-10-30 10:59:53 PCM loss
EXECUTED
```

Note: The C or A character in the CLA field indicates the current status as A (active) or C (cleared). The meaning of the ID field depends on the alarm code and is described in Chapter 8, “Alarm Fault Code Listing”.

6.4.6 ALREI – Alarm Reset Initiate

Synopsis

This command removes alarms that have cleared from the alarm log.

Attempts to remove commands that do not have the status CLEARED are rejected.

If parameter ALP is omitted, all alarms with status CLEARED are removed.

Syntax

```
ALREI[:ALP=];
```

Prerequisites

None

Attributes

None

Examples

```
ALREI:ALP=100;
ALREI;
```

6.4.7 ALTEI – Alarm Test Initiate

Synopsis

The command generates an active test alarm of the specified class, which is entered in the alarm log.

Alarm tests can be useful for validating the operation of hardware such as LEDS and alarm relays, as well as ensuring proper communication with an SNMP manager without impacting the operation of the system.

Syntax

```
ALTEI:{[CLA=1]|[CLA=2]|[CLA=3]};
```

Prerequisites

- Only one test alarm can be active at any one time. Test alarms can only be generated for classes 1, 2 and 3.

Attributes

None

Examples

```
ALTEI:CLA=3;
```

6.4.8 ALTEE – Alarm Test End

Synopsis

Clears a test alarm.

Syntax

```
ALTEE;
```

Prerequisites

- The alarm test must already have been initiated.

Attributes

None

Examples

```
ALTEE;
```

6.5 Configuration Commands

The configuration commands include:

- CNBOI - Configuration Board Initiate
- CNBOE - Configuration Board End
- CNBOP - Configuration Board Print
- CNBUI - Configuration Back Up Initiate
- CNMOI - Configuration Monitor Initiate
- CNMOE - Configuration Monitor End
- CNMOP - Configuration Monitor Print
- CNPCI - Configuration PCM Initiate
- CNPCC - Configuration PCM Change
- CNPCE - Configuration PCM End
- CNPCP - Configuration PCM Print
- CNRDI - Configuration Remote Data Centre Initiate
- CNRDC - Configuration Remote Data Centre Change
- CNRDE - Configuration Remote Data Centre End
- CNRDP - Configuration Remote Data Centre Print
- CNSWP - Configuration Software Print
- CNSYS - Configuration System Set
- CNSYP - Configuration System Print
- CNTDS - Configuration Time and Date Set
- CNTDP - Configuration Time And Date Print
- CNTOS - Configuration Timeout Value Set
- CNTOP - Configuration Timeout Value Print
- CNTSP - Configuration Timeslot Print
- CNUPI - Configuration Update Initiate
- CNXCI - Configuration Cross Connect Initiate
- CNXCE - Configuration Cross Connect End
- CNXCP - Configuration Cross Connect Print

6.5.1 CNBOI – Configuration Board Initiate

Synopsis

This command defines a new board on the system.

The user should specify the board position (BPOS) within the unit, the physical type of the board (BRDTYPE) and the signaling type (SIGTYPE), which identifies the software that will run on the board.

See Section 7.1.2, “Boards and PCMs” on page 136 for a more detailed description of board configuration.

Syntax

```
CNBOI:BPOS=,BRDTYPE=,SIGTYPE=;
```

Prerequisites

- No board has already been defined for the specified board position.
- A board must physically exist for the board position and be licensed for the signaling gateway.
- A board type of SS7HDP must have a signaling type of SS7.

Attributes

CONFIG

Examples

```
CNBOI:BPOS=1,BRDTYPE=SPCI4-4-4,SIGTYPE=SS7;
CNBOI:BPOS=1,BRDTYPE=SPCI2S-4-2,SIGTYPE=SS7;
CNBOI:BPOS=3,BRDTYPE=SS7HDP-64-4,SIGTYPE=SS7;
```

6.5.2 CNBOE – Configuration Board End

Synopsis

This command deassigns a board from a board position.

Syntax

```
CNBOE:BPOS=;
```

Prerequisites

- A board has been defined for the specified board position.
- No signaling processor on the board has been allocated to a signaling link.
- No PCM on the board is configured.
- The board has been blocked.

Attributes

CONFIG

Examples

```
CNBOE:BPOS=3;
```

6.5.3 CNBOP – Configuration Board Print

Synopsis

This command gives a print out of all configured boards.

Syntax

```
CNBOP;
```

Prerequisites

None

Attributes

None

Examples

```
CNBOP;
```

Output Format

```
Board Configuration
BPOS  BRDTYPE     SIGTYPE
1     SPCI2S-4-2  SS7
3     SPCI2S-4-2  SS7
EXECUTED
```

6.5.4 CNBUI – Configuration Back Up Initiate

Synopsis

This command backs up either the configuration data or the current software distribution to a Remote Data Centre (RDC).

A filename (FILE) should be entered on the command line without a suffix. The command automatically reads the filename with a suffix. The command determines the suffix from the DTYPE parameter. For example, if the user specifies FILE=CFG and DTYPE=CONFIG, the full filename would be CFG.CF4.

The file suffix and default filename for each DTYPE is as follows:

- For DTYPE=CONFIG, the filename suffix is .CF3. If a filename is not specified, the default is “SDC”.
- For DTYPE=SOFTWARE, the filename suffix is .tgz. If a filename is not specified, the default is “sgw”.

Optionally, the file may be backed up to a subdirectory (DIRECTORY) of the account on the RDC.

> ***Note:*** During execution of this command, the system may not respond for up to three minutes while the command is being executed.

Syntax

```
CNBUI:RDC=,DTYPE=,[FILE=,][DIRECTORY=,];
```

Prerequisites

- The RDC should be initiated and not blocked.
- The DTYPE can only be CONFIG or SOFTWARE.
- If the RDC is the “local” RDC, a FILE name of SDC or SGW is not allowed.

Attributes

None

Examples

```
CNBUI:RDC=1,DTYPE=CONFIG,FILE=SDC;
```

6.5.5 CNMOI – Configuration Monitor Initiate

Synopsis

This command initiates the monitoring of an object on the Signaling Gateway. An object is currently a C7LINK.

For signaling, the STS monitors information sent from the EQU of the signaling link and the RTS monitors information received by the signaling link.

Syntax

```
CNMOI:C7LINK=,STS=,RTS=;
```

Prerequisites

- If specified, the C7LINK has already been initiated and must have a TS and EQU.
- The PCM on which STS exists must have already been initiated and STS must be within the correct range for the PCM type (0 to 31 for E1 and 1 to 24 for T1 PCMs).
- The PCM on which RTS exists must have already been initiated and RTS must be within the correct range for the PCM type (0 to 31 for E1 and 1 to 24 for T1 PCMs).
- STS is not already assigned elsewhere on the system for output.
- RTS is not already assigned elsewhere on the system for output.
- A signaling link can only be monitored once.

Attributes

CONFIG

Examples

```
CNMOI:C7LINK=1,STS=3-3-15,RTS=5-3-16;
```

6.5.6 CNMOE – Configuration Monitor End

Synopsis

This command ends the monitoring of an object. An object is currently only an signaling link.

Syntax

```
CNMOE:C7LINK=;
```

Prerequisites

- The C7LINK is being monitored.

Attributes

CONFIG

Examples

```
CNMOE:C7LINK=1;
```

6.5.7 CNMOP – Configuration Monitor Print

Synopsis

This command is used to obtain a print out of the objects being monitored. An object is currently only a signaling link.

For signaling, the STS monitors information sent from the EQU of the signaling link and the RTS monitors information received by the signaling link.

Syntax

```
CNMOP;
```

Prerequisites

None

Attributes

None

Examples

```
CNMOP;
```

Output Format

```
Monitoring Configuration
C7LINK STS    RTS
1      3-3-1  3-3-2
3      3-3-3  3-3-4
EXECUTED
```

6.5.8 CNPCI – Configuration PCM Initiate

Synopsis

This command configures a PCM (PCM) for T1 or E1 operation (PCMTYPE) on a board such that it is available for signaling or voice. The command optionally configures the PCM to be used as a potential synchronization source for the system (SYNCPRI). The command also allows the frame format (FF) and line code (LC) to be configured. See Section 7.1.2, “Boards and PCMs” on page 136 for a more detailed description of PCM configuration.

Syntax

```
CNPCI:PCM=,PCMTYPE=,[SYNCPRI=,][FF=,][LC=,][IDLE=][BM=][BUILDOUT=,];
```

Prerequisites

- The board on which the PCM exists has been initiated.
- The PCM has not already been initiated.
- For a PCMTYPE of E1, the LC can be set to HDB3 and the FF can be set to G704, CRC4, CRC4C or CRC4G706.
- For a PCMTYPE of T1, the LC can be set to AMI or B8ZS and the FF can be set to SF, ESF or CRC6.
- An FF of CRC4G706 can only be set on a board type of SS7HDP.
- The BUILDOUT parameter can only have a value of 0 for E1 and a value of 1 for T1s on boards of a type other than SS7HDP.

Attributes

CONFIG

Examples

```
CNPCI:PCM=1-1,PCMTYPE=E1,SYNCPRI=1;
```

6.5.9 CNPCC – Configuration PCM Change

Synopsis

This command allows changes to the configuration of a PCM.

Syntax

```
CNPCC:PCM=,{[PCMTYPE=,]|[SYNCPRI=,][FF=,][LC=,][IDLE=][BM=][BUILDOUT=,]};
```

Prerequisites

- The PCM has already been initiated.
- For a PCMTYPE of E1, the LC can be set to HDB3 and the FF can be set to G704, CRC4, CRC4C or CRC4G706.
- For a PCMTYPE of T1, the LC can be set to AMI or B8ZS and the FF can be set to SF, ESF or CRC6.
- An FF of CRC4G706 can only be set on a board type of SS7HDP.
- The BUILDOUT parameter can only have a value of 0 for E1 and a value of 1 for T1s on boards of a type other than SS7HDP.

Attributes

CONFIG

Examples

```
CNPCC:PCM=1-1,SYNCPRI=3;
```

6.5.10 CNPCE – Configuration PCM End

Synopsis

This command ends the configuration of a PCM such that it is unavailable for voice or signaling.

Syntax

```
CNPCE:PCM=;
```

Prerequisites

- No timeslot on the PCM has been assigned to voice, signaling monitoring or cross connections.
- The board on which the PCM exists has been blocked.

Attributes

CONFIG

Examples

```
CNPCE:PCM=1-1;
```

6.5.11 CNPCP – Configuration PCM Print

Synopsis

This command gives a printout of all the configured PCMs.

Syntax

```
CNPCP;
```

Prerequisites

None

Attributes

None

Examples

```
CNPCP;
```

Output Format

```
PCM Configuration
PCM     PCMTYPE LC      FF      SYNCPRI IDLE  BUILDOUT
1-2     E1      HDB3    G704    6       2A    0
2-2     E1      HDB3    G704    1       2A    0
3-1     T1      B8ZS    SF      2       2A    7
 EXECUTED
```

6.5.12 CNRDI – Configuration Remote Data Centre Initiate

Synopsis

This command is used to configure Remote Data Centre (RDC) so that data from periodic report or continuous recording can be transferred to that location. The connection itself is established when the RDC is unblocked.

An RDC is an account, with an FTP logon name (USER) and password (PASSWORD) on a remote system (IPADDR) operating as an FTP server. No proprietary software is required to run on the remote system.

> ***Note:*** If an RDC has previously been ended, but a file transfer was already in progress, subsequent CNRDIs using that RDC fail with “NO SYSTEM RESOURCES” until the file transfer has completed.

To configure the Signaling Gateway to act itself as an RDC, the user must specify a local address (127.0.0.1) together with the “siuftp” account name and password.

> ***Note:*** Local operation functions only if the ftp server on the system is active.

Syntax

```
CNRDI:RDC=,IPADDR=,USER=,PASSWORD=,[LABEL=,];
```

Prerequisites

- The RDC is not already initiated.
- The IP address is not already in use.

Attributes

CONFIG

Examples

```
CNRDI:RDC=1,IPADDR=255.123.0.124,USER=JOHN,PASSWORD=BAZZA123;
```

6.5.13 CNRDC – Configuration Remote Data Centre Change

Synopsis

This command is used to change the configuration of a Remote Data Centre (RDC).

Syntax

```
CNRDC:RDC=,{[IPADDR=,][USER=,][PASSWORD=,][LABEL=,]};
```

Prerequisites

- The RDC is already initiated and blocked.
- If specified, the IP address is not already in use.
- Remote data operation must be allowed by the system.

Attributes

CONFIG

Examples

```
CNRDC:RDC=1,IPADDR=194.192.184.77,USER=JOHN,PASSWORD=BAZZA23;
```

6.5.14 CNRDE – Configuration Remote Data Centre End

Synopsis

This command is used to end a Remote Data Centre (RDC).

Syntax

```
CNRDE:RDC=;
```

Prerequisites

- The RDC is already initiated.
- The RDC is blocked.
- The RDC is not attached to a continuous record or periodic report.

Attributes

CONFIG

Examples

```
CNRDE:RDC=1;
```

6.5.15 CNRDP – Configuration Remote Data Centre Print

Synopsis

This command is used to print out the Remote Data Centre parameters.

The password is not printed.

Syntax

```
CNRDP;
```

Prerequisites

None

Attributes

None

Examples

```
CNRDP;
```

Output Format

```
Remote Data Centre Configuration
RDC  IPADDR           USER         PASSWORD     LABEL
1    194.192.184.33   JOHN         ********     PRIMARY
2    127.0.0.1        siuftp       ********     Local
EXECUTED
```

6.5.16 CNSWP – Configuration Software Print

Synopsis

This command is used print out the version numbers of the software operating on the main CPU and signaling boards within a Signaling Gateway. The command also displays the library version numbers for each protocol configured on the unit.

Syntax

```
CNSWP;
```

Prerequisites

None

Attributes

None

Output Format

```
Software Configuration
SS7G20      V3.02

Board Codefiles
SYS   SPCI  V1.16

Protocol Libraries
MTP3  CPU   V5.01
MTP2  SPCI  V5.03
EXECUTED
```

6.5.17 CNSYS – Configuration System Set

Synopsis

This command is used to enter the system identity string, personality setting, IP address of the Signaling Gateway, system reference number, and to turn on and off certain features and signaling systems on the Signaling Gateway.

If the IP address used to login to the unit for the telnet session is changed, the user is automatically logged out of the session. However, the user can log in again without delay using the new IP address.

The user can specify whether they wish to allow ftp access to the Signaling Gateway by using the FTPSER parameter. The Signaling Gateway can act as an ftp server to allow update of configuration, software and purchasable licenses. For security, it is recommended that ftp server access is switched off when the user does not need to execute these functions. The user can disable FTPSER by setting the parameter to N. Activation or deactivation of the ftp server takes immediate effect.

The user can specify whether they wish to restrict access to the Signaling Gateway so that it operates only over secure shell (SSH) by using the SECURE parameter. By default, there is no restriction allowing the use normal telnet and ftp access. The user can enable SECURE operation by setting the parameter to Y. Activation or deactivation of SECURE operation takes immediate effect.

Activation of SNMP requires a system restart.

When a password is specified, all new MML sessions apart from serial port 2 (COM2) require a password before entry.

> ***Note:*** IPADDR, IPADDR2, IPADDR3, IPADDR4 correspond to physical Ethernet ports **ENET 1**, **ENET 2**, **ENET LNK A**, **ENET LNK B** respectively, as marked on the rear of the SS7G2x chassis.

The SIU supports resilient IP connectivity when the user configures a team of two ports in an active/standby role. Two IP bonding teams can be created from the four ethernet ports available. A bonding team, assigned a single IP address, consists of a primary (active) port and a secondary (standby) port. The secondary port IP address should be set to one of the following values:

- STANDBY1 - The configured IP address acts as the standby port in a team with IPADDR.
- STANDBY2 - The configured IP address acts as the standby port in a team with IPADDR2.
- STANDBY3 - The configured IP address acts as the standby port in a team with IPADDR3.
- STANDBY4 - The configured IP address acts as the standby port in a team with IPADDR4.

See Section 7.6.1, “IP Port Bonding” on page 142 for more information.

The system is delivered with a pre-configured default IPADDR set to the value of 192.168.0.1. This is set to allow the user to have immediate access to the telnet interface over a private network. As part of their initial configuration, the user should change the IPADDR to a value consistent with their IP network.

The personality parameter is used to select customer-specific, non-standard operating functionality for the Signaling Gateway. To achieve the standard operating functionality, the personality should be set to the default value (that is, zero). Unless otherwise notified, all customers should select the standard operating functionality.

See Section 7.1.1, “System Configuration” on page 135 for a more detailed description of system configuration.

Syntax

```
CNSYS:{[SYSID=,]|[SYSREF=,]|[PER=,]|[SECURE=,]|[FTPSER=,]|[FTPPWD=,]|[SNMP=,]|
[GATEWAY=,]}
CNSYS:{[IPADDR=][SUBNET=,]};
CNSYS:{[IPADDR2=][SUBNET2=,]};
CNSYS:{[IPADDR3=][SUBNET3=,]};
CNSYS:{[IPADDR4=][SUBNET4=,]};
CNSYS:PASSWORD=,CONFIRM=,
```

Prerequisites

- When changing the personality or activating/deactivating signaling protocols, all boards and groups within the system must be blocked.
- A password, if provided, must be confirmed using the CONFIRM parameter to ensure that the password has not been mistyped.
- The user cannot enter a PER parameter value that already exists in the system.
- The user cannot specify an IP address, subnet or gateway value that already exists in the system.

Attributes

CONFIG

Examples

```
CNSYS:SYSID=STATION1,PER=2,IPADDR=255.123.0.123;
```

6.5.18 CNSYP – Configuration System Print

Synopsis

This command is used to print the system configuration. The configuration items include the unit identity (UNIT ID), Software options and the unit's IP configuration.

Software options not licensed on the unit do not appear in the list. Most of these configuration items are set using the CNSYS command, which also contains more details of other options. The "Password" value shows "********" if a password is set and blank if a password is not set.

Syntax

```
CNSYP;
```

Prerequisites

None

Attributes

None

Examples

```
CNSYP;
```

Output Format

```
System Configuration
UNITID:     0004238734ef
SYSID:
SYSREF:     0
PASSWORD:   ********
FTPPWD:     N
FTPSER:     Y
SECURE:     N
PER:        0
IPADDR:     172.28.148.99
SUBNET:     255.255.255.0
IPADDR2:    170.28.148.100
SUBNET2:    255.255.255.0
IPADDR3:    170.28.148.101
SUBNET3:    255.255.255.0
IPADDR4:    0.0.0.0
SUBNET4:    255.255.255.0
GATEWAY:    172.28.148.1
SNMP:       N
SGW:        Y
DSC:        N
SIU:        N
EXECUTED
```

Note: The protocol and mode parameters are only present if licensed. When a protocol or mode is active, the parameter shows the value "Y", and when inactive, the parameter shows the value "N".

6.5.19 CNTDS – Configuration Time and Date Set

Synopsis

This command is used to specify the date (DATE) and time (TIME) as used by the system. System time is used by the Signaling Gateway to indicate the time an alarm occurred or cleared and to provide timestamps for such things as measurements and data records.

See the CNTDP command to verify the time and date settings.

Syntax

```
CNTDS:{[DATE=,][TIME=,]};
```

Prerequisites

- The date cannot be changed if periodic reports or continuous records are configured.

Attributes

CONFIG

Examples

```
CNTDS:DATE=2001-10-03,TIME=18:32:21;
```

6.5.20 CNTDP – Configuration Time And Date Print

Synopsis

This command is used to print the system date and time.

Syntax

```
CNTDP;
```

Prerequisites

None

Attributes

None

Examples

```
CNTDP;
```

Output Format

```
2001-10-03 09:04:02
EXECUTED
```

6.5.21 CNTOS – Configuration Timeout Value Set

Synopsis

This command is used to change the value of a timer for a particular signaling system.

The user should specify the timer type (TTYPE), the timer itself (TO) and time that it should be set to, expressed in either seconds (TSEC) or milliseconds (TMSEC).

> ***Note:*** Some signaling system timer values are not changeable.

See the CNTOP command to verify timer values. See Section 5.3, “Signaling Gateway Timers” on page 38 for the definition of signaling system specific timers.

Syntax

```
CNTOS:TTYPE=,TO=,{TSEC=|TMSEC=};
```

Prerequisites

None

Attributes

CONFIG

Examples

```
CNTOS:TTYPE=MTP3,TO=7,TSEC=30;
```

6.5.22 CNTOP – Configuration Timeout Value Print

Synopsis

This command is used to print the value of either a single timer or all the timers for a particular protocol module. (Refer to CNTOS command to set timer values.)

Syntax

```
CNTOP:TTYPE=,[TO=,];
```

Prerequisites

None

Attributes

None

Examples

```
CNTOP:TTYPE=MTP3;
```

Output Format

```
Timeout Values:
TTYPE  TO     TSEC   TMSEC
MTP3   1      60
MTP3   2      360
MTP3   3      120
MTP3   4      360
MTP3   5      5
MTP3   6      5
MTP3   7      3
MTP3   10     60
EXECUTED
```

6.5.23 CNTSP – Configuration Timeslot Print

Synopsis

This command is used to print the configuration of all timeslots on a PCM.

A timeslot on a PCM can be allocated to signaling, voice, cross connect, monitoring or it can be unallocated. Data is printed for a timeslot when it is acting as an outgoing timeslot.

A timeslot can act as an outgoing timeslot for the following types:

- SIG - Carries signaling information. It forms a duplex connection.
- OTS - Acts as an outgoing timeslot for a cross connection. It may form a duplex connection.
- STS - The outgoing timeslot monitoring the send direction of an object.
- RTS - The outgoing timeslot monitoring the receive direction of an object.

> ***Note:*** An object is currently only a signaling link.

For signaling, the STS monitors information sent from the EQU of the signaling link and the RTS monitors information received by the signaling link.

Syntax

```
CNTSP:PCM=;
```

Prerequisites

None

Attributes

None.

Examples

```
CNTSP:PCM=3-3;
```

Output Format

```
PCM Timeslot Configuration
TS       TYPE C7LINK ITS
3-3-22   SIG  6
3-3-24   OTS         4-4-4
3-3-25   RTS  7
3-3-25   STS  8
EXECUTED
```

6.5.24 CNUPI – Configuration Update Initiate

Synopsis

This command is used to update configuration data, software or a license on the Signaling Gateway. The operation involves reading files containing either configuration data, software or a license from a Remote Data Centre (if specified) or CD ROM and loading it into memory. Optionally, the file may be read from a subdirectory (DIRECTORY) of the account on the RDC.

A FILE name should be entered on the command line without a suffix. The command automatically reads the file name with a suffix. The command determines the suffix by use of the DTYPE parameter. For example, the file CFG.CF3 for a DTYPE of CONFIG would be entered as CFG.

The filename suffix for DTYPE=CONFIG is .CF3.

The filename suffix for DTYPE=SOFTWARE is .tgz.

The filename suffix for DTYPE=LICENSE is .lic.

If not specified, the default filename for a DTYPE=CONFIG is “SDC”.

If not specified, the default filename for a DTYPE=SOFTWARE is “sgw”.

If not specified, the default filename for a DTYPE=LICENSE is “sgw”.

> ***Note:*** During execution of this command, there system may not respond for up to 3 minutes while the command is being executed.

Syntax

```
CNUPI:DTYPE=,RDC=,[DIRECTORY=,][FILE=,];
```

Prerequisites

- If the RDC is specified, it should be initiated and not blocked.

Attributes

CONFIG

Examples

```
CNUPI:RDC=1,DTYPE=CONFIG,DIRECTORY=AUTH,FILE=CFG;
```

6.5.25 CNXCI – Configuration Cross Connect Initiate

Synopsis

This command initiates a cross connect path across the Signaling Gateway between 2 PCM timeslots; the incoming timeslot (ITS) and the outgoing timeslot (OTS). If DUPLEX is not set to Y, a simplex cross connect is initiated from ITS to OTS.

Syntax

```
CNXCI:OTS=,ITS=,[DUPLEX=];
```

Prerequisites

- The PCM on which the OTS exists must have already been initiated and the OTS must be within the correct range for the PCM type (0 to 31 for E1 and 1 to 24 for T1 PCMs).
- The PCM on which the ITS exists must have already been initiated and the ITS must be within the correct range for the PCM type (0 to 31 for E1 and 1 to 24 for T1 PCMs).
- OTS is not already assigned elsewhere on the system for output.
- ITS is not already assigned elsewhere on the system for input.

Attributes

CONFIG

Examples

```
CNXCI:OTS=1-1-16,ITS=2-1-16,DUPLEX=Y;
```

6.5.26 CNXCE – Configuration Cross Connect End

Synopsis

This command ends a Cross Connect connection across the converter.

Syntax

```
CNXCE:OTS=,[DUPLEX=,];
```

Prerequisites

- The OTS must already be initiated as an OTS in a Cross Connect connection path.
- If DUPLEX=Y is specified, a duplex connection must already exist for the specified OTS.

Attributes

CONFIG

Examples

```
CNXCE:OTS=1-1-16;
```

6.5.27 CNXCP – Configuration Cross Connect Print

Synopsis

This command is used to obtain a printout of Cross Connect connection path(s).

Syntax

```
CNXCP:PCM=;
CNXCP:OTS=;
CNXCP;
```

Prerequisites

None

Attributes

None

Examples

```
CNXCP:PCM=1-2;
CNXCP:OTS=1-1-16;
CNXCP;
```

Output Format

```
Path Configuration
OTS      ITS      DUPLEX
1-1-16   2-1-16   Y
EXECUTED
```

6.6 SS7 Signaling Commands

The SS7 signaling commands include:

- C7LSI - CCS SS7 Link Set Initiate
- C7LSC - CCS SS7 Link Set Change
- C7LSE - CCS SS7 Link Set End
- C7LSP - CCS SS7 Link Set Print
- C7RTI - CCS SS7 Route Initiate
- C7RTC - CCS SS7 Route Change
- C7RTE - CCS SS7 Route End
- C7RTP - CCS SS7 Route Print
- C7SLI - CCS SS7 Signaling Link Initiate
- C7SLC - CCS SS7 Signaling Link Change
- C7SLE - CCS SS7 Signaling Link End
- C7SLP - CCS SS7 Signaling Link Print

6.6.1 C7LSI – CCS SS7 Link Set Initiate

Synopsis

This command is used to initiate the SS7 link set (LS) between the point code of the unit, the Originating Point Code (OPC), and an adjacent point code, the Destination Point Code (DPC). The user should specify the maximum number of links in the link set (LSSIZE), the SS7 Signaling mode (SS7MD), which identifies the point code size and mode of operation, and the Network Context (NC) the link set exists within.

See Section 7.2, "Signaling Configuration" on page 136 for a more detailed description of the SS7 Signaling configuration.

This command is used to initiate the SS7 link set. Note that the DPC (Destination Point Code) is the adjacent Point Code for the link set.

Syntax

```
C7LSI:LS=,OPC=,DPC=,LSSIZE=,NI=,SS7MD=,NC=,;
```

Prerequisites

- The SS7 link set has not already been initiated.
- The SS7MD associated with a NC cannot be different to an SS7MD associated with the same NC anywhere else in the system.
- The NC/DPC combination must be different for all link sets.
- If SS7MD indicates 14-bit Point Code, OPC and DPC must be less than or equal to 16383.
- If SS7MD indicates 16-bit Point Code, OPC and DPC must be less than or equal to 65535.
- Only one OPC can exist within a network context.

Attributes

CONFIG

Examples

```
C7LSI:LS=1,NC=1,OPC=1,DPC=2,LSSIZE=2,SS7MD=ITU14,NI=0;
```

6.6.2 C7LSC – CCS SS7 Link Set Change

Synopsis

This command allows changes to the configuration of an SS7 link set.

Syntax

```
C7LSC:LS=,{[OPC=,][DPC=,][LSSIZE=,][NC=,][NI=,]};
```

Prerequisites

- The SS7 link set has already been initiated.
- All configured SS7 links must be blocked.

  Note: After blocking, an SS7 link cannot be unblocked until all the boards processing the SS7 signaling are blocked and then unblocked.

- The LSSIZE cannot be set to less than the number of links attached to the link set.
- DPC must be different across link sets.
- If SS7MD indicates a 14-bit Point Code, OPC and DPC must be less than or equal to 16383.
- Only one OPC can exist within a network context.
- The NC/DPC combination must be different for all link sets.
- The NC/OPC combination must be different for all link sets.

Attributes

CONFIG

Examples

```
C7LSC:LS=1,OPC=1,DPC=2,LSSIZE=2;
```

6.6.3 C7LSE – CCS SS7 Link Set End

Synopsis

This command is used to end the SS7 link set.

Syntax

```
C7LSE:LS=;
```

Prerequisites

- There should be no signaling links attached to the link set.
- All configured SS7 links within the system must be blocked.

  Note: After blocking, an SS7 link cannot be unblocked until all the boards processing the SS7 signaling are blocked and then unblocked.
- There are no C7 Routes using this link set.

Attributes

CONFIG

Examples

```
C7LSE:LS=1;
```

6.6.4 C7LSP – CCS SS7 Link Set Print

Synopsis

This command obtains a printout of the attributes for the SS7 link set. If no link is specified, the values for all link sets are shown.

Syntax

```
C7LSP:[LS=,];
```

Prerequisites

None

Attributes

None

Examples

```
C7LSP;
```

Output Format

```
CCS SS7 Link Set
LS      NC      OPC       DPC       NI      LSSIZE  SS7MD
1       1       1         3         2       2       ITU14
2       2       2         4         0       2       ANSI
EXECUTED
```

6.6.5 C7RTI – CCS SS7 Route Initiate

Synopsis

This command is used to initiate an SS7 Route (C7RT) to a Destination Point Code (DPC) within a Network Context (NC). An SS7 Route utilizes one (LS1) or two (LS2) link sets which route via adjacent point codes to reach the eventual destination (DPC).

On a per network context basis, a default MTP route may be specified. On a per network context basis, traffic for all point codes not known to the Signalling Gateway are routed to the default route. A default route can be specified by setting the DPC value on the route to DFLT.

See Section 7.2, “Signaling Configuration” on page 136 for a more detailed description of the SS7 signaling configuration.

Syntax

```
C7RTI:C7RT=,DPC=,LS1=,NC=,[LS2=,][LSH=,][LABEL=,];
```

Prerequisites

- The NC must be the same as the NC of the underlying link sets.
- The DPC/NC combination must be unique.
- The link set specified has already been initiated.
- If the route is to an adjacent point code, then all links in the linkset to that point code must be either inhibited or blocked.
- Only one default Route can be configured per Network Context.
- If a default route is specified, a network context cannot be configured with a DPC of 0.

Attributes

CONFIG

Examples

```
C7RTI:C7RT=1,LS1=1,DPC=130,LABEL=ROUTE130;
```

6.6.6 C7RTC – CCS SS7 Route Change

Synopsis

This command is used to change the attributes of an SS7 Route. The DPC parameter in this command supports an extra value ‘DFLT’. When a route is specified as default, messages destined for DPCs within the network context that have not been configured by the system is sent to the default route.

Syntax

```
C7RTC:C7RT=,NC=,[DPC=,][LS1=,][LS2=,][LSH=,][LABEL=,];
```

Prerequisites

- If specified, LS2 must have same SS7MD, NI, NC, and OPC as LS1.
- If specified, LS1 must have same SS7MD, NI, NC, and OPC as LS2.
- The specified route has already been initiated.
- Any link set specified has already been initiated.
- The DPC/NC combination (associated with the route’s link sets) must be different for each route.
- If changing any parameter other than the LABEL, all SS7 signaling links must be blocked.
  Note: After blocking, an SS7 link cannot be unblocked until all the boards processing the SS7 signaling are blocked and then unblocked.
- Only one default route can be configured per network context.
- If a default route is specified, a network context cannot be configured with a DPC of 0.

Attributes

CONFIG

Examples

```
C7RTC:C7RT=1,NC=1,LS1=2;
```

6.6.7 C7RTE – CCS SS7 Route End

Synopsis

This command is used to end an SS7 Signaling Route.

Syntax

```
C7RTE:C7RT=,NC=;
```

Prerequisites

- All SS7 signaling links must be blocked.

  Note: After blocking an SS7 link cannot be unblocked until all the boards processing the SS7 signaling are blocked and then unblocked.

- The specified route and NC combination has already been initiated.

Attributes

CONFIG

Examples

```
C7RTE:C7RT=1,NC=1;
```

6.6.8 C7RTP – CCS SS7 Route Print

Synopsis

This command shows the attributes of the specified SS7 Route or range of routes within a network context. If no route or network context is specified, the values for all routes are shown.

Syntax

```
C7RTP;
C7RTP:NC=;
C7RTP:C7RT=,NC=;
```

Prerequisites

None

Attributes

None

Examples

```
C7RTP;
```

Output Format

```
CCITT SS7 Signaling Route Configuration
C7RT    NC DPC      LS1     LS2     LSH     LABEL
1        1  2        1       3       Y       LONDON
2        1  3        2       4       N       EDINBURGH
3        1  DFLT     5               N       DEFAULT
1        2  66       12      13      N       BATH
EXECUTED
```

6.6.9 C7SLI – CCS SS7 Signaling Link Initiate

Synopsis

This command is used to initiate a SS7 Signaling Link (C7LINK).

The command allows the user to specify the signaling processor (EQU), Signaling Timeslot (TS) as well as which SS7 linkset (LS) the link belongs to. The user may alternatively specify an M2PA SIGTRAN link (SNLINK) instead of a processor and timeslot for communication of SS7 information.

See Section 7.2, "Signaling Configuration" on page 136 for a more detailed description of the SS7 signaling configuration.

Syntax

```
C7SLI:C7LINK=,LS=,SLC=,EQU=,TS=,[M56K=,][PCR=,];
C7SLI:C7LINK=,LS=,SLC=,SNLINK=;
C7SLI:C7LINK=,LS=,SLC=,EQU=, M56K=,[PCR=,];
```

Prerequisites

- The specified link has not already been initiated.
- The specified PCM time slot is not already assigned elsewhere in the system.
- The PCM on which the timeslot exists has been initiated.
- The board on which the EQU exists has been initiated.
- The timeslot is a valid timeslot for the PCM type (up to 31 for an E1 PCM and 24 for a T1 PCM).
- The signaling processor specified by the EQU parameter must be equipped with a valid board type and not already assigned to a link.
- The link set has already been initiated.
- The board position specified by EQU must be blocked.
- If M56K is set to 3 or 4, the TS cannot be specified and if M56K is not set to 3 or 4, EQU must be specified.
- Only EQU signaling processors 1 and 2 can be used if M56K is 3 or 4.
- If an SNLINK is present, the EQU, TS, M56K and PCR cannot be present.
- If an SNLINK is specified, its SNTYPE must be M2PA.
- If an SNLINK is specified, it must be initiated, blocked and cannot be associated with any other SS7 link.
- Either a SNLINK or EQU must be present.
- SS7 links can use signaling processors 1 to 4 on a SPCI4 or SPCI2S board or 1 to 64 on a SS7HDP board.

Attributes

CONFIG

Examples

```
C7SLI:C7LINK=4,EQU=3-1,TS=3-3-17,LS=1,SLC=5;
C7SLI:C7LINK=5,SNLINK=1,LS=2,SLC=0;
```

6.6.10 C7SLC – CCS SS7 Signaling Link Change

Synopsis

This command is used to change the attributes of an SS7 signaling link.

Syntax

```
C7SLC:C7LINK=,{[EQU=,][SNLINK=,][TS=,][M56K=,][PCR=,]};
```

Prerequisites

- The specified link has already been initiated.
- The specified PCM time slot is not already assigned elsewhere in the system.
- The PCM on which the timeslot exists has been initiated.
- If specified, the board on which the EQU exists has been initiated.
- If specified, the PCM on which the timeslot exists has been initiated.
- The timeslot is a valid timeslot number for the PCM type (up to 31 for a E1 PCM and 24 for a T1 PCM).
- The signaling processor specified by the EQU parameter must be equipped with a valid board type and not already assigned to a link.
- All links within the link set must be blocked.
- If the EQU, PCR or M56K parameters are specified the link must be blocked and C7 links EQU board must be blocked. To change the other parameters on the C7 link, the link must be inhibited.
- If M56K is set to either 1 or 2, all links on the same board for which M56K is set to 1 or 2 must also use the same M56K value (that is, only one mode of 56kbits/s operation is supported on any board at one time. However, it is possible for some links to operate at 64kbits/s, while others operate at 56kbits/s).
- The signaling processor specified by the EQU parameter must be equipped with a valid board type and not already assigned to a link.
- All links within the link set must be blocked.

  Note: After blocking, an SS7 link cannot be unblocked until all the boards processing the SS7 signaling are blocked and then unblocked.

- If the EQU, PCR or M56K parameters are specified, the link must be blocked and the C7 link's EQU board must be blocked. To change the other parameters on the C7 link, the link must be inhibited.
- If M56K is set to 3 or 4, the TS cannot be specified and if M56K is not set to 3 or 4, the EQU must be specified.
- Only EQU signaling processors 1 and 2 can be used if M56K is 3 or 4.
- If an SNLINK is present, the EQU, TS, M56K and PCR cannot be present.
- If an SNLINK is specified, it's SNTYPE must be M2PA.
- If an SNLINK is specified, it must be initiated, blocked and cannot be associated with any other SS7 link.
- The command cannot change between SNLINK and EQU type C7LINKs.
- SS7 links can use signaling processors 1 to 4 on a SPCI4 or SPCI2S board or 1 to 64 on a SS7HDP board.

Attributes

CONFIG

Examples

```
C7SLC:C7LINK=4,EQU=2-3,TS=3-3-16,M56K=1;
```

6.6.11 C7SLE – CCS SS7 Signaling Link End

Synopsis

This command is used to end an SS7 signaling link.

Syntax

```
C7SLE:C7LINK=;
```

Prerequisites

- The signaling link must be blocked.
- The signaling link must not be monitored.

Attributes

CONFIG

Examples

```
C7SLE:C7LINK=1;
```

6.6.12 C7SLP – CCS SS7 Signaling Link Print

Synopsis

This command is used to obtain a printout of the attributes of SS7 signaling link(s). If no link is specified, all initialized links are output.

Syntax

```
C7SLP:[C7LINK=…];
```

Prerequisites

None

Attributes

None

Examples

```
C7SLP:C7LINK=1;
C7SLP;
```

Output Format

```
Signaling Link Configuration
C7LINK  EQU     TS      SNLINK  LS      SLC     M56K    PCR
1       1-1     1-3-16          1        0        0       N
2       1-2     2-3-16          1        1        0       N
3                            1  2        0        0       N
4                            2  2        1        0       N
EXECUTED
```

6.7 IP Commands

The IP commands include:

- IPEPS - Set Ethernet Port Speed
- IPEPP - Display Ethernet Port Speed
- IPGWI - Internet Protocol Gateway Initiate
- IPGWE - Internet Protocol Gateway End
- IPGWP - Internet Protocol Gateway Print

6.7.1 IPEPS – Set Ethernet Port Speed

Synopsis

This command sets the Ethernet port speed.

Syntax

```
IPEPS:ETH=,SPEED=;
```

Prerequisites

None.

Attributes

None.

Examples

```
IPEPS:ETH=1,SPEED=100;
```

Output Format

```
IPEPS:eth=1,speed=100;
EXECUTED
```

6.7.2 IPEPP – Display Ethernet Port Speed

Synopsis

This command displays the Ethernet port speed. A speed displayed with an H indicates it is halfduplex, otherwise it is full-duplex.

Syntax

```
IPEPP;
```

Prerequisites

None.

Attributes

None.

Examples

```
IPEPP;
```

Output Format

```
ETH SPEED
1   10H
2   100
3   AUTO
4   AUTO
EXECUTED
```

6.7.3 IPGWI – Internet Protocol Gateway Initiate

Synopsis

This command allows the user to specify a route (IPGW) to a IP network (IPNW) via an IP gateway (GATEWAY) for a range of IP addresses within that network as defined by a network mask (MASK).

Syntax

```
IPGWI:IPGW=,MASK=,GATEWAY=,IPNW=;
```

Prerequisites

- The IP gateway ID has not been initiated.
- Two gateways cannot have overlapping IP addresses.

Attributes

CONFIG

Examples

```
IPGWI:IPGW=1,MASK=255.255.255.0,GATEWAY=194.192.185.1,
       IPNW=128.66.1.0;
```

6.7.4 IPGWE – Internet Protocol Gateway End

Synopsis

This command removes an IP route via an IP gateway.

Syntax

```
IPGWE:IPGW=;
```

Prerequisites

- The IP gateway ID has already been initiated.

Attributes

CONFIG

Examples

```
IPGWE:IPGW=1,;
```

6.7.5 IPGWP – Internet Protocol Gateway Print

Synopsis

This command prints out routes via IP gateways.

Syntax

```
IPGWP:[IPGW=];
```

Prerequisites

- If specified, the gateway ID should already have been initiated.

Attributes

None

Examples

```
IPGWP;
```

Output Format

```
IP Gateway Configuration
IPGW MASK              GATEWAY         IPNW
1    255.255.255.0     143.123.202.122 128.66.1.0
2    255.255.255.0     111.155.153.111 143.44.174.0
EXECUTED
```

6.8 MML Commands

The MML commands include:

- MMLOI - MML Log Off Initiate
- MMLOP - MML Log Off Print
- MMLOS - MML Log Off Set
- MMPTC - MML Port Change
- MMPTP - MML Port Print

6.8.1 MMLOI – MML Log Off Initiate

Synopsis

This command ends the current logon session and allows a new session to be used on the port. It does not affect other MML sessions.

Syntax

```
MMLOI;
```

Prerequisites

This command ends the current logon session and allows a new session to be used on the port. It does not affect other MML sessions.

Attributes

CONFIG

Examples

```
MMLOI;
```

6.8.2 MMLOP – MML Log Off Print

Synopsis

This command prints the current logon time-out parameters.

Syntax

```
MMLOP:[PORT=];
```

Prerequisites

None

Attributes

None

Examples

```
MMLOP;
MMLOP:PORT=1;
```

Output Format

```
Log on timeouts
PORT     TLO   TLOW
1        30    25
2        25    20
3        25    30
4        25    35
EXECUTED
```

6.8.3 MMLOS – MML Log Off Set

Synopsis

This command sets the current log-on time-out (TLO) and timeout warning (TLOW) parameters. If TLOW is set to zero, the automatic time-out is disabled. If port (PORT) is omitted, the command applies to all ports.

Syntax

```
MMLOS:{[TLO=,][TLOW=,]}[PORT=,];
```

Prerequisites

None

Attributes

CONFIG

Examples

```
MMLOS:TLO=35;
MMLOS:TLOW=19;
```

6.8.4 MMPTC – MML Port Change

Synopsis

This command sets the data input/output parameters for serial and telnet data ports.

> ***Note:*** Only serial port 2 (COM2) is accessible by the user.

Syntax

```
MMPTC:PORT=,{[BAUD=,][DBITS=,][PARITY=,][SBITS=,][LINES=,][PTMODE=,]};
```

Prerequisites

- No user must be logged on to the port affected.
- For the telnet ports, only the LINES parameter can be changed.

Attributes

CONFIG

Examples

```
MMPTC:PORT=2,BAUD=300;
MMPTC:PORT=2,SBITS=2;
```

6.8.5 MMPTP – MML Port Print

Synopsis

This command gives a printout of the attributes of the serial port. Where the PORT parameter is omitted, the printout is provided for all ports. The connected port executing this command is marked with a "*".

Note: Only serial port 2 (COM2) is accessible by the user.

Syntax

```
MMPTP[:PORT=];
```

Prerequisites

None

Attributes

None

Examples

```
MMPTP:PORT=1;
MMPTP;
```

Output Format

```
Serial Port Configuration
PORT    BAUD    DBITS   SBITS   PARITY  LINES   PTMODE   CONNECTED

1       9600    8       1       NONE    20      DTRDSR
2       1200    7       2       EVEN    8       NONE     *

3                                       25      TELNET

4                                       25      TELNET
EXECUTED
```

6.9 Maintenance Commands

The maintenance commands include:

- MNBLI - Maintenance Blocking Initiate
- MNBLE - Maintenance Blocking End
- MNINI - Maintenance Inhibit Initiate
- MNINE - Maintenance Inhibit End
- MNRSI - Maintenance Restart System Initiate

6.9.1 MNBLI – Maintenance Blocking Initiate

Synopsis

This command initiates blocking for boards, signaling links, remote data centres, SIGTRAN links and SIGTRAN Application Servers. A blocking command removes from use the board, link, route or server covered by the command, it also removes their configuration data from the lower levels of the Signaling Gateway and only configuration management maintains knowledge of their existence.

Possible grouping are:

- SS7 signaling links
- Boards
- Remote Data Centres (RDCs)
- SIGTRAN signaling links
- SIGTRAN Application Servers

If the grouping being blocked is already in the blocked state, no action is taken.

If a C7 link has been inhibited, the inhibiting is removed as part of the blocking action.

Syntax

```
MNBLI:C7LINK=…;
MNBLI:BPOS=…;
MNBLI:RDC=…;
MNBLI:SNLINK=…;
MNBLI:AS=…;
```

Prerequisites

- The item being blocked has been initiated.
- When blocking a board, all SS7 links on the board must already be blocked.
- If this is the last RDC to be blocked, then it cannot be blocked until all continuous records and periodic reports are ended.
- An SNLINK of SNTYPE M2PA can only be blocked if its associated C7LINK is either blocked or inhibited.

Attributes

```
CONFIG,PROMPT
```

Examples

```
MNBLI:SNLINK=12;
MNBLI:C7LINK=4;
```

Output Format

```
Blocking C7LINK 1
Blocking C7LINK 2
EXECUTED
```

6.9.2 MNBLE – Maintenance Blocking End

Synopsis

This command ends the blocked condition of boards, signaling links, remote data centres, SIGTRAN links and SIGTRAN Application Servers and brings them into service. The command restores configuration data to the lower levels of the Signaling Gateway and brings the timeslots into service. Possible grouping are:

- SS7 signaling links
- Boards
- Remote Data Centres (RDCs)
- SIGTRAN signaling links
- SIGTRAN Application Servers

Note: If an RDC has previously been blocked but a file transfer was already in progress, subsequent MNBLE commands which use that RDC fail with “NO SYSTEM RESOURCES” until the file transfer is complete.

Syntax

```
MNBLE:C7LINK=…;
MNBLE:BPOS=…;
MNBLE:RDC=…;
MNBLE:SNLINK=…;
MNBLE:AS=…;
```

Prerequisites

- The item being unblocked has been initiated and is currently blocked.
- When unblocking an SS7 link with a signaling processor (EQU), both the board containing the signaling processor and the board containing the signaling timeslot must already be unblocked.
- An SS7 link with a signaling processor (EQU) cannot be unblocked until all the boards processing the SS7 signaling are blocked and then unblocked.
- An SS7 link cannot be unblocked if it is on a C7 route that has more than one link set and those link sets have either different OPCs, SS7MDs, NCs or NIs.
- An AS cannot be unblocked unless it has a SNLINK attached.
- An M3UA SNLINK must have a default NC or a mapping of an NA into an NC.
- An M3UA SNLINK must have a mapping of an NA into an NC or a default NC matching the AS NC the SNLINK is attached to.
- All the underlying SNLINKs of an AS must have a mapping of an NA into an NC or a default NC matching the AS NC.
- A C7LINK cannot be unblocked if an associated SNLINK is blocked.
- A network facing M2PA C7LINK can only be unblocked if the Signaling Gateway is licensed for M2PA operation.

Note: M2PA can be used for DUAL operation without a license.

Attributes

CONFIG

Examples

```
MNBLE:C7LINK=4;
```

Output Format

```
Unblocking C7LINK 1
EXECUTED
```

6.9.3 MNINI – Maintenance Inhibit Initiate

Synopsis

This command initiates the inhibiting of SS7 signaling. When specified without the INH parameter, the C7 signaling link is deactivated and no further signaling is allowed. When specified with INHIBIT =Y, the SS7 link inhibit message is sent over the signaling link.

Syntax

```
MNINI:C7LINK=…;
MNINI:C7LINK=,INHIBIT=Y;
```

Prerequisites

- When specified without the INHIBIT parameter, the SS7 links have been initiated and are uninhibited.

Attributes

CONFIG, PROMPT

Examples

```
MNINI:C7LINK=5;
```

Output Format

```
Inhibiting C7LINK 23
Inhibiting C7LINK 31
EXECUTED
```

6.9.4 MNINE – Maintenance Inhibit End

Synopsis

This command ends the inhibiting of C7 links. The C7 link is activated and signaling is allowed to proceed. When specified without the INHIBIT parameter, the C7 signaling link is activated and signaling is allowed to proceed. When specified with INHIBIT =N, the SS7 link uninhibit message is sent over the signaling link.

Syntax

```
MNINE:C7LINK=…;
MNINE:C7LINK=,INHIBIT=N;
```

Prerequisites

- When specified without the INHIBIT parameter, the SS7 links have been initiated and are inhibited.

Attributes

CONFIG

Examples

```
MNINE:C7LINK=5;
```

Output Format

```
Uninhibiting C7LINK 23
Uninhibiting C7LINK 31
EXECUTED
```

6.9.5 MNRSI – Maintenance Restart System Initiate

Synopsis

This command restarts the entire system. All current logon sessions are terminated.

If a software update disk is present, in the CD-ROM drive, then the software update procedure commences.

If no software update disk is present, but a CD containing a configuration dump is present, this configuration is loaded into memory and the system restarts.

In all other cases, no change to the system configuration occurs and the state of all links is automatically restored.

If RESET is set to Y, all configuration data is removed.

If SYSTYPE is set, the systems operating mode changes after restart. Possible operation modes are:

- DSC – Digital Signaling Conveter
- SGW – SIGTRAN Signaling Gateway
- SIU – Signaling Interface Unit

Syntax

```
MNRSI:[RESTART=,][RESET=Y,][SYSTYPE=,];
```

Prerequisites

- SYSTYPE can only be set to system types that have been licensed for the unit. See the CNSYP command.

  Note: SIU is always licensed.

Attributes

PROMPT

Examples

```
MNRSI;
MNRSI:RESET=Y;
MNRSI:SYSTYPE=SGW;
```

6.10 Measurement Commands

The measurement commands include:

- MSC7P - Measurements SS7 Print
- MSEPP - Measurement Ethernet Port Print
- MSPCP - Measurements PCM Print
- MSSLP - Measurements SIGTRAN Link Print
- MSSYP - Measurements System Print

6.10.1 MSC7P – Measurements SS7 Print

Synopsis

This command prints traffic measurements for SS7 signaling links. The measurements are cumulative between system startup and the next time the measurements are reset.

The fields have the following meanings:

- C7LINK - SS7 signaling Link.
- OOSDUR - Duration that the link was not in service. This field is not currently supported.
- RXNACK - Number of negative acknowledgements received.

  Note: RXNACK is not applicable for M2PA SS7 links and is set to 0. See the MSSLP command description for SNLINK measurements.

- RXMSU - Number of message signaling units octets received.
- RXOCT - Number of SIF and SIO octets received.
- TXMSU - Number of message signaling units octets transmitted.
- TXOCT - Number of SIF and SIO octets transmitted.
- RTXOCT - Octets retransmitted.

  Note: RTXOCT is not applicable for M2PA SS7 links and is set to 0. See the MSSLP command description for SNLINK measurements.

- NCONG - Congestion counter.
- PERIOD - Time since measurements on the route were last reset. Specified in hours, minutes and seconds.
- ALIGN - Number of failed signaling link alignment attempts
- SUERR - Number of signal units in error
- TBUSY - Duration of local busy condition
- TCONG - Duration of link congestion
- NDISCARD - Number of MSUs discarded due to congestion
- NEVENT - Number of congestion events leading to MSU discard

Syntax

```
MSC7P:[PAGE=,][C7LINK=,][RESET=,];
```

Prerequisites

- If specified, the SS7 signaling link must be initiated and unblocked.

Attributes

None

Examples

```
MSC7P:C7LINK=1;
MSC7P;
```

Output Format

```
SS7 Link Traffic Measurements (Page 1 of 2)
C7LINK OSSDUR RXNACK RXMSU  RXOCT  TXMSU    TXOCT  RTXOCT NCONG  PERIOD
1      0      0      188    4136   188      4136   0      0      00:46:39
2      0      0      188    4136   188      4136   0      0      00:46:39
3      0      0      0      0      0        0      0      0      00:46:39
EXECUTED

SS7 Link Traffic Measurements (Page 2 of 2)
C7LINK ALIGN  SUERR  TBUSY  TCONG  NDISCARD NEVENT PERIOD
1      0      0      0      0      0        0      00:46:39
2      0      0      0      0      0        0      00:46:39
3      92     0      0      0      0        0      00:46:39
EXECUTED
```

6.10.2 MSEPP – Measurement Ethernet Port Print

Synopsis

This command prints the traffic measurements for each Ethernet port on the system taken over a period of time. The meaning of each field in the output is as follows:

- ETH - Ethernet port number in the range 1 to 4, where:
  - ETH=1 corresponds to physical port ENET 1
  - ETH=2 corresponds to physical port ENET 2
  - ETH=3 corresponds to physical port ENET LNK A
  - ETH=4 corresponds to physical port ENET LNK B
- RXKBTYE - Number of kilobytes of data received (in kilobytes)
- RXPKT - Number of packets of data received
- RXERR - Number of receive errors detected
- RXDROP - Number of received packets dropped by the device driver during the measurement period
- TXKBTYE - Number of kilobytes of data transmitted (in kilobytes)
- TXPKT - Number of packets of data transmitted
- TXERR - Number of transmit errors detected
- TXDROP - Number of transmit packets
- PERIOD - The period over which the measurement was taken
- RXFIFO - The number of FIFO buffer errors received
- RXFRAME - The number of packet framing errors received
- RXCOMP - The number of compressed packets received
- RXMULT - The number of multicast frames received
- TXFIFO - The number of FIFO buffer error transmitted
- TXCOLLS - The number of collisions detected on the transmit side
- TXCARRIER - The number of carrier losses detected on the transmit side
- TXCOMP - The number of compressed packets transmitted

Note: Values are reset using the RESET parameter. MSEPP:RESET=Y; resets the measurement values to 0.

Syntax

```
MSEPP:[RESET=,][PAGE=,];
```

Prerequisites

None.

Attributes

None.

Examples

```
MSEPP:RESET=YES,PAGE=2;
MSEPP;
```

Output Format

```
Ethernet Port Measurements (Page 1 of 2)
ETH RXKBYTE RXPKT  RXERR  RXDROP TXKBYTE TXPKT  TXERR  TXDROP PERIOD
1   0       0      0      0      0       0      0      0      16:34:41
2   96324   135705 0      4204E5 28169   4444   0      0      16:34:41
3   0       0      0      0      0       0      0      0      16:34:41
4   3760    3273   0      33615  12503   3455   0      0      16:34:41
EXECUTED

Ethernet Port Measurements (Page 2 of 2)
ETH RXFIFO RXFRAME RXCOMP RXMULT TXFIFO TXCOLLS TXCARRIER TXCOMP PERIOD
1   0      0       0      0      0      0       0         0      16:34:41
2   0      0       0      0      0      0       0         0      16:34:41
3   0      0       0      0      0      0       0         0      16:34:41
4   0      0       0      0      0      0       0         0      16:34:41
EXECUTED
```

6.10.3 MSPCP – Measurements PCM Print

Synopsis

This command prints traffic measurements for PCMs. The measurements are cumulative between system startup and the next time the measurements are reset.

The fields have the following meanings:

- PCM - PCM on a board
- FMSLIP - Frame Slip count
- OUTSYN - Out-sync transitions
- ERRSEC - Errored Seconds count
- SEVSEC - Severely Errored seconds count
- PERIOD - Time since measurements on the route were last reset. Specified in hours, minutes and seconds

Syntax

```
MSC7P:[C7LINK=,][RESET=,];
```

Prerequisites

- If specified, the PCM must be initiated and on an unblocked board.

Attributes

None

Examples

```
MSPCP:PCM=5-1;
MSPCP;
```

Output Format

```
PCM Traffic Measurements
PCM     FMSLIP  OUTSYN  ERRSEC  SEVSEC  PERIOD
3-3     57      60      23      1       23:00:00
3-4     12      35      33      4       01:00:00
4-4     53      55      4       0       01:00:00
EXECUTED
```

6.10.4 MSSLP – Measurements SIGTRAN Link Print

Synopsis

This command prints traffic measurements for SIGTRAN signaling links. The measurements are cumulative between system startup and the next time the measurements are reset.

The fields have the following meanings:

- SNLINK - SIGTRAN signaling link
- RXCK - Number of data chunks received
- TXCK - Number of data chunks transmitted
- RTXCK - Number of data chunks re-transmitted
- NOOS - Number of times a SIGTRAN link has either been aborted or shutdown
- OSDUR - Duration that the link was not in service
- PERIOD - Time since measurements on the route were last reset. Specified in hours, minutes and seconds

Syntax

```
MSSLP:[SNLINK =,][RESET=,];
```

Prerequisites

- If specified, the SIGTRAN signaling link must be an initiated and unblocked.

Attributes

None

Examples

```
MSSLP:SNLINK=1;
MSSLP;
```

Output Format

```
SIGTRAN Link Traffic Measurements
SNLINK RXCK TXCK  RTXCK  OSDUR  NOOS PERIOD
1      54   6330  23     0      0    05:00:00
2      21   12    345    0      0    05:00:00
3      12   53    500    0      0    05:00:00
EXECUTED
```

6.10.5 MSSYP – Measurements System Print

Synopsis

This command prints out system related measurements for load and congestion taken over a period of time. The fields in the output have the following meanings:

- NOVLD - The number of periods of congestion (overload) during the measurement period.
- MAXLOAD - Maximum load average measurement taken over one minute (based on the UNIX load average).
- LOADAVG - The average load on the system (based on the UNIX load average) measurement taken over the measurement period.
- PERIOD - The period the measurement was taken over.

Note: Values are reset using the RESET parameter. MSSYP:RESET=Y; resets the measurement values to 0.

Syntax

```
MSSYP:[RESET=,];
```

Prerequisites

None

Attributes

None

Examples

```
MSSYP;
```

Output Format

```
System Measurements
NOVLD        0
MAXLOAD      28.81%
LOADAVG      2.28%
PERIOD       18:36:55
EXECUTED
```

6.11 Remote Data Centre Commands

The Remote Data Centre (RDC) commands include:

- RDCRI - Remote Data Centre Continuous Record Initiate
- RDCRC - Remote Data Centre Continuous Record Change
- RDCRE - Remote Data Centre Continuous Record End
- RDCRP - Remote Data Centre Continuous Record Print
- RDPDI - Remote Data Centre Periodic Data Initiate
- RDPDE - Remote Data Centre Periodic Data End
- RDPDP - Remote Data Centre Periodic Data Print
- RDPRI - Remote Data Centre Periodic Report Initiate
- RDPRC - Remote Data Centre Periodic Report Change
- RDPRE - Remote Data Centre Periodic Report End
- RDPRP - Remote Data Centre Periodic Report Print

6.11.1 RDCRI – Remote Data Centre Continuous Record Initiate

Synopsis

This command initiates a continuous record collection for which collected data is transferred via Ethernet to a Remote Data Centre (RDC).

The period is the maximum amount of time allowed before the transfer of a block of continuous records must be performed.

The minimum number of records that must be collected before the transfer of records can be performed should be specified.

The label is used as the directory name on the Remote Data Centre (RDC) that the files are written to.

Syntax

```
RDCRI:RECORD=,CRTYPE=,PERIOD=,MINREC=,RDC1=,LABEL=,[RDC2=,];
```

Prerequisites

- The record has not already been initiated.
- The Signaling Gateway must have an IPADDR.
- If the record is an alarm record, an alarm record must not already exist.
- RDC1 must already be initiated.
- If specified, RDC2 must already be initiated.
- If specified, RDC2 must not equal RDC1.

Limitations

- Before transfer to a RDC can take place, the directory (represented by the label) must exist on the remote site.
- PERIOD must be in the range 30 seconds to 30 minutes.

Attributes

CONFIG

Examples

```
RDCRI:RECORD=1,CRTYPE=ALARM,PERIOD=00:05:00,MINREC=100,
RDC1=1,LABEL=ALARM;
```

6.11.2 RDCRC – Remote Data Centre Continuous Record Change

Synopsis

This command changes the parameters for a continuous record collection for which collected data is transferred via Ethernet to a Remote Data Centre (RDC).

The period is the maximum amount of time allowed before the transfer of a block of continuous records must be performed.

The label is used as the directory name on the RDC that the files are written to.

Syntax

```
RDCRC:RECORD=,[PERIOD=,][MINREC=,][RDC1=,][RDC2=,][LABEL=];
```

Prerequisites

- The record must already be initiated.
- If specified, RDC1 must already be initiated.
- If specified, RDC2 must already be initiated
- If specified, RDC2 must not equal RDC1.

Limitations

- Before transfer to a RDC can take place, the directory (represented by the label) must exist on the remote site.
- PERIOD must be in the range 30 seconds to 30 minutes.

Attributes

CONFIG

Examples

```
RDCRC:RECORD=1,PERIOD=00:05:00,MINREC=100,
RDC1=1,LABEL=ALARM;
```

6.11.3 RDCRE – Remote Data Centre Continuous Record End

Synopsis

This command ends a continuous record.

If DISCARD is set to Y, any data associated with the continuous record is discarded. If DISCARD is not set to Y, and if there is data awaiting transfer, the end continuous record is rejected.

Syntax

```
RDCRE:RECORD=,[DISCARD=Y];
```

Prerequisites

- The report has already been initiated.
- There is no continuous data associated with the continuous record.

Attributes

CONFIG

Examples

```
RDCRE:RECORD=1;
```

6.11.4 RDCRP – Remote Data Centre Continuous Record Print

Synopsis

This command prints data relating to a continuous record for which collected data is transferred to a Remote Data Centre (RDC).

Syntax

```
RDCRP;
```

Prerequisites

None

Attributes

CONFIG

Examples

```
RDCRP;
```

Output Format

```
Remote Data Centre Continuous Record
RECORD CRTYPE     PERIOD     MINREC   RDC1 RDC2 LABEL
1      ALARM      00:05:00   100      2    1    ALARM
EXECUTED
```

6.11.5 RDPDI – Remote Data Centre Periodic Data Initiate

Synopsis

This command attaches an SS7 link (C7LINK), SIGTRAN link (SNLINK) or PCM (PCM) to a periodic report.

Syntax

```
RDPDI:REPORT=,[C7LINK=|SNLINK=|PCM=];
```

Prerequisites

- The report has already been initiated.
- The specified SS7 link has already been initiated.
- SS7 links can only be specified for MSC7 reports.
- An association between the report and the SS7 link has not already been initiated.

Attributes

CONFIG

Examples

```
RDPDI:REPORT=1,C7LINK=1&&8;
```

6.11.6 RDPDE – Remote Data Centre Periodic Data End

Synopsis

This command ends the attachment between an outgoing route and a report.

Syntax

```
RDPDE:REPORT=,[C7LINK= | SNLINK=| PCM=];
```

Prerequisites

- The report has already been initiated.
- An association between the report and the SS7 link has already been initiated.

Attributes

CONFIG

Examples

```
RDPDE:REPORT=1,C7LINK=1;
```

6.11.7 RDPDP – Remote Data Centre Periodic Data Print

Synopsis

This command prints the outgoing routes associated with a periodic data collection report.

The command prints a list of report elements depending on the type of the report.

Syntax

```
RDPDP:REPORT=;
```

Prerequisites

- The periodic report has been initiated.

Attributes

CONFIG

Examples

```
RDPDP:REPORT=1;
```

Output Format

```
Remote Data Centre Periodic Data
REPORT C7LINK
1      1
1      2
1      3
1      5
1      8
EXECUTED
```

6.11.8 RDPRI – Remote Data Centre Periodic Report Initiate

Synopsis

This command initiates a report collection period for which data is collected and transferred over Ethernet to a Remote Data Centre (RDC).

Reports for outgoing route traffic measurements can be specified.

The label is used as the directory name on the RDC that the files are written to.

The period is the interval between which data is collected. It is rounded to the nearest 5-minute interval.

Data can be added or deleted from the periodic report using the RDPDI or RDPDE commands.

Syntax

```
RDPRI:REPORT=,PRTYPE=,PERIOD=,LABEL=,RDC1=,[RESET=,][RDC2=,];
```

Prerequisites

- The report has not already been initiated.
- If specified, RDC2 cannot have the same value as RDC1.
- RDC1 must already have been initiated.
- If specified, RDC2 must already be initiated.

Limitations

Before transfer to an RDC can take place, the directory (represented by the label) must exist on the remote site.

Attributes

CONFIG

Examples

```
RDPRI:REPORT=1,PRTYPE=MSC7,PERIOD=01:00:00,RDC1=1,LABEL=SS7;
```

6.11.9 RDPRC – Remote Data Centre Periodic Report Change

Synopsis

This command changes parameters relating to a report collection period for which data is collected and transferred over Ethernet to a Remote Data Centre (RDC).

Reports for outgoing route traffic measurements can be specified.

The label is used as the directory name on the RDC that the files are written to.

The period is the interval between which data is collected. It is rounded to the nearest 5 minute interval.

Data can be added or deleted from the periodic report using the RDPDI or RDPDE commands.

Syntax

```
RDPRC:REPORT=,[PERIOD=,][LABEL=,][RDC1=,][RDC2=,][RESET=,];
```

Prerequisites

- The report must already be initiated.
- If specified, RDC2 cannot have the same value as RDC1.
- If specified, RDC1 must already be initiated.
- If specified, RDC2 must already be initiated.

Limitations

Before transfer to an RDC can take place, the directory (represented by the label) must exist on the remote site.

Attributes

CONFIG

Examples

```
RDPRC:REPORT=1,PERIOD=01:00:00,RDC1=1,LABEL=SS7;
```

6.11.10 RDPRE – Remote Data Centre Periodic Report End

Synopsis

This command ends a periodic report.

Syntax

```
RDPRE:REPORT=;
```

Prerequisites

- The report has already been initiated.
- There is no periodic data associated with the periodic report.

Attributes

CONFIG

Examples

```
RDPRE:REPORT=1;
```

6.11.11 RDPRP – Remote Data Centre Periodic Report Print

Synopsis

This command prints data relating to a periodic report collection period for which collected data is transferred to a Remote Data Centre (RDC).

Syntax

```
RDPRP;
```

Prerequisites

None

Attributes

CONFIG

Examples

```
RDPRP;
```

Output Format

```
Remote Data Centre Periodic Report Configuration
REPORT PRTYPE PERIOD   RESET RDC1 RDC2 LABEL
1      MSC7   01:00:00 Y     1    2    SS7
EXECUTED
```

6.12 Signaling Gateway Commands

The Signaling Gateway commands include:

- SGDPI - Signaling Gateway Destination Point Initiate
- SGDPC - Signaling Gateway Destination Point Change
- SGDPE - Signaling Gateway Destination Point End
- SGDPP - Signaling Gateway Destination Point Print
- SGIRI - Signaling Gateway Incoming Route Initiate
- SGIRC - Signaling Gateway Incoming Route Change
- SGIRE - Signaling Gateway Incoming Route End
- SGIRP - Signaling Gateway Incoming Route Print
- SGRKI - Signaling Gateway Routing Key Initiate
- SGRKE - Signaling Gateway Routing Key End
- SGRKP - Signaling Gateway Routing Key Print

6.12.1 SGDPI – Signaling Gateway Destination Point Initiate

Synopsis

This command initiates routing to a destination point identified by a routing key or incoming route. Destination selection either selects an Application Server (AS) or attempts to route to the MTP or IP side on a priority basis. If an Application Server is not configured, the Signaling Gateway attempts to find a route to the Destination Point Code (DPC) of the received message over MTP or IP. The user can configure whether to route the message via MTP or IP if the Point Code is available over both by setting the RTPRI parameter.

A destination can either be a route (MTP or IP or a combination of both) or a Application Server. If both MTP and IP routes are specified, the default priority indicates which route to the Point Code should be selected first if available. MTPONLY and IPONLY state that no attempt to other domain should be made if the routes through these domains are unavailable.

Syntax

```
SGDPI:DEST=,RTPRI=,[LABEL=,];
SGDPI:DEST=,AS=,[LABEL=,];
```

Prerequisites

- The destination point has not already been initiated.
- An AS, if specified, must serve only 1 destination.
- If an AS is specified, it must be initialized.
- RTPRI cannot be set to NONE if an AS is not present.
- NONE is the only value allowed for RTPRI if an AS is present.

Attributes

CONFIG

Examples

```
SGDPI:DEST=1, AS=1;
```

6.12.2 SGDPC – Signaling Gateway Destination Point Change

Synopsis

This command changes parameters on the Signaling Gateway destination point.

Syntax

```
SGDPC:DEST=,[RTPRI=,][AS=,][LABEL=,];
```

Prerequisites

- The destination point has already been initiated.
- If an AS is specified, it must serve only one destination.
- If an AS is specified, it must be initialized.
- RTPRI cannot be set to NONE if an AS is not present.
- NONE is the only value allowed for RTPRI if AS is present.
- If an AS is specified, there cannot be any routing key in the system with a destination to this AS, not having or not matching the NC/DPC parameters with the AS NC/DPC.

Attributes

CONFIG

Examples

```
SGDPC:DEST=1, AS=1;
```

6.12.3 SGDPE – Signaling Gateway Destination Point End

Synopsis

This command ends a Signaling Gateway destination point.

Syntax

```
SGDPE:DEST=;
```

Prerequisites

- The destination ID has already been initiated.
- The destination ID is not used elsewhere in the system.

Attributes

CONFIG

Examples

```
SGDPE:DEST=1;
```

6.12.4 SGDPP – Signaling Gateway Destination Point Print

Synopsis

This command prints the configuration of routing parameters on a SS7 Signaling Gateway.

Syntax

```
SGDPP:[DEST=];
```

Prerequisites

- The destination ID has already been initiated.

Attributes

None

Examples

```
SGDPP;
```

Output Format

```
SS7 Routing Key Configuration
DEST RTPRI    AS LABEL
1    NONE     1  AS1
2    IP          SGW2
3    MTP         DEST3
EXECUTED
```

6.12.5 SGIRI – Signaling Gateway Incoming Route Initiate

Synopsis

This command initiates an incoming route on a Signaling Gateway. The incoming route is selected by the network and domain (TDM or SIGTRAN) that a data message came from. The network is specified on an SS7 link set on the TDM side and a SIGTRAN link on the SIGTRAN side.

An incoming route can either go directly to a destination or perform analysis of the received message to determine a destination. If analysis fails, or the destination determined by analysis is not available, the incoming route can use the destination associated with it as a default destination.

For RKTAB, DEST, NC, and DOMAIN, a value of “null” is supported. “null” indicates a wildcard value and means any value. “null” is the default value for an RKTAB/DEST entry.

Note: The value “null” cannot be used for these parameters elsewhere in the system unless explicitly specified in the command.

Syntax

```
SGIRI:IR=,[NC=,][DOMAIN=,]{[RKTAB=,][DEST=,]}[LABEL=,];
```

Prerequisites

- If specified, the destination index exists.
- Either an RKTAB or DEST must exist.
- The incoming route does not already exist.
- The NC/DOMAIN combination has not already been specified nor does it form a superset or subset of an existing NC/DOMAIN combination

Note: This check takes into account one or more routing elements marked as a wild card.

Attributes

CONFIG

Examples

```
SGIRI:IR=1, DOMAIN=IP,RKI=1;
```

6.12.6 SGIRC – Signaling Gateway Incoming Route Change

Synopsis

This command changes the configuration of a Signaling Gateway incoming route.

For RKTAB/DEST, a value of “null” is supported. “null” indicates a wildcard value and means any value. “null” is the default value for an RKTAB/DEST entry.

> ***Note:*** The value “null” cannot be used for these parameters elsewhere in the system unless explicitly specified in the command.

Syntax

```
SGOPC:IR=,[RKTAB=,][DEST=,][LABEL=];
```

Prerequisites

- The incoming route already exists.
- If specified, the destination index exists.
- The NC/DOMAIN combination has already been initiated.
- Either an RKTAB or DEST must exist.

Attributes

CONFIG

Examples

```
SGIRC:IR=1,DEST=5;
```

6.12.7 SGIRE – Signaling Gateway Incoming Route End

Synopsis

This command ends the configuration of a Signaling Gateway incoming route.

Syntax

```
SGIRE:IR=;
```

Prerequisites

- The incoming route already exists.

Attributes

CONFIG

Examples

```
SGIRE:IR=1;
```

6.12.8 SGIRP – Signaling Gateway Incoming Route Print

Synopsis

This command prints the configuration of a Signaling Gateway incoming route.

Syntax

```
SGIRP:[IR=];
```

Prerequisites

- If specified, the IR has already been initiated.

Attributes

None

Examples

```
SGIRP;
```

Output Format

```
Signaling Gateway Incoming Route Configuration
IR NC DOMAIN   RKTAB DEST LABEL
1  1  TDM      1          ORIG1
2  1  SIGTRAN  1          ORIG1
3  2           2          ORIG2
4  3  TDM      3          ORIG3
EXECUTED
```

6.12.9 SGRKI – Signaling Gateway Routing Key Initiate

Synopsis

This command initiates a routing key or partial routing key to determine a destination identifier. The destination identifier is then used to select the outgoing destination. The Signaling Gateway compares the routing keys with a data message in an attempt to find a data match. If a match is found, the destination identifier is then used to select a route to an eventual destination.

The user can define a number of different tables of routing keys. In the routing model, the incoming route identifies which routing table to use.

Apart from the routing key index and routing key table, the routing key elements are optional and can be wildcarded with a null string.

A routing key is defined as a combination of NC//NI/SI/OPC/DPC/BCIC/RANGE.

For DPC, OPC, NI, SI, NC, BCIC and RANGE, a value of “null” is supported. “null” indicates a wildcard value and means any value. “null” is the default value for a routing key entry.

> ***Note:*** The value “null” cannot be used for these parameters elsewhere in the system unless explicitly specified in the command.

Syntax

```
SGRKI:RKI=,RKTAB=,[NC=,][OPC=,][NI=,][SI=,][DPC=,][RANGE=,BCIC=,]DEST=;
```

Prerequisites

- The routing key ID has not already been specified.
- The routing key combination has not already been specified nor does it form a superset or subset of an existing routing key.

> ***Note:*** This check takes into account one or more routing elements marked as a wild card.

- The destination ID has already been initiated.
- If SI is set to SCCP, the BCIC/RANGE parameters cannot be specified.
- If one of BCIC/RANGE are specified, the other must be specified.
- For circuit related keys, the CIC ranges specified for an NC/OPC/NI/DPC combination must not overlap existing ranges for that combination.
- If an OPC or DPC are specified, the NC cannot be wildcarded.
- BCIC cannot be negative.
- If the routing key has a destination to an AS, the NC/DPC parameters are required and must match with the AS NC/DPC.

Attributes

CONFIG

Examples

```
SGRKI:RKI=1,RKTAB=,NC=1,OPC=55,DPC=33,DEST=1;
```

6.12.10 SGRKE – Signaling Gateway Routing Key End

Synopsis

This end configuration of a routing key or a particular subset of routing keys.

Syntax

```
SGRK:RKI=;
```

Prerequisites

- The routing key combination has already been specified.

Attributes

CONFIG

Examples

```
SGRKE:RKI=1,NC=1,OPC=55,DPC=33;
```

6.12.11 SGRKP – Signaling Gateway Routing Key Print

Synopsis

This command prints the configuration of Routing Keys.

Syntax

```
SGRKP:[RKI=,][RKTAB=,][DEST=,];
```

Prerequisites

None

Attributes

CONFIG

Examples

```
SGRKP;
```

Output Format

```
Routing Key Analysis configuration
RKI RKTAB NC NI SI OPC      DPC      BCIC RANGE DEST
1   1     1  2     2        194      0    32    2
2   1     2  2     2        133                 3
3   1     3  2              1332                43

EXECUTED
```

6.13 SIGTRAN Commands

The SIGTRAN commands include:

- SNALI - SIGTRAN Application Server List Initiate
- SNALE - SIGTRAN Application Server List End
- SNALP - SIGTRAN Application Server List Print
- SNAPI - SIGTRAN Application Server Initiate
- SNAPE - SIGTRAN Application Server End
- SNAPP - SIGTRAN Application Server Print
- SNNAI - SIGTRAN Network Appearance Initiate
- SNNAE - SIGTRAN Network Appearance End
- SNNAP - SIGTRAN Network Appearance Print
- SNSLI - SIGTRAN Signaling Link Initiate
- SNSLC - SIGTRAN Signaling Link Change
- SNSLE - SIGTRAN Signaling Link End
- SNSLP - SIGTRAN Signaling Link Print

6.13.1 SNALI – SIGTRAN Application Server List Initiate

Synopsis

This command attaches a list of SIGTRAN links to an Application Server (AS). The SIGTRAN links provide the SCTP associations to reach the AS.

See Section 7.2, “Signaling Configuration” on page 136 for a more detailed description of SIGTRAN signaling configuration.

Syntax

```
SNALI:AS=,SEQ=,SNLINK=;
```

Prerequisites

- The AS has already been initiated.
- The specified SIGTRAN link has already been initiated.
- A SIGTRAN link cannot be specified in more than one hunt sequence position for this server.
- The server/hunt sequence combination must not already be initiated.
- The SIGTRAN links attached to the server must be M3UA and their peers be able to process ASs (that is, not act as Signaling Gateways).
- A SNLINK cannot be attached to more than 32 ASs.
- The SNTYPE of the SNLINK cannot be M2PA.

Attributes

CONFIG

Examples

```
SNALI:AS=1,SEQ=1,SNLINK=1;
```

6.13.2 SNALE – SIGTRAN Application Server List End

Synopsis

This command ends a relationship between an Application Server (AS) and a SIGTRAN link.

Syntax

```
SNALE:AS=,SEQ=;
```

Prerequisites

- The AS sequence combination has already be initiated.
- The last entry in a list of SIGTRAN links attached to an AS cannot be removed unless the AS is blocked.

Attributes

CONFIG

Examples

```
SNALE:AS=,SEQ=;
```

6.13.3 SNALP – SIGTRAN Application Server List Print

Synopsis

This command reports the relationship between a SIGTRAN Application Server (AS) and SIGTRAN links.

Syntax

```
SNALP;
SNALP:AS=;
SNALP:SNLINK=;
```

Prerequisites

- The server/hunt sequence combination has already be initiated.

Attributes

None

Examples

```
SNALP;
```

Output Format

```
Application Server List Configuration
AS      AS LABEL SEQ  SNLINK SNLINK LABEL
1         AS1      1     1      ASP1
1         AS1      2     2      ASP2
2         AS2      1     3      ASP3
EXECUTED
```

6.13.4 SNAPI – SIGTRAN Application Server Initiate

Synopsis

This command initiates an adjacent Application Server (AS). An AS is a logical entity representing an SS7 end point that can process either circuit-related or non circuit-related signaling. The end point is represented by a routing context which uniquely identifies a routing key combination of SIO/DPC/OPC and CIC range.

See Section 7.2, “Signaling Configuration” on page 136 for a more detailed description of SIGTRAN signaling configuration.

Syntax

```
SNAPI:AS=,DPC=,RC=,NC=,[PCMD=,][NASP=,][LABEL=,];
```

Prerequisites

- The AS has not already been initiated.
- No other AS can use the routing context.
- No more than 32 ASs can be configured with the same DPC/NC combination.
- All ASs within the same DPC/NC combination must have the same PCMD value.

Attributes

CONFIG

Examples

```
SNAPI:AS=1,DPC=555,RC=1,NC=1;
```

6.13.5 SNAPE – SIGTRAN Application Server End

Synopsis

This command ends an Application Server (AS).

Syntax

```
SNAPE:AS=;
```

Prerequisites

- The server has already be initiated.
- There are no SIGTRAN links attached to the server.
- The server is not part of a destination.
- The server must be blocked.

Attributes

CONFIG

Examples

```
SNAPE:AS=1;
```

6.13.6 SNAPP – SIGTRAN Application Server Print

Synopsis

This command prints information relating to a SIGTRAN Application Server (AS).

Syntax

```
SNAPP:[AS=];
```

Prerequisites

- If specified, the AS has already be initiated.

Attributes

None

Examples

```
SNAPP;
```

Output Format

```
SIGTRAN Application Server Configuration
AS  DPC       NC  RC          PCMD NASP  LABEL
1   55        1   5           ANY  0     AS1
2   44        2   44          ANY  2     AS2
EXECUTED
```

6.13.7 SNNAI – SIGTRAN Network Appearance Initiate

Synopsis

This command initiates a relationship between a Network Context and a Network Appearance on a per SIGTRAN link basis.

See Section 7.2, “Signaling Configuration” on page 136 for a more detailed description of SIGTRAN signaling configuration.

Syntax

```
SNNAI:NC=,SNLINK=,SS7MD=,NA=;
```

Prerequisites

- The SNLINK has been already initiated.
- The SS7MD associated with the NC cannot be different to a SS7MD associated with a NC anywhere else in the system.
- There is a one-to-one relation between NC and NA on a SNLINK.
- The NC cannot be the default value for this SNLINK.
- The SNTYPE of the SNLINK cannot be M2PA.

Attributes

CONFIG

Examples

```
SNNAI:NC=1,SNLINK=1,SS7MD=ITU14,NA=63;
```

6.13.8 SNNAE – SIGTRAN Network Appearance End

Synopsis

This command ends a relationship between an NC and NA on a per SNLINK basis.

Syntax

```
SNNAE:SNLINK=,NC=;
```

Prerequisites

- The NC has already been initiated.
- The SNLINK has already been initiated.
- There is a configured relationship between NC and NA in this SNLINK.
- There are no unblocked ASs using this SNLINK and NC combination.
- If the SNLINK is unblocked, there are NA mapping in other Network Contexts for the SNLINK.

Attributes

CONFIG

Examples

```
SNNAE:SNLINK=1,NC=1;
```

6.13.9 SNNAP – SIGTRAN Network Appearance Print

Synopsis

This command gives a printout of the relationship between Network Contexts (NCs) and Network Appearances (NAs) on a per SNLINK basis.

Syntax

```
SNNAP:[NC=,][SNLINK=,];
```

Prerequisites

- If specified, the NC or SNLINK has already be initiated.

Attributes

None

Examples

```
SNNAP;
```

Output Format

```
SIGTRAN Network Appearances
NC   SNLINK   SS7MD NA
1    1        ITU14 63
2    2        ITU14 64
EXECUTED
```

6.13.10 SNSLI – SIGTRAN Signaling Link Initiate

Synopsis

This command initiates a SIGTRAN link. A SIGTRAN link (SNLINK) provides an SCTP association to an adjacent Application Server Process or Signaling Gateway specified by one (IPADDR) or two (IPADDR2) IP addresses as well as the host (HPORT) and peer (PPORT) SCTP port. The user should specify the type of SIGTYPE link (SNTYPE) and which IP end (END) the Signaling Gateway is acting as.

For M2PA, the SIGTRAN link is associated with a SS7 link by the C7SLI command.

For M3UA, a default SS7 mode (SS7MD) and network context (NC) can be specified. This allows the user to designate an SS7 format and mode of operation to a link. If the user requires the SNLINK to exist in multiple networks, the user should not specify a default network context nor an SS7 mode, instead they should associate it with a Network Appearance using the SNNAI command prior to unblocking.

If two IP addresses are specified, the first IP address is used until it proves unreliable, in which case the second IP address is used.

When SECURE is set to Y, the SIGTRAN link does not come into service on unblocking if it receives messaging from a peer that has an IP address not associated with the SIGTRAN link.

> ***Note:*** Normal operation for M2PA would be to set one end to client and the other end to server. The signaling gateway provides the ability for both ends to operate as client; however in this case, the SECURE parameter must be set to Y.

See Section 7.2, “Signaling Configuration” on page 136 for a more detailed description of SIGTRAN signaling configuration.

Syntax

```
SNSLI:SNLINK=,SNTYPE=,IPADDR=,END=,[SS7MD=,NC=,]
      [IPADDR2=,][HPORT=,][PPORT=,][SRTX=,][LABEL=,][SECURE=,];
```

Prerequisites

- The SIGTRAN link has not already been initiated.
- An IP address of 0.0.0.0 cannot be specified.
- The IPADDR, HPORT, and PPORT combination must not be the same as that of a previously configured SNLINK.
- The END can only be Client (C) or Server (S).
- Both NC and SS7MD parameters must either be present or both parameters must not be present.
- The SS7MD associated with an NC cannot be different to a SS7MD associated with the same NC anywhere else in the system.
- If the SNTYPE is M2PA, SS7MD, and NC cannot be specified.

Limitations

None

Attributes

CONFIG

Examples

```
SNSLI:SNLINK=1,SNTYPE=SGM3UA,END=S, IPADDR=193.112.111.123;
SNSLI:SNLINK=2,SNTYPE=M2PA,END=C,IPADDR=193.112.111.123,
       IPADDR2=192.112.111.123;;
```

6.13.11 SNSLC – SIGTRAN Signaling Link Change

Synopsis

This command changes parameters on a SIGTRAN link. A SIGTRAN link provides an SCTP association to an adjacent SIGTRAN server.

If two IP addresses are specified, the first IP address is used until it proves unreliable in which case the second is used.

An IP address of 0.0.0.0 indicates that the parameter is not configured.

When SECURE is set to Y, the SIGTRAN link does not come into service on unblocking if it receives messaging from a peer that has an IP address not associated with the SIGTRAN link.

> ***Note:*** Normal operation for M2PA would be to set both ends to client.

Syntax

```
SNSLC:SNLINK=,END=,[IPADDR=,][IPADDR2=,][HPORT=]
       [PPORT=,][SRTX=,][LABEL=,][SECURE=,];
```

Prerequisites

- The SIGTRAN link has already been initiated and is blocked.
- The END can only be Client (C) or Server (S).

Attributes

CONFIG

Examples

```
SNSLC:SNLINK=1, PPORT=2905;
```

6.13.12 SNSLE – SIGTRAN Signaling Link End

Synopsis

This command ends the configuration of parameters on a SIGTRAN signaling link.

Syntax

```
SNSLE:SNLINK=;
```

Prerequisites

- The SIGTRAN link has already been initiated and is blocked.
- The SIGTRAN link cannot be ended if it is attached to an Application Server (AS).
- There cannot be any NC/NA mapping configured on the SNLINK.
- The SNLINK cannot be ended if it is associated with a C7LINK.

Attributes

CONFIG

Examples

```
SNSLE:SNLINK=1;
```

6.13.13 SNSLP – SIGTRAN Signaling Link Print

Synopsis

This command prints the configuration of SIGTRAN signaling links.

Syntax

```
SNSLP:[SNLINK=][PAGE=,];
```

Prerequisites

- If specified, the SNLINK link has already been initiated.

Attributes

None

Examples

```
SNSLP:SNLINK=1;
```

Output Format

```
Page 1 of 2 SIGTRAN Signaling Link Configuration
SNLINK SNTYPE SG   END NC    SS7MD IPADDR          IPADDR2         LABEL
1      SGM3UA      S   1     ITU14 194.192.184.111 194.192.198.120 ASP1
2      SGM3UA      S   2     ANSI  111.143.134.122 111.111.123.100 ASP2
EXECUTED

Page 2 of 2 SIGTRAN Signaling Link Configuration
SNLINK HPORT PPORT SRTX SECURE LABEL
1      2905  2905  2    N      Dual
EXECUTED
```

6.14 Status Commands

The status commands include:

- STALP - Status Alarm Print
- STAPP - Status Application Server Print
- STBOP - Status Board Print
- STCRP - Status C7 Route Print
- STC7P - Status C7 Link Print
- STEPP - Status Ethernet Port Print
- STIPP - Status IP Print
- STPCP - Status PCM Print
- STRDP - Status Remote Data Centre Print
- STSLP - Status SIGTRAN Link Print

6.14.1 STALP – Status Alarm Print

Synopsis

This command requests an alarm status report summary. The interpretation of the ID field in the listing is dependent on the alarm type (see Chapter 8, “Alarm Fault Code Listing”).

The fields have the following meanings:

- SYS - The number of system alarms
- PCM - The number of PCM alarms
- SIG - The number of signaling alarms
- CLA1 - The number of minor alarms
- CLA2 - The number of major alarms
- CLA3 - The number of critical alarms

Syntax

```
STALP;
```

Prerequisites

None

Attributes

None

Examples

```
STALP;
```

Output Format

```
Alarm Status

SYS  PCM  SIG  CLA1  CLA2  CLA3
  1    0    1     2     0     0
EXECUTED
```

6.14.2 STAPP – Status Application Server Print

Synopsis

This command provides the status of SIGTRAN servers. It also provides the status of a link when it is serving the Application Server (AS).

Definitions of the AS status:

- BLOCKED - The AS is blocked.
- AVAILABLE - The AS is available.
- UNAVAILABLE - The AS is unavailable.
- INSUFF_ASP - The AS is available but it has insufficient ASPs active as configured in SNAPP (only valid for load sharing).

Definitions of the ASP within the server:

- DOWN - The link attached to the server is down.
- ACTIVE - The link attached to the server is active.
- INACTIVE - The link attached to the server is inactive.

Definitions of TRMD (Traffic Mode):

- LS - Load sharing mode
- OR - Override mode
- BC - Broadcast mode

Syntax

```
STAPP:[AS =…];
```

Prerequisites

None

Attributes

None

Examples

```
STAPP:AS=1;
```

Output Format

```
Application Server Status
AS  AS STATUS   SNLINK  ASP STATUS   TRMD ASP ID     AS LABEL
1   AVAIlABLE   1       ACTIVE       LS              AS1
2   AVAILABLE   2       DOWN         LS              AS2
2   AVAILABLE   3       INACTIVE     LS              AS2
3   BLOCKED
EXECUTED
```

6.14.3 STBOP – Status Board Print

Synopsis

This command requests a status report of boards on the system. Possible status values are:

- INACTIVE - The board is not in operation.
- RESETTING - The board is undergoing a reset.
- ACTIVE - The board is operational.
- FAILED - The board has failed and is out of service.

Syntax

```
STBOP:[BPOS=…];
```

Prerequisites

- If specified, the board should have already been initiated.

Attributes

None

Examples

```
STBOP:BPOS=1;
```

Output Format

```
Board Status
BPOS STATUS
Active
Failed
Blocked
EXECUTED
```

6.14.4 STCRP – Status C7 Route Print

Synopsis

This command shows the status of the specified SS7 route or range of routes within a network context. If no route or network context is specified, then the values for all routes are shown.

The command indicates whether a route is available or unavailable as well as indicating which routsets within the route are available or unavailable. The command also provides the congestion state of the route.

Possible ROUTE STATUS values are:

- Available
- Unavailable
- Available - The route is available for traffic to the remote point code of the route.
- Unavailable - The route is unavailable for traffic to the remote point code of the route.

Possible CONG LEVEL values are:

- 0 no congestion
- 1, 2 or 3 indicating the level of congestion

Possible LS1 STATUS and LS2 STATUS values are:

- Available - The linkset on the route is available for traffic to the adjacent point code.
- Unavailable - The linkset on the route is unavailable for traffic to the adjacent point code.

Syntax

```
STCRP;
STCRP:NC=;
STCRP:C7RT=,NC=;
```

Prerequisites

None

Attributes

None

Examples

```
STCRP;
```

Output Format

```
CCITT SS7 Route Status
C7RT NC DPC      ROUTE STATUS CONG LEVEL LS1 STATUS   LS2 STATUS   LABEL
1    1  1        Available    0          Available
2    1  2        Available    0          Unavailable  Available
64   4  99       Unavailable  0          Unavailable
EXECUTED
```

6.14.5 STC7P – Status C7 Link Print

Synopsis

This command requests a status report of the SS7 signaling links or SS7 link sets.

L2 STATUS - Possible values are:

- In service
- Out of service
- Proc outage
- Aligned rdy
- Init align
- Align not rdy

L3 STATUS - Possible values are:

- Available
- Unavailable
- Congested
- Deactivated (the link has been deactivated)
- Blocked (the link is blocked)

L3 BLOCKING STATUS - Possible values are:

- INHR - The link is remotely inhibited
- INHL - The link is locally inhibited
- BLKR - The link is remotely blocked
- COIP - Changeover is in progress
- CBIP - Changeback is in progress
- LIIP - Local link inhibiting is in progress
- LUIP- Local link uninhibiting is in progress

Syntax

```
STC7P:[PAGE=…][C7LINK=…];
STC7P:[PAGE=…][LS=…];
```

Prerequisites

None

Attributes

None

Examples

```
STC7P;
```

Output Format

```
CCS SS7 Signalling Link Status (Page 1 of 2)
C7LINK  LS      EQU     TS      SNLINK  L2 STATUS       L3 STATUS
1       1       1-3     1-3-16                          BLOCKED
2       1       1-4     1-4-16          IN SERVICE      AVAILABLE
3       2       3-3     3-3-16          INITIAL ALIGN   UNAVAILABLE
4       2       3-4     3-4-16          OUT OF SERVICE  DEACTIVATED
EXECUTED
```

```
CCS SS7 Signalling Link Status (Page 2 of 2)
C7LINK  L2 STATE        L3 STATE     L3 BLOCKING STATUS
1                       BLOCKED      ---- ---- ---- ---- ---- ---- ----
2       IN SERVICE      AVAILABLE    ---- ---- ---- ---- ---- LIIP ----
3       INITIAL ALIGN   UNAVAILABLE  ---- ---- ---- ---- ---- ---- ----
4       OUT OF SERVICE  DEACTIVATED  ---- ---- ---- ---- ---- ---- ----
EXECUTED
```

6.14.6 STEPP – Status Ethernet Port Print

Synopsis

This command provides the status of Ethernet ports on the system. The parameters output are:

- ETH - The Ethernet port identity.
- PARTNER - Identifies the other port member of a port bonding team.
- SPEED - The speed of the Ethernet port (10 / 100 / 1000).
- DUPLEX - Whether the port is FULL or HALF Duplex.
- STATUS - Whether the port is UP or DOWN. If the port is in a team, and it is “up”, the status indicates instead whether the port is ACTIVE or in STANDBY.

Syntax

```
STEPP;
```

Prerequisites

None

Attributes

None

Examples

```
STEPP;
```

Output Format

```
ETH PARTNER SPEED DUPLEX STATUS
1                        DOWN
2           100   FULL   UP
3   4       1000  FULL   ACTIVE
4   3       1000  FULL   STANDBY
EXECUTED
```

6.14.7 STIPP – Status IP Print

Synopsis

This command sends four ICPM (Internet Control and Management Protocol) Echo Request frames to the specified remote IP address and measures the maximum round trip time, similar to the standard Unix ping command. SEND shows the number of frames transmitted. RECV shows the number of replies received and MAXRTD shows the maximum delay between sending a frame and receiving a reply, in milliseconds. The measurement is accurate to 10ms, hence any value less than 10ms is displayed as ‘<10’. If the destination IP address is not reachable, RECV is shown as 0 and MAXTP as ‘-‘.

Syntax

```
STIPP:IPADDR=;
```

Prerequisites

None

Attributes

None

Examples

```
STIPP:IPADDR=173.132.23.3;
```

Output Format

```
IP Status
IPADDR                  SEND      RECV      MAXRTD
193.195.185.16          4         4         20
EXECUTED
```

6.14.8 STPCP – Status PCM Print

Synopsis

This command requests a status report of the PCMs. The PCM status is one of the following:

- OK - Normal operational state
- PCM Loss - No signal sensed on the PCM input
- Sync Loss - Loss of frame alignment since no frame synchronization has been received
- RAI - Remote alarm indication. The remote end indicates that is it is OK, but also indicates that it is detecting an error condition.
- AIS - Alarm indication signal. The remote side sends all ones indicating that there is an error condition, or it is not initialized.
- BER > 1:10^3 - The PCM is encountering a Bit Error Rate (BER) of 10^3.
- BER > 1:10^5 - The PCM is encountering a BER of 10^5.

The Clock Status field is one of the following:

- OK - The board is detecting a valid PCM signal which could potentially be used for synchronization.
- Standby - The board is detecting a valid PCM signal which will be used for synchronization in the event of failure of the active clock source.
- Active - The board is detecting a valid PCM signal which is currently providing synchronization for the Signaling Gateway.
- Not OK – The input to the board is not currently suitable for use as a synchronization source.
- Fault - A fault has been detected on the board which prevents it being used as a synchronization source.

Syntax

```
STPCP;
```

Prerequisites

None

Attributes

CONFIG

Examples

```
STPCP;
```

Output Format

```
PCM Status
PCM SYNCPRI PCM Status  Clock
1-3 1       PCM Loss    Fault
1-4 2       SYNC Loss   Not OK
2-3 3       AIS         Not OK
2-4 4       RAI         OK
3-3 1       OK          Active
3-4 1       OK          OK
EXECUTED
```

6.14.9 STRDP – Status Remote Data Centre Print

Synopsis

This command requests a status report for the Remote Data Centres (RDCs). The status can be one of the following:

- OK - The RDC is available to receive data.
- Initiating - Initiating connection to the RDC.
- Failed - The RDC is not available to receive data.
- Blocked - The RDC is user blocked from receiving data.

File transfer is to the lowest numbered available RDC.

> ***Note:*** If the system does not have an IPADDR, then status indicates OK for communication with the RDC; however, no data can be transferred.

Syntax

```
STRDP;
```

Prerequisites

None

Attributes

None

Examples

```
STRDP;
```

Output Format

```
Remote Data Centre Status
RDC  IPADDR           RDCSTAT
1    25.03.203.52     Initiating
2    102.03.211.140   OK
EXECUTED
```

6.14.10 STSLP – Status SIGTRAN Link Print

Synopsis

This command requests the status of a SIGTRAN link.

Definitions for the status of the peer signaling process (SP):

- BLOCKED - The signaling link is blocked.
- UNAVAILABLE - The signaling link is unavailable.
- AVAILABLE - The signaling link is available.

Note: The SP STATUS is blank for M2PA SNLINKs. Layer 2 status is provided by the STC7P command.

Definitions for SCTP Status are:

- CONFIGURING - Association is being configured.
- COOKIE_WAIT - Association is waiting for a cookie.
- COOKIE_ECHOED - Association has echoed a cookie.
- CLOSED - Association is closed.
- INITIATING - Association is initiating.
- ESTABLISHED - Association is established.
- SHUTDOWN_PENDING - Association is pending shutdown.
- SHUTDOWN_SENT - Association has sent shutdown.
- SHUTDOWN_RECEIVED - Association has received shutdown.
- SHUTDOWN_ACK_SENT - Association has shutdown.

Definitions of the status of Links IP Addresses are:

- INACTIVE - Network address is inactive.
- ACTIVE - Network address is available for data transfer.
- BLOCKED - Network address is blocked.

The Retransmission TimeOut (RTO) is a time between 500 and 6000 milliseconds where SCTP waits before retransmitting an octet to an IP address. The timeout dynamically changes based on line conditions and provides an indication on the quality of the connection to that IP address.

Syntax

```
STSLP:[SNLINK=…];
```

Prerequisites

- If specified, the SIGTRAN link should already have been initiated.

Attributes

None

Examples

```
STSLP:SNLINK=1;
```

Output Format

```
Page 1 of 2 SIGTRAN Signaling Link Status
SNLINK SP STATUS   SCTP STATUS  LABEL
1      AVAILABLE   ESTABLISHED
2      BlOCKED
EXECUTED

Page 1 of 2 SIGTRAN Signaling Link Status
SNLINK IPADDR STATUS IPADDR RTO IPADDR2 STATUS IPADDR2 RTO LABEL
1      ACTIVE        500        ACTIVE         1500
2      BlOCKED
EXECUTED
```

6.14.11 STSYP – Status System Print

Synopsis

This command provides a summary of the load, uptime and alarms on the system. The meaning of each field in the output is as follows:

- CPU - A string identifying the CPU type and speed
- MEMORY - The amount of RAM in the system
- UPTIME - The length of time the application software has been running
- NRESTART - The number of times the system has restarted since factory installation
- LOADAVG1 - The UNIX load average measurement taken over one minute
- LOADAVG5 - The UNIX load average measurement taken over five minutes
- LOADAVG15 - The UNIX load average measurement taken over 15 minutes
- ALMSYS - The number of system alarms
- ALMPCM - The number of PCM alarms
- ALMSIG - The number of signaling alarms
- ALMCLA1 - The number of minor alarms
- ALMCLA2 - The number of major alarms
- ALMCLA3 - The number of critical alarms

Syntax

```
STSYP;
```

Prerequisites

None

Attributes

None

Examples

```
STSYP;
```

Output Format

```
System Status
CPU          2 X Intel(R) Xeon(TM) CPU 2.4GHz
MEMORY       1024MB
UPTIME       01:04:43
NRESTART     307
LOADAVG1     1.48%
LOADAVG5     1.49%
LOADAVG15    1.45%
ALMSYS       0
ALMPCM       9
ALMSIG       4
ALMCLA1      0
ALMCLA2      13
ALMCLA3      0
EXECUTED
```

Chapter 7: Configuration Overview

This section provides an overview of the various components that are used in the configuration of a Dialogic® SS7G2x Signaling Gateway and how these components relate to each other. The Signaling Gateway configuration is described in the following categories:

- System and Hardware – The configuration of system Ethernet addresses, signaling boards and PCMs.
- Signaling – The transmission of messages on the SS7 and IP side.
- Routing – The route SS7 messages take through the gateway.
- Management – Bringing entities in and out of service and monitoring system status.
- Dual Resilient Operation – Two Signaling Gateways acting as a single Point Code.
- MTP Default Routing – Allocation of a default route to MTP.

7.1 System, Hardware and Signaling Configuration

7.1.1 System Configuration

Each Signaling Gateway contains four Ethernet ports allowing it to communicate with four separate IP networks. The Ethernet interface is used for the transfer of SS7 signaling information over IP, for telnet communication with the management interface and the transfer of files (such as those for software update and configuration backup) using ftp between the Signaling Gateway and a remote server. The fourth IP network (IPADDR4) is reserved for management only and cannot be used for SIGTRAN operation.

A Signaling Gateway can be given a presence within an IP network using its first Ethernet port configured with an IP Address (IPADDR) and a Subnet Mask (SUBNET). If the Signaling Gateway is communicating with a destination that is not on the local subnet, a default IP gateway (GATEWAY) can be configured.

Optionally, the Signaling Gateway can be given a presence in up to two more subnets using additional Ethernet ports configured with a an IP addresses ((IPADDR2 or IPADDR3) and additional subnet masks (SUBNET2 or SUBNET3).

System level configuration is configured using the CNSYx set of commands.

Potentially the user may require communication with different IP gateways to reach other IP networks. Additional IP Gateways can be configured using the IPGWx set of commands.

After changing the IP configuration of a Signaling Gateway, it should be restarted using the MNRSI command.

Figure 4. Multiple IP Networks

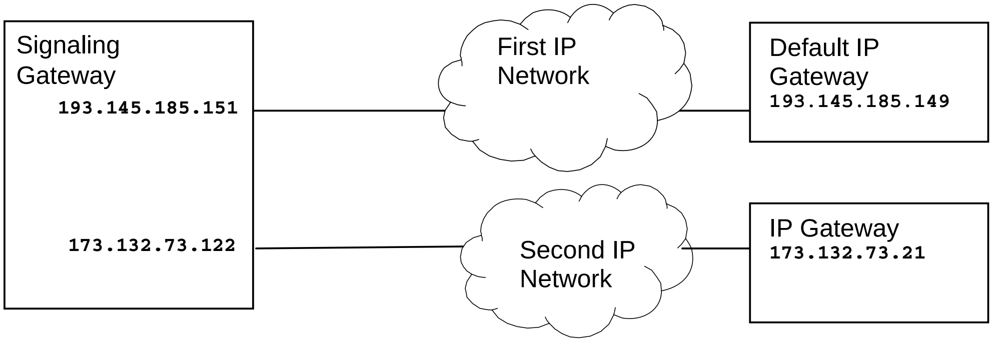


Figure 4 demonstrates the Signaling Gateway configured to exist in multiple IP networks. Example MML for the above configuration is:

```
CNSYS:IPADDR=193.145.185.151,SUBNET=255.255.255.0;
CNSYS:IPADDR2=173.132.73.122,SUBNET2=255.255.255.0;
CNSYS:GATEWAY=193.145.185.149;
MNRSI;
```

7.1.2 Boards and PCMs

A Signaling Gateway contains a number of SS7 signaling boards located in individual board positions (BPOS). Signaling boards are managed using the CNBOx commands.

An SS7 signaling board can terminate up to two PCM (PCM) trunks for connection to either a Signaling End Point (SEP) or Signaling Transfer Point (STP). When configuring the PCM, the user can specify whether it should act as E1 or T1 as well as its frame format (FF) and line code (LC). The configuration of a PCM also determines whether the port signal is to be used as the external clock synchronization source of the Signaling Gateway. Each PCM can be assigned a synchronization priority (SYNCPRI) specifying the priority it has within the Signaling Gateway to receive the external clock for the system. The PCM in the system with the lowest numbered synchronization priority that is active and in service provides the clocking source for the Signaling Gateway. If the current PCM providing clock for the system goes out of service, the PCM with the next highest clock priority that is in service provides clock for the Signaling Gateway. If a PCM's synchronization priority is set to 0, that PCM never provides clock for the system.

PCMs are managed using the CNPCx commands.

Figure 5. Physical Configuration

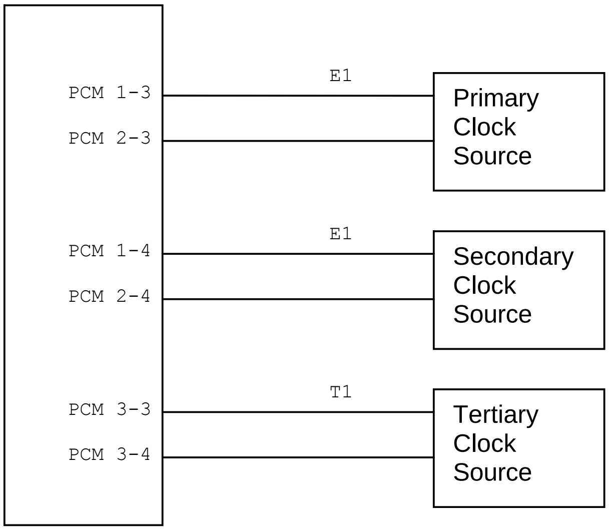


Figure 5 demonstrates a Signaling Gateway configured with three boards and six PCMs, four E1 and two T1 connect to primary, secondary and tertiary clock sources. Example MML for the above configuration is:

```
CNBOI:BPOS=1,BRDTYPE=SPCI2S-4-2,SIGTYPE=SS7;
CNBOI:BPOS=2,BRDTYPE=SPCI2S-4-2,SIGTYPE=SS7;
CNBOI:BPOS=3,BRDTYPE=SPCI2S-4-2,SIGTYPE=SS7;
CNPCI:PCM=1-3,PCMTYPE=E1,SYNCPRI=1;
CNPCI:PCM=2-3,PCMTYPE=E1,SYNCPRI=1;
CNPCI:PCM=1-4,PCMTYPE=E1,SYNCPRI=2;
CNPCI:PCM=2-4,PCMTYPE=E1,SYNCPRI=2;
CNPCI:PCM=3-3,PCMTYPE=T1,SYNCPRI=3;
CNPCI:PCM=3-4,PCMTYPE=T1,SYNCPRI=3;
```

7.2 Signaling Configuration

7.2.1 SS7 Configuration

A Link Set (LS) is the set of signaling links between an Originating Point Code (OPC) on the Signaling Gateway and an adjacent Destination Point Code (DPC). When specifying a link set the user can specify the MTP type and point code size (SS7MD), the SS7 Network Identifier (NI) and the logical network (NC) it belongs in. Link sets are managed using the C7LSx commands.

An SS7 Route (C7RT) identifies the link sets that are used to reach an eventual Destination Point Code (DPC). Two SS7 routes cannot have the same DPC within the same network. An SS7 route utilizes link sets (LS1 and LS2) to adjacent points to reach an eventual destination. An adjacent point can be a Signaling Transfer Point (STP), where SS7 information is forwarded on into the SS7 network, or the eventual destination. SS7 routes are managed using the C7RTx commands.

SS7 MTP2 Operation

An SS7 signaling link (C7LINK) processor (EQU) receives and transmits SS7 signaling information over a timeslot (TS) on an E1 or T1 bearer or a serial V.11 interface. An SS7 Signaling link is identified uniquely within an SS7 link set by the Signaling Link Code (SLC). Signaling links are managed using the C7SLx commands.

Figure 6. SS7 Signaling Example

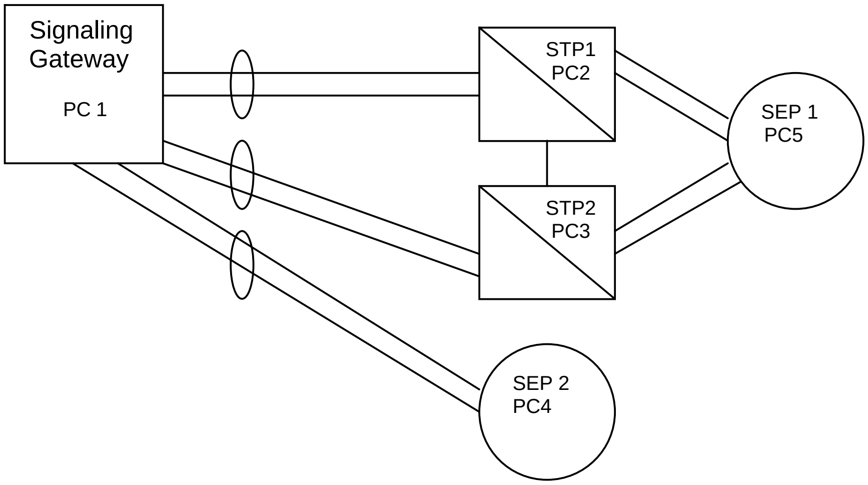


Figure 6 demonstrates a Signaling Gateway routing to two SS7 Signaling End Points (SEP). The first SEP is reached by a pair of STPs, while the second SEP is reached directly from the Signaling Gateway. Example MML for the above configuration is:

```
C7LSI:LS=1,OPC=1,DPC=2,SS7MD=ITU14,LSSIZE=2,NI=2,NC=1;
C7LSI:LS=2,OPC=1,DPC=3,SS7MD=ITU14,LSSIZE=2,NI=2,NC=1;
C7LSI:LS=3,OPC=1,DPC=4,SS7MD=ITU14,LSSIZE=2,NI=2,NC=1;
C7SLI:C7LINK=1,LS=1,EQU=2-1,TS=1-3-16,SLC=0;
C7SLI:C7LINK=2,LS=1,EQU=3-1,TS=2-3-16,SLC=1;
C7SLI:C7LINK=3,LS=2,EQU=2-2,TS=1-4-16,SLC=0;
C7SLI:C7LINK=4,LS=2,EQU=3-2,TS=2-4-16,SLC=1;
C7SLI:C7LINK=5,LS=3,EQU=2-3,TS=3-3-16,SLC=0;
C7SLI:C7LINK=6,LS=3,EQU=3-3,TS=3-4-16,SLC=1;
C7RTI:C7RT=1,NC=1,DPC=2,LS1=1,LABEL=STP1;
C7RTI:C7RT=2,NC=1,DPC=3,LS1=2,LABEL=STP2;
C7RTI:C7RT=3,NC=1,DPC=4,LS1=3,LABEL=SEP2;
C7RTI:C7RT=4,NC=1,DPC=5,LS1=1,LS2=2,LABEL=SEP1;
```

SS7 M2PA Operation

The Signaling Gateway is capable of replacing TDM SS7 links with signaling links operating over IP providing the equivalent functionality to MTP layer 2 by using the SIGTRAN M2PA protocol. Typically M2PA signaling links would be used when the Signalling Gateway is either offering longhaul over IP operation between two SEPs, or when two Signaling Gateways are acting as a single Point Code and the inter Signaling Gateway SS7 link is provided by M2PA over IP.

For M2PA operation, rather than associating an EQU or TS with an SS7 signaling link (C7LINK), the SS7 link is instead associated with a SIGTRAN link (SNLINK) defined to be of type M2PA. The SIGTRAN link is used to identify a SCTP Association as being used for M2PA operation.

Figure 7. M2PA Example

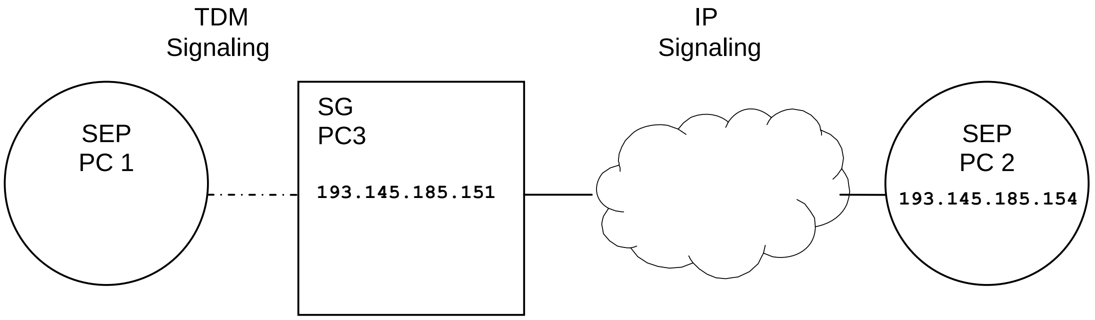


Figure 7 shows an example of a Signaling Gateway connected to a SEP on the TDM side and a SEP on the IP side.

Example MML for the SIGTRAN M2PA part of the above configuration is:

```
SNSLI:SNLINK=1,SNTYPE=M2PA,END=C,IPADDR=194.192.185.11,
      HPORT=3565,PPORT=3565,LABEL=SEP2-1;
SNSLI:SNLINK=2,SNTYPE=M2PA,END=C,IPADDR=194.192.185.11,
      HPORT=3566,PPORT=3566,LABEL=SEP2-2;
C7LSI:LS=2,OPC=3,DPC=2,LSSIZE=2,SS7MD=ITU14,NC=1,NI=2;
C7SLI:C7LINK=3,SNLINK=1,LS=2,SLC=0;
C7SLI:C7LINK=4,SNLINK=2,LS=2,SLC=1;
C7RTI:C7RT=2,NC=1,DPC=2,LS1=2;
```

7.2.2 M3UA Configuration

The Signaling Gateway employs M3UA to “backhaul” SS7 information to an SS7 resident application. The Signaling Gateway uses the Stream Control Transmission Protocol (SCTP) to provide a reliable transport protocol operating on top of IP. The relationship between the SCTP node on the Signaling Gateway and a peer node is known as an “association”. The Signaling Gateway employs the M3UA protocol to support the transport of any SS7 MTP3 user signaling (for example, ISUP and SCCP messages) over IP using the services of SCTP.

In backhaul operation, the Signaling Gateway communicates over an SCTP association using M3UA to an Application Server Process (ASP). An ASP is a host computer serving as an active or backup process of an Application Server (for example, part of a distributed virtual switch or database). Examples of ASPs are processes (or process instances) of MGCs, IP SCPs or HLRs. An ASP is an SCTP endpoint and may be configured to process signaling traffic within more than one Application Server.

A SIGTRAN link (SNLINK) identifies both the SCTP Association and the peer ASP that uses the Association.

The user can configure the Peer IP addresses (IPADDR, and optionally IPADDR2, a second IP address for resilience), a host port (HPORT) and a peer port (PPORT). The user can also configure the SIGTRAN link to act as an IP client or IP server (END), the network the SIGTRAN link exists in (NC) and the Point Code format that the SIGTRAN link uses (SS7MD). SIGTRAN links are managed using the SNSLx commands.

An Application Server (AS) is the logical entity serving a specific “routing key”. An example of an Application Server is a virtual switch element handling all call processing for a unique range of PSTN trunks, identified by an SS7 DPC/OPC/CIC range. Another example is a virtual database element, handling all HLR transactions for a particular SS7 DPC/OPC/SCCP SSN combination.

The Application Server contains a set of one or more unique SNLINKs of which one or more is normally actively processing traffic. There is a 1:1 relationship between an Application Server and a specific “routing key”. The user can configure an Application Server’s Destination Point Code (DPC) of the routing key as well as the Routing Context (RC) that uniquely identifies the routing key to the peer host application across the SIGTRAN link.

Application Servers are managed using the SNAPx commands and are associated to SIGTRAN links using the SNALx commands.

Figure 8. M3UA Backhaul Example

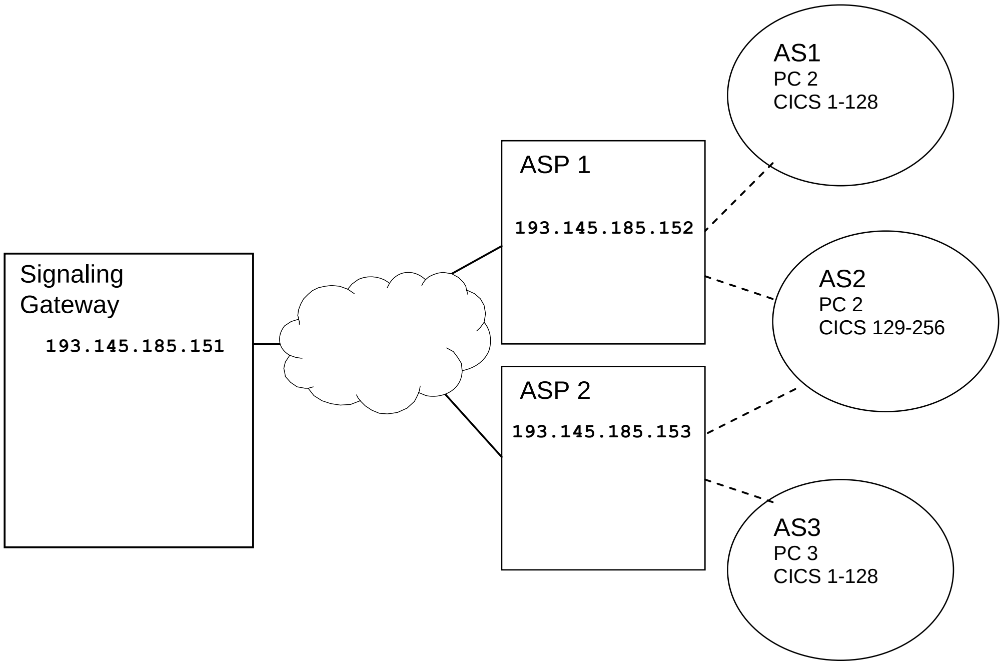


Figure 8 demonstrates a Signaling Gateway communicating over SIGTRAN links with two ASPs. ASP 1 is running two AS instances, AS1 processes CICs 1 to 128 in PC 2, and AS2 processes CICs 129 to 256 also in PC 2. ASP 2 is also running two AS instances, AS3 processes CICs 1 to 128 in PC 3 and AS2 processes CICs 129 to 256 also in PC 2. Note that AS2 is running on ASP1 and ASP2. The two ASPs could be load sharing processing for the AS or one could be active, while the other standby. The configuration of load sharing is performed by the ASPs. Example MML for the above configuration is:

```
SNSLI:SNLINK=1,SNTYPE=SGM3UA,END=S,IPADDR=193.145.185.152,
      SS7MD=ITU14,NC=1,LABEL=ASP1;
SNSLI:SNLINK=2,SNTYPE=SGM3UA,END=S,IPADDR=193.145.185.153,
      SS7MD=ITU14,NC=1,LABEL=ASP2;
SNAPI:AS=1,NC=1,DPC=2,RC=1,LABEL=AS1;
SNAPI:AS=2,NC=1,DPC=2,RC=2,LABEL=AS2;
SNAPI:AS=3,NC=1,DPC=3,RC=3,LABEL=AS3;
SNALI:AS=1,SEQ=1,SNLINK=1;
SNALI:AS=2,SEQ=1,SNLINK=1;
SNALI:AS=2,SEQ=2,SNLINK=2;
SNALI:AS=3,SEQ=1,SNLINK=2;
```

7.3 Routing Configuration

The routing model for the Signaling Gateway can be broken into three parts; incoming route selection, routing key processing and destination selection.

An Incoming Route (IR) identifies the side from which signaling data originates. MTP messages are considered to arrive from either the MTP domain over an SS7 link set (LS) using MTP2 or M2PA SS7 links (C7LINK) or the SIGTRAN IP domain over a M3UA SIGTRAN link (SNLINK). The SS7 link set or M3UA SIGTRAN link identifies the network (NC) and SS7 format (SS7MD) of the message. The IR configuration either explicitly identifies a destination or a routing key table (RKTAB) that is used to identify a destination (DEST). Incoming routes are managed using the SGIRx commands.

If the Signaling Gateway determines that a Routing Key Table (RKTAB) should be looked up, data from the message is compared with routing keys components (such as NC, SI, NI, OPC, DPC, CICs) in a routing key table. If a match is found and the Destination Point (DEST) for that routing key combination is in service, the routing key's Destination Point is used otherwise if the incoming route also had a Destination Point associated with it, then that default destination is used. Routing keys are managed using the SGRKx commands.

A Destination Point (DEST) can route a message to an Application Server (AS) or to MTP (using MTP2 or M2PA SS7 links) for routing based on Point Code. MTP routing can be selected by specifying an RTPRI of MTP. AS routing can be selected by specifying an RTPRI of NONE and identifying the AS that the messages should be routed to. Destinations are managed using the SGDPx commands.

It is worth noting that in many configurations, routing key analysis is not required and the user can configure an Incoming Route to go directly to a Destination without having to explicitly provide routing key information, such as Destination Point Codes, for every eventual destination.

Figure 9. Routing Configuration Example

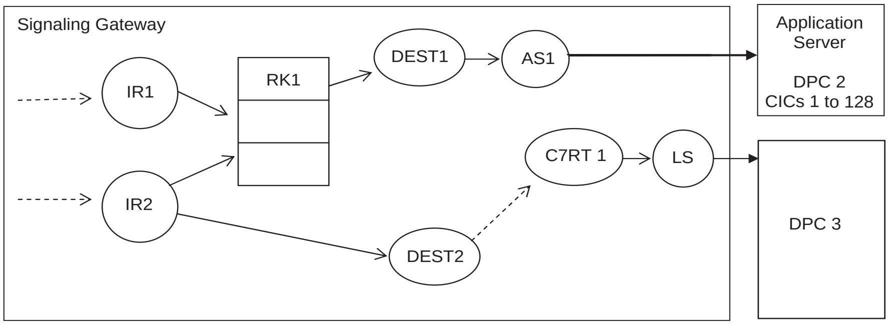


Figure 9 demonstrates example relationships between entities in the routing model. Relationships with full lines indicate that there is an explicit relationship between the entities (that is, one entity selects the other). Relationships with dotted lines indicate that the relationship is implicit, for example, if data arrives on a SIGTRAN link over M3UA, it is implicitly coming from the SIGTRAN IP domain and similarly if data arrives on an SS7 link set, it is implicitly arriving from the MTP domain.

> ***Note:*** A message arriving from M2PA is considered as arriving from the MTP domain.

This example identifies two incoming routes, IR 1 from SIGTRAN IP and IR 2 from the MTP side. IR 1 and IR 2 go to the Routing Key Table 1 for routing key analysis. If the analysis fails, or the destination found by the analysis (Application Server AS1) is out of service, the Signaling Gateway discards messages from IR 1. The Signaling Gateway however attempts to route messages from IR 2 to Destination 2 only discards those messages if the SS7 route C7RT 1 is also out of service.

This example identifies two incoming routes, IR 1 from SIGTRAN IP and IR 2 from the MTP side. IR 1 goes to Routing Key Table 1 for routing key analysis. IR 2 also goes to Routing Key Table 1 for analysis, however, if analysis fails, or the destination found by analysis (either a MTP or SIGTRAN IP route or Application Server) is out of service, it attempts to route to Destination 2.

The routing key table has one entry as follows:

- The entry that routes all SS7 messages with DPC 2 and CICs 1 to 128 to Destination 1.

There are two Destinations:

- Destination 1 routes to Application Server 1.
- Destination 2 routes all messages to the MTP side.

Example MML for the routing part of the above configuration is as follows:

> ***Note:*** The Destinations Point are configured first, followed by the Routing Key Tables, and then finally the Incoming Routes.

```
SGDPI:DEST=1,RTPRI=NONE,AS=1;
SGDPI:DEST=2,RTPRI=MTP;
SGRKI:RKI=1,RKTAB=1,DPC=2,BCIC=1,RANGE=128,NC=1,DEST=1;
SGIRI:IR=1,NC=1,DOMAIN=IP,RKTAB=1;
SGIRI:IR=2,NC=1,DOMAIN=MTP,RKTAB=1,DEST=2;
```

7.4 Management and Operations

Entities such as boards, SS7 links, SIGTRAN links and Application Servers after configuration are considered to be in the “blocked” state. The configuration exists in the system for these entities, but these entities are not considered to be active. To activate an entity, the MNBLI command should be used. To temporally deactivate an entity, the MNBLE command should be used.

The status of entities such as boards, SS7 links, SIGTRAN links and Application Servers can be examined using the STxxx set of commands.

Alarms that occur on the Signaling Gateway can be view using the ALLOP and ALLIP commands.

7.5 Default Routing

The Signaling Gateway offers a Default Routing service. This service allows the Signaling Gateway to onward route MTP Message Signal Units (MSUs) with unknown Destination Point Codes (DPCs). It also provides a mechanism for Signaling Network Management messages to be generated for unknown Point Codes.

Figure 10 shows a typical system that uses Default Routing. The SPCs with Point Codes 1, 2 and 3 can each communicate with many Point Codes within the MTP Network not all of which the SS7G2x has been configured to know about. The SS7G2x connects to two STPs that have been explicitly configured to know about more Point Codes than the SS7G2x.

7.5.1 Configuring Default Routing

Default Routing is configured using the C7RTI command with the DPC parameter set to “DFLT”. An additional route is configured with the LS1 and LS2 parameters identifying the link sets to the STPs and the PC set to DFLT.

Routing MSUs

When the Default Route is configured, on receipt of an MSU for an unknown DPC, the message is sent out on an available link set in the Default Route or discarded.

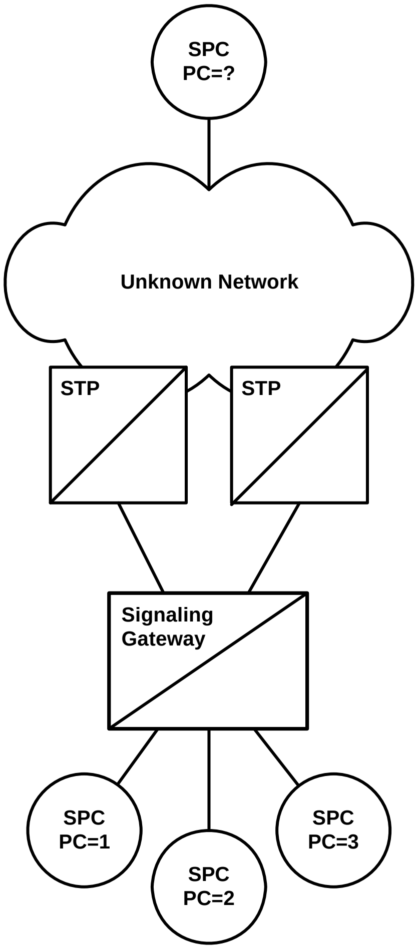
Route Set Test

SEPs send the Signaling Gateway RST messages for unknown Point Codes. The SS7G2x regenerates these messages and sends them to the STPs that responds to the Signaling Gateway with appropriate SNM messages.

Transfer Prohibited / Transfer Allowed

On receipt of TFA or TFP from one of the STPs in the Default Route, the Signaling Gateway regenerates and broadcasts these to all SEPs not in the Default Route.

Figure 10. System Using Default Routing



7.6 Resilience

7.6.1 IP Port Bonding

The Signalling Gateway allows the user to configure a resilient IP connection across an IP port bonding team of two ports in an active/standby configuration. Up to two port teams may be created using the four Ethernet ports on the SIU. Each team has a single IP address configured with a primary (active) and secondary (standby) port. Any IP port on the system may be the primary port in a team and any port may be the secondary port. The primary port is a port configured with the IP address of the team and the secondary port is a port configured with a string to associate it with the primary port (see Section 6.5.17, “CNSYS” on page 57).

If the system detects that the Primary port has failed, it passes the primary’s MAC and Layer 3 address to the failover (secondary) adapter, enabling it to act as the active port in the team. On the restoration of the primary port, the secondary port is removed from service and the primary port resumes control of its MAC and IP addresses.

The subnet mask of a secondary IP address in a team is ignored. Data loss may occur between the actual failure of an IP connect and the detection of that failure and subsequent switching to the standby port. All adapters in a team should be connected to the same hub or switch with Spanning Tree (STP) set to **off**.

Whenever teaming is activated, or deactivated, MMI sessions using those ports are reset. An IP address may not teamed with:

- itself
- an IP address of 0.0.0.0
- another IP address already acting as a primary or standby in an IP team

7.6.2 Dual Resilient Operation

Two Signaling Gateways have the ability to work in conjunction with one another to realize a single SS7 signaling point where the operation of the Message Transfer Part (MTP) is distributed. Failure (or planned maintenance) of one or other of the Signaling Gateways operating in “Dual Mode” therefore does not result in a loss of SS7 signaling capability.

The use of the dual functionality does introduce some restrictions that are described below. The user is responsible for ensuring that these restrictions are acceptable, otherwise the dual mode of operation may not be applicable.

7.6.2.1 Overview of Dual Resilience

The dual Signaling Gateway solution assumes that each Signaling Gateway has one (or more) signaling links facing the network.

The ability for each of the Signaling Gateways to communicate with each other is addressed by adding an additional link set (containing one or two links, for example LS2 in Figure 11, “Dual Resilient Operation” on page 144) between the two platforms. This link set is used to convey network status and management messages between the two halves of the system and to pass signaling traffic as necessary.

On each Signaling Gateway, there is (a minimum of) two link sets, one connected to the adjacent signaling point and the other connected to the other half of the dual pair. Each MTP route is configured so that the primary link set is the link set connected to the adjacent signaling point and the secondary link set is the link set connected to the partner Signaling Gateway. Load sharing across these link sets is disabled.

The link set between the two halves of the dual Signaling Gateway is configured so that the originating and destination point codes are identical.

Under normal circumstances, messages that have been determined for the SS7 network are routed directly over the link set that connects to the adjacent signaling point. Under failure conditions, when the link to the adjacent signaling point is not available, the traffic messages are sent instead on the secondary link set to the partner Signaling Gateway. On receipt of these messages, the partner Signaling Gateway recognizes that the message is not destined for itself and transfers the message to its network-facing link set.

The signaling that takes place between each half of the dual Signaling Gateway system makes use of two reserved Network Indicator values in the Sub-Service Field, these values designated “National - Reserved” and “International - Reserved” must therefore not be used for signaling either to or from the network.

The link set between the two halves of the dual pair now becomes a key element in the system and to avoid a single point of failure, this link set should contain at least two signaling links. Where possible, these links should be located on different signaling boards.

7.6.2.2 Configuration

Each half of the dual configuration needs to be configured separately using existing configuration techniques and noting the following.

The additional link set between the two Signaling Gateways should have the local point code and the adjacent point code set to the same value.

Each route to a destination signaling point should be configured to use the network link set as the primary link set and the inter Signaling Gateway link set as the secondary link set. Load sharing must be disabled.

When connecting to a pair of adjacent STPs, each STP must have a route declared on each Signaling Gateway and in all cases the inter-Signaling Gateway link set must be specified as the secondary link set.

A route must be configured to the other half of the dual Signaling Gateway system, this must use the inter-Signaling Gateway link set as the only link set.

In addition, the link set between the two halves of the dual Signaling Gateway system must be designated as a “special” link set. The method of achieving this depends on the equipment and configuration tools in use as follows:

Use the C7LSI command to initiate a link set with the same values for the OPC and DPC parameters and the value of the DUAL parameter set to zero.

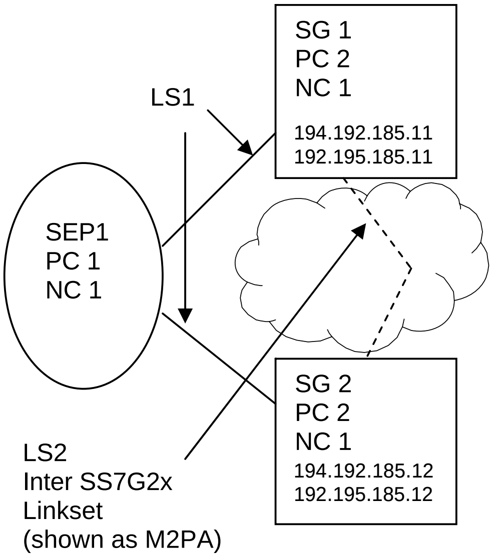
7.6.2.3 M2PA Inter Unit Signaling Links

The Signaling Gateway supports the use of M2PA SIGTRAN links for inter Signaling Gateway communication. M2PA SS7 links use the SCTP IP protocol to transmit signaling data. Use of IP links between the units rather than TDM SS7 links allow the systems to be able to present a greater number of TDM links and PCMs to face the SS7 network. In addition, since the Signaling Gateway supports two IP ports and M2PA supports IP multihoming, resilience between the units can be gained using redundant IP networks rather than the two SS7 boards that would be required to offer the same level of resilience.

7.6.2.4 Example

Figure 11 is an example of a DUAL resilient configuration using M2PA links for the resilient links between units.

Figure 11. Dual Resilient Operation



On Signaling Gateway 1, configure the IP addresses as follows and restart:

```
CNSYS:IPADDR=194.192.185.11,IPADDR2=194.192.185.11;
MNRSI;
```

On Signaling Gateway 1, configure the link sets as follows:

```
C7LSI:LS=1,OPC=2,DPC=1,LSSIZE=2,SS7MD=ITU14,NI=2,NC=1;
C7LSI:LS=2,OPC=2,DPC=2,LSSIZE=2,SS7MD=ITU14,NI=2,NC=1;
```

On Signaling Gateway 1, configure the SIGTRAN link as follows:

```
SNSLI:SNLINK=1,SNTYPE=M2PA,IPADDR=194.192.185.12,
IPADDR2=192.195.185.12,END=C;
```

On Signaling Gateway 1, configure the signaling links as follows:

```
C7SLI:C7LINK=1,EQU=1-1,TS=1-1-1,LS=1,SLC=0;
C7SLI:C7LINK=2,SNLINK=1,LS=2,SLC=0;
```

On Signaling Gateway 1, configure the SS7 routes as follows:

```
C7RTI:C7RT=1,DPC=1,LS1=1,LS2=2,NC=1,LABEL=SEP1;
C7RTI:C7RT=2,LS1=2,DPC=2,NC=1,LABEL=INTERLINK;
```

On Signaling Gateway 2, configure the IP addresses as follows and restart:

```
CNSYS:IPADDR=194.192.185.12,IPADDR2=194.192.185.12;
MNRSI;
```

On Signaling Gateway 2, configure the link sets as follows:

```
C7LSI:LS=1,OPC=2,DPC=1,LSSIZE=2,SS7MD=ITU14,NI=2,NC=1;
C7LSI:LS=2,OPC=2,DPC=2,LSSIZE=2,SS7MD=ITU14,NI=2,NC=1;
```

On Signaling Gateway 2, configure the SIGTRAN link as follows:

```
SNSLI:SNLINK=1,SNTYPE=M2PA,IPADDR=194.192.185.11,
IPADDR2=192.195.185.11,END=C;
```

On Signaling Gateway 2, configure the signaling links as follows:

```
C7SLI:C7LINK=1,EQU=1-1,TS=1-1-1,LS=1,SLC=1;
C7SLI:C7LINK=2,SNLINK=1,LS=2,SLC=0;
```

On Signaling Gateway 2, configure the SS7 routes as follows:

```
C7RTI:C7RT=1,DPC=1,LS1=1,LS2=2,NC=1,LABEL=SEP1;
C7RTI:C7RT=2,LS1=2,DPC=2,NC=1,LABEL=INTERLINK;
```

Linkset 1 is configured for both Signaling Gateways and has a destination point code of the SS7 switch.

Linkset 2 is a special linkset that has the same OPC and DPC. It is used to route messages destined for CICs on the partner Signaling Gateway.

C7 route 1 is used to route calls from the Signaling Gateways to the SS7 switch, if LS1 is not available, the signaling is routed via the partner Signaling Gateway using LS2. This is the C7 route assigned to circuit groups.

7.6.3 Multihoming

An inherent property of the SCTP layer on the Signaling Gateway that is used in SIGTRAN Signaling (for example, SS7 over M2PA) is that it supports IP multihoming. IP multihoming allows the SIGTRAN signaling link SCTP association to be configured to communicate with multiple IP addresses in an active/standby relationship. Multihoming offers a SIGTRAN signaling link significantly greater resilience since the link can be configured with multiple IP addresses to operate over separate Ethernet ports within wholly separate IP networks. IP ports and local IP addresses on the Signaling Gateway may be configured using the CNSYS command (see page 57). SIGTRAN links may be configured to communicate with multiple remote IP addresses using the SNSLI command (see page 120).

Chapter 8: Alarm Fault Code Listing

A system operator can obtain a listing of the current alarm status (class, category and ID) of a SS7G2x using the ALLIP management terminal command described in Section 6.4.4, "ALLIP" on page 44 or a log of current and cleared alarms using the ALLOP management terminal command described in Section 6.4.5, "ALLOP" on page 45. Table 9 details the possible alarm types accessed by the ALLIP command. Alarm status/events may also be accessed/reported by front panel LEDs, relay connections and SNMP, as described in Section 1.9.6, "Alarm Log" on page 12.

Note: The meaning of individual event codes (in particular, the coding of the DIAG field) may be changed in subsequent releases of the Signaling Gateway software without prior notification.

Table 9. Alarm Fault Codes

Severity (LED)	CODE	Name	Event Description	CATEGORY	ID	Class †	DIAG
Critical (CRT)	11	Link set fail	All signaling links in an SS7 signaling link set have failed. Usually due to incorrect configuration (Point Codes or signaling timeslots), connectivity fault or inactive signaling terminal at the remote end.	SIG	LS	3	0
Critical (CRT)	12	Board failure	The Signaling Gateway has detected a fault with a signaling processor. This may either be due to a faulty signaling processor board or due to the Signaling Gateway performing a controlled shutdown of a signaling processor following persistent overload of the processor in order to prevent the overload affecting the remainder of the system. Usually due to faulty board (which can be confirmed by changing SS7 links to an alternative processor board using the C7LSC command) or unusual signaling conditions which may be due to incorrect configuration or a mismatch of configuration between the Signaling Gateway and the remote end. This alarm condition can only be cleared by manual intervention, the user should block and unblock the affected board. Note that a Processor Fail entry always appears in the alarm log when a board is unblocked, this condition is identified by an event with identical Occurred and Cleared times.	SYS	BPOS	3	0
Critical (CRT)	14	Self Test fail	The Signaling Gateway has detected a self test failure which prevents normal operation.	SYS	0	3	0
Critical (CRT)	18	Alarm Test 3	This event indicates that the user has invoked the alarm test for alarm class 3 using the ALTEI command.	SYS	0	3	0

† The "Class" column provides the initial default setting of the alarm class for each fault code. The alarm class for any particular alarm code is configurable using the ALCLS command and can be viewed using the ALCLP command. Changing the alarm class for an event type changes the Severity indicated by the LEDs and/or relays.

Table 9. Alarm Fault Codes (Continued)

Severity (LED)	CODE	Name	Event Description	CATEGORY	ID	Class †	DIAG
Critical (CRT)	32	Overload	The Signaling Gateway has detected the onset of an internal overload condition. This is usually due either to exceptionally high traffic rates or failure conditions causing additional invocation of maintenance procedures. During overload the Signaling Gateway will continue to operate as normal. Should the condition occur on a frequent basis (for example, during the busy hour every day) the condition should be reported to your support representative.	SYS	0	3	0
Critical (CRT)	41	All RDC fail	Failure of communication with all remote data centres. Continuous records are written to hard disk or discarded as appropriate. Periodic report data is discarded.	SYS	0	3	0
Critical (CRT)	46	Hard disk fail	Interaction with the hard disk is no longer possible. No further use of the hard disk is attempted until the system is restarted. The most likely cause is a physical failure of the hard disk drive.	SYS	0	3	Diagnostic code
Critical (CRT)	63	PSU failure	The system has detected that one or more power supplies have failed. The system is able to operate with the loss of a single power supply but the power supply must be replaced at the earliest possible opportunity.	SYS	PSU ID	3	0
Critical (CRT)	72	Fan failure	The system has detected a failure of one or more or its cooling fans leading to an inadequate cooling supply. The faulty fan(s) should be replaced immediately.	SYS	0	3	0
Critical (CRT)	76	CPU warning	The system has detected that one or more of the CPUs is likely to fail.	SYS		3	
Critical (CRT)	77	CPU failure	The system has detected that one or more of the CPUs has failed.	SYS		3	
Critical (CRT)	78	Memory failure	The system has detected that one or more of its memory modules has failed.	SYS		3	
Major (MJR)	1	PCM loss	Loss of signal at PCM input port	PCM	PCM	2	0
Major (MJR)	2	AIS	PCM input port contains the Alarm Indication Signal (all ones on all timeslots)	PCM	PCM	2	0
Major (MJR)	3	Frame sync loss	Loss of frame alignment on PCM port	PCM	PCM	2	0
Major (MJR)	4	Frame slip	A frame slip occurred on the PCM port. This alarm event is given for each occurrence of a frame slip.	PCM	PCM	2	0
Major (MJR)	5	Remote alarm	PCM port is receiving a Remote Alarm Indication. This usually indicates that the remote end is either failing to achieve frame alignment or that it is experiencing a high bit error rate on the received signal.	PCM	PCM	2	0

† The “Class” column provides the initial default setting of the alarm class for each fault code. The alarm class for any particular alarm code is configurable using the ALCLS command and can be viewed using the ALCLP command. Changing the alarm class for an event type changes the Severity indicated by the LEDs and/or relays.

Table 9. Alarm Fault Codes (Continued)

Severity (LED)	CODE	Name	Event Description	CATEGORY	ID	Class †	DIAG
Major (MJR)	6	BER > 1:10^5	The input PCM signal contains a Bit Error Rate (BER) in excess of 1 in 100,000 as measured on the frame alignment pattern. This is usually due to faulty cabling or a faulty PCM board at the remote end.	PCM	PCM	2	0
Major (MJR)	7	BER > 1:10^3	The input PCM signal contains a Bit Error Rate (BER) in excess of 1 in 1000 as measured on the frame alignment pattern. This is usually due to faulty cabling or a faulty PCM board at the remote end.	PCM	PCM	2	0
Major (MJR)	9	C7 link fail	An SS7 signaling link has failed. Usually due to incorrect configuration (signaling timeslot), connectivity fault or inactive signaling terminal at the remote end.	SIG	C7LINK	2	0
Major (MJR)	15	Fan warning	The system has detected either the failure of one of the cooling fans or that a fan is likely to fail. The cooling will remain adequate during this condition but the fan should be replaced at the next convenient opportunity.	SYS	0	2	0
Major (MJR))	17	Alarm Test 2	This event indicates that the user has invoked the alarm test for alarm class 2 using the ALTEI command.	SYS	0	2	0
Major (MJR)	20	Temperature	The internal temperature is outside a preset threshold indicating either an internal fault or failure of the cooling arrangements. Inspection should take place immediately.	SYS	CPU ID	2	0
Major (MJR)	33	Sync failure	None of the PCM ports that have been configured as possible clock sources contain a valid PCM signal. Under these conditions the Signaling Gateway will generate synchronisation using a local oscillator.	PCM	0	2	0
Major (MJR)	35	PCM error ind	Diagnostic event relating to the PCM functionality. Persistent events of this type should be reported to your support representative.	NONE		2	
Major (MJR)	36	PCM event ind	Diagnostic information relating to PCMs.	NONE		2	
Major (MJR)	39	System restart req	The user has changed configuration parameters that require the system to be restarted before they can take effect. The alarm will persist until the system is restarted.	SYS	0	2	0
Major (MJR)	40	RDC failure	Failure of communication with a remote data centre. Usually due to incorrect configuration (IP address, username or password), connectivity fault or inactive equipment at the remote end.	SIG	RDC	2	0
Major (MJR)	42	RDC err ind	Diagnostic event relating to the transfer of data to an RDC. Persistent events of this type should be reported to your support representative.	NONE		2	

† The “Class” column provides the initial default setting of the alarm class for each fault code. The alarm class for any particular alarm code is configurable using the ALCLS command and can be viewed using the ALCLP command. Changing the alarm class for an event type changes the Severity indicated by the LEDs and/or relays.

Table 9. Alarm Fault Codes (Continued)

Severity (LED)	CODE	Name	Event Description	CATEGORY	ID	Class †	DIAG
Major (MJR)	44	CR send fail	The Signaling Gateway is unable to transfer information to an RDC for a Continuous Record. Possible problems include: no RDCs available, directory does not exist on RDC for this CR, write failure on RDC. If the problem clears, this alarm will persist until any records saved on the hard disk during the failure have been successfully transferred to an RDC.	NONE	RECORD	2	Diagnostic code
Major (MJR)	45	PR send fail	The Signaling Gateway is unable to transfer information to an RDC for a Periodic Report. Possible problems include: no RDCs available, directory does not exist on RDC for this PR, write failure on RDC. If the problem clears, then the alarm will clear at the next successful transfer of data for the Periodic Report.	NONE	REPORT	2	Diagnostic code
Major (MJR)	47	Hard disk full	The hard disk drive capacity for a Continuous Record has reached its limit. Either there is no more space on the hard disk drive to store data, or this continuous record has the maximum amount of data stored for it on the hard drive. In both cases, records is discarded until an RDC recovers and all stored records are transferred from the Signaling Gateway. The alarm will then clear.		RECORD	2	
Major (MJR)	50	Board cong	A board has reached a congestion threshold. Boards repeatedly entering congestion indicate a need to increase the dimensioning of the switch.	SYS	BPOS	2	
Major (MJR)	53	PCM mismatch	The PCMTYPE setting is inconsistent with the hardware settings on the board.	SYS	PCM	2	0
Major (MJR)	61	Software mismatch	The system has only partially been upgraded and a full software update is required. The system is running in 'safe' mode running limited management software. No circuits have been brought into service.	SYS	0	2	0
Major (MJR)	62	C7 link Cong	A SS7 signaling link is encountering congestion.	SIG	C7LINK	2	0
Major (MJR)	64	Power warning	The system has detected that the voltage on one or more power rails is out of range. This is usually due to either a faulty power supply module or a faulty board causing excessive current consumption.	SYS	0	2	0
Major (MJR)	65	Assoc fail	A SIGTRAN signaling link has failed. Usually due to incorrect configuration (connectivity fault or inactive signaling at the remote end.	SIG	SNLINK	2	0
Major (MJR)	66	NIF event ind	Diagnostic event relating to the Nodal Interworking Function. Persistent events of this type should be reported to your support representative.	NONE		2	

† The "Class" column provides the initial default setting of the alarm class for each fault code. The alarm class for any particular alarm code is configurable using the ALCLS command and can be viewed using the ALCLP command. Changing the alarm class for an event type changes the Severity indicated by the LEDs and/or relays.

Table 9. Alarm Fault Codes (Continued)

Severity (LED)	CODE	Name	Event Description	CATEGORY	ID	Class †	DIAG
Major (MJR)	67	NIF err ind	Diagnostic event relating to the Network Interface Function. Persistent events of this type should be reported to your support representative.	NONE		2	
Major (MJR)	68	SNRT unavail	Reserved	SIG	NC	2	0
Major (MJR)	69	C7RT unavail	One or more SS7 routes are unavailable	SIG	NC	2	0
Major (MJR)	70	AS unavail	One or more SIGTRAN Application Servers are unavailable	SIG	NC	2	0
Major (MJR)	71	AS under res	One or more SIGTRAN Application Servers are available but have insufficient number of ASP (load sharing mode only)	SIG	NC	2	0
Major (MJR)	73	M2PA event ind	Diagnostic event relating to the M2PA protocol layer. Persistent events of this type should be reported to your support representative.	NONE		2	
Major (MJR)	74	M2PA err ind	Diagnostic event relating to the M2PA protocol layer. Persistent events of this type should be reported to your support representative.	NONE		2	
Minor (MRN)	16	Alarm Test 1	This event indicates that the user has invoked the alarm test for alarm class 1 using the ALTEI command.	SYS	0	1	0
Minor (MRN)	19	System Restart	This event indicates the time at which a system restart occurred.	SYS	0	1	0
Minor (MRN)	34	New sync source	The Signaling Gateway has selected a new PCM as the clock synchronization source.	PCM	PCM	1	
Minor (MRN)	79	Default alarm	The system has detected a low priority low level alarm condition. The user should contact their support contact for further information.	SYS		1	

† The “Class” column provides the initial default setting of the alarm class for each fault code. The alarm class for any particular alarm code is configurable using the ALCLS command and can be viewed using the ALCLP command. Changing the alarm class for an event type changes the Severity indicated by the LEDs and/or relays.

Chapter 9: Remote Data Centre Operation

The Remote Data Centre (RDC) service allows the transfer of data between the Signaling Gateway and a remote computer located at a remote management centre. Data is transferred over a local or wide area network using the ftp protocol.

Up to four different RDCs can be configured and each report can be configured to use two RDC's (one as the primary RDC and the other as the backup RDC). This ensures continuity of service in case the connection to the primary RDC fails.

The RDC uses the ftp file transfer mechanism to exchange data with the remote site. The remote site requires only an industry standard ftp server to handle the file transfer and does not require any proprietary software on the remote computer. The Signaling Gateway “logs on” to the remote computer using a user-configured user name and password.

Two categories of report are made to the RDC, Continuous Records and Periodic Reports. In each case, there are several report types as detailed below.

The data transferred for each report type is stored in a different directory on the remote system using a new file for each day's information. The directory name is user configurable.

9.1 Local Data Centres

As the Signaling Gateway can act as an ftp server, the Signaling Gateway itself can act as a “Remote Data Centre”’ locally storing files and providing RDC services. Configuration in the manner is particularly useful as a backup when loss of communication with normal RDCs occur.

When the unit is configured to store continuous records and periodic reports locally, the user is responsible for the management of the file space used on the Signaling Gateway. If the file system becomes full, the Signaling Gateway is no longer able to back up files locally. A full file system has no other impact on the operation of the Signaling Gateway and the user is able to correct the problem by removing files from within the “siuftp” account.

9.2 Continuous Records

Continuous records provide the capability to transfer records to an RDC on a continuous basis in near real time. The minimum number of records collected prior to transfer and the maximum time interval before the transfer is attempted are configured by the user. This allows the user complete control over when records are transferred to the remote data centre, within system limits.

Continuous recording can be configured to support the occurrence and clearing of alarms to an RDC. The records are formatted as a comma separated variable (CSV) text file.

9.3 Periodic Reporting

Periodic reports can be configured to support the transfer to an RDC of data at user-defined intervals, typically allowing, for example, hourly reports of traffic measurements on a per SS7 link basis. The reports are formatted as a CSV file.

9.3.1 C7 Link Traffic Measurements

Measurements collected on a per CCS SS7 signaling basis can be transferred periodically to the RDC. These measurements can optionally be reset at the expiry of each interval.

9.3.2 PCM Traffic Measurements

Measurements collected on a per PCM basis can be transferred periodically to the RDC. These measurements can optionally be reset at the expiry of each interval.

9.3.3 SIGTRAN Link Traffic Measurements

Measurements collected on a per SIGTRAN link basis can be transferred periodically to the RDC. These measurements can optionally be reset at the expiry of each interval.

9.3.4 Ethernet Port Traffic Measurements

Measurements collected on performance data associated with Ethernet ports can be transferred periodically to the RDC. These measurements can optionally be reset at the expiry of each interval.

9.3.5 System Measurements

Measurements collected on system performance data can be transferred periodically to the RDC. These measurements can optionally be reset at the expiry of each interval.

9.4 RDC File Formats

This section specifies the file formats for records that are sent from the Signaling Gateway to a Remote Data Centre (RDC). As shown in the examples, the records are provided in CSV (Comma Separated Variable) text file format.

9.4.1 Alarm Record File Format

```
10,11,1,0,3,A,2001-01-01,00:00:35,,,Linkset fail
11,9,1,0,2,A, 2001-01-01,00:00:35,,,C7 link fail
2,44,1,3,2,C, 2001-01-01,00:00:28, 2001-01-01,00:00:36,CR send fail
11,9,1,0,2,C, 2001-01-01,00:00:35, 2001-01-01,00:00:36,C7 link fail
10,11,1,0,3,C, 2001-01-01,00:00:35, 2001-01-01,00:00:36,Linkset fail
```

Field	Title	Example	Range	Description
1	ALP	10	1 to 9999	Sequence reference number of an entry in the alarm log
2	CODE	11	1 to 999	Fault code of a system alarm
3	ID	1	0 to 9999	Identifier for alarm (usage depends on the alarm code)
4	DIAG	0	0 to 9999	Diagnostic of the alarm (usage depends on the alarm code)
5	CLA	3	0 to 3	Alarm class number
6	ACTIVE	C	A or C	Indication whether the alarm is Active or Cleared
7	DATE OCCURRED	1970-01-01	yyyy-mm-dd	Date the alarm occurred
8	TIME OCCURED	00:00:35	hh:mm:ss	Time the alarm occurred
9	DATE CLEARED	1970-01-01	yyyy-mm-dd	Date the alarm cleared
10	TIME CLEARED	00:00:36	hh:mm:ss	Time the alarm cleared
11	TITLE	Linkset fail	Up to 12 text characters	Title of the alarm

9.4.2 Ethernet Port Measurements File Format

```
2005-11-16,14:40:01,1,265,2016,0,0,0,0,0,0,119,1136,0,0,0,0,0,0,2077
2005-11-16,14:40:01,4,4664602,3448084,0,0,0,0,0,0,1183455,1809415,0,0,0,0,0,0,2077
2005-11-16,14:45:01,1,301,2368,0,0,0,0,0,0,145,1379,0,0,0,0,0,0,2377
2005-11-16,14:45:01,4,10220775,7212808,0,0,0,0,0,0,1270164,3077831,0,0,0,0,0,0,2377
```

Field	Field	Example	Range	Description
1	Date	2005-11-16	yyyy-mm-dd	Date when measurements collected
2	Time	14:40:01	hh:mm:ss	Time when measurements collected
3	ETH	1	1 to 4	Ethernet port number
4	RXKBYTE	10220775	0 to 4294967295	Number of kilobytes of data received (in kilobytes)
5	RXPKT	7212808	0 to 4294967295	Number of packets of data received
6	RXERR	0	0 to 4294967295	Number of receive errors detected
7	RXDROP	0	0 to 4294967295	Number of received packets dropped by the device driver
8	RXFIFO	0	0 to 4294967295	The number of FIFO buffer errors received
9	RXFRAME	0	0 to 4294967295	The number of packet framing errors received
10	RXCOMP	0	0 to 4294967295	The number of compressed packets received
11	RXMULT	0	0 to 4294967295	The number of multicast frames received
12	TXKBYTE	1270164	0 to 4294967295	Number of kilobytes of data transmitted (in kilobytes)
13	TXPKT	3077831	0 to 4294967295	Number of packets of data transmitted

9.4.3 PCM Measurements File Format

```
2001-12-31,13:07:25,600,1-1,5,50,20,500
2001-01-01,01:01:00,86400,1-2,90,1000,1000,1000
2001-11-22,19:07:38,3600,2-1,1,0,0,0
```

Field	Title	Example	Range	Description
1	Date	2001-12-31	yyyy-mm-dd	Date when measurements collected
2	Time	13:07:25	hh:mm:ss	Time when measurements collected
3	Period	600	0:4294967295	Duration of measurement period in seconds
4	PCM	3-1	x: 1 to 3 y: 1 to 4	PCM: x-y board id – port id.
5	Frame Slip counter	50	0 to 4294967295	Number of frame slips occurred.
6	Out of synchronism transitions	1000	0 to 4294967295	Number of out-sync transitions.
7	Errored Seconds counter	20	0 to 4294967295	Number of Errored Seconds occurred.
8	Severely Errored Seconds counter	500	0 to 4294967295	Number of Severely Errored Seconds.

9.4.4 SS7 Link Measurements File Format

```
2001-12-31,13:07:25,600,3,1000,56,513,502,20,6512,6502,10
2001-01-01,01:01:00,86400,2,5000,10,1000,1000,10,1000,1000,0
2001-11-22,19:07:38,3600,1,0,0,0,0,0,0,0,0
```

Field	Title	Example	Range	Description
1	Date	2001-12-31	yyyy-mm-dd	Date when measurements collected
2	Time	13:07:25	hh:mm:ss	Time when measurements collected
3	Period	600	0 to 4294967295	Duration of measurement period in seconds
4	SS7 Link	3	0 to 32	SS7 Link Number.
5	In Service	1000	0 to 4294967295	Duration of the link IN-SERVICE state.
6	Negative ACK	56	0 to 4294967295	Number of negative acknowledgement received. **NOTE:** Not applicable for M2PA SS7 links and is set to 0. See SIGTRAN Link measurements.
7	Octects Transmitted	513	0 to 4294967295	Number of octetcs transmitted.
8	Octects Received	502	0 to 4294967295	Number of octetcs received.
9	Octets Retransmitted	20	0 to 4294967295	Number of octetcs retransmitted. **NOTE:** Not applicable for M2PA SS7 links and is set to 0. See SIGTRAN Link measurements.
10	MSU Transmitted	6512	0 to 4294967295	Number of MSU transmitted.
11	MSU Received	6502	0 to 4294967295	Number of MSU received.
12	Congestion Counter	10	0 to 4294967295	Number of congestion events occurred.

9.4.5 SIGTRAN Link Measurements File Format

```
2001-12-31,13:07:25,600,2,886,888,5,0,0
2001-01-01,01:01:00,86400,5,5000,6000,1000,1000,65
2001-11-22,19:07:38,3600,1,0,0,0,0,0
```

Field	Title	Example	Range	Description
1	Date	2001-12-31	yyyy-mm-dd	Date when measurements collected
2	Time	13:07:25	hh:mm:ss	Time when measurements collected
3	Period	600	0 to 4294967295	Duration of measurement period in seconds
4	SIGTRAN Link	2	0 to 32	SIGTRAN Link Number.
5	Chunks Received	886	0 to 4294967295	Number of chunks received in the link.
6	Chunks Transmitted	888	0 to 4294967295	Number of chunks transmitted in the link.
7	Chunks Retransmitted	5	0 to 4294967295	Number of chunks retransmitted in the link.
8	Number of times out of service.	0	0 to 4294967295	Duration in abort and shutdown states.
9	Out of service duration.	0	0 to 4294967295	Duration of the link out of service since last reset.

9.4.6 System Measurements File Format

```
2005-11-16,14:40:01,0,231,155,8462
2005-11-16,14:45:01,0,368,159,8762
2005-11-16,14:50:01,0,380,164,9062
```

Field	Field	Example	Range	Description
1	Date	2005-11-16	yyyy-mm-dd	Date when measurements collected
2	Time	14:40:01	hh:mm:ss	Time when measurements collected
3	NOVLD	0	0 to 65535	The number of periods of congestion (overload) during the measurement period
4	MAXLOAD	380 (3.8%)	0 to 10000	Maximum load average measurement taken over 1 minute (based on the UNIX load average) multiplied by 100
5	LOADAVG	164 (1.64%)	0 to 10000	The average load on the system (based on the UNIX load average) measurement taken over the measurement period multiplied by 100
6	PERIOD	9062	0 to 4294967295	Duration of measurement period in seconds

9.5 RDC Configuration and Usage

This section provides a guide to the configuration of the Signaling Gateway for RDC operation, the text demonstrates by example, the man machine language (MML) commands and parameters required to invoke those services that transfer data to and from the RDC.

9.5.1 RDC Initialization

Initialize the RDC using the CNRDI command:

```
CNRDI:RDC=1,IPADDR=123.123.123.12,USER=ANONYMOUS,PASSWORD=ANONYMOUS,     LABEL=MYWORKSTN;
```

Unblock the RDC using the MNBLE command:

```
MNBLE:RDC=1;
```

Check the status of the RDC with the STRDP command:

```
STRDP;
```

9.5.2 Continuous Records

Continuous records, once created, are automatically transferred to the hard drive of the RDC. The user can configure the transfer interval ranging from 30 seconds to 24 hours. A different directory should be specified for each record type.

A file is created on the RDC during the first transfer for each record type during any 24 hour period beginning at midnight. Filenames are unique, identifying the date of transfer in the form YYYYMMDD.

Alarm Data

As alarms are generated, they are stored in the alarm logs on the converter. A record of these alarms can also be transferred to an RDC.

The following examples describe how a continuous record of type ALARM is initialized:

```
RDCRI:RECORD=3,CRTYPE=ALARM,PERIOD=00:30:00,MINREC=100,RDC1=1,
       LABEL=ALARMS;
```

The RDCRI command creates record number 3 that is of type ALARM. The contents of the record is transferred to the RDC when either the period or minrec, (minimum number of records), conditions are met.

RDC number 1 is the primary RDC; no secondary RDC has been identified. Records are transferred to the ALARMS directory on the RDC.

9.5.3 Periodic Reports

Periodic reports, once created, are periodically transferred to the RDC. The user can configure the transfer interval ranging from five minutes to 24 hours. Each report type should be collected in a different directory.

A file is created on the RDC during the first transfer for each report type during any 24 hour period beginning at midnight. Filenames are unique, identifying the date of transfer in the form YYYYMMDD.

Periodic report data can optionally be reset, (all values to zero), following each file transfer.

SS7 Signaling Link Traffic Measurements

Traffic measurement data can be generated for each SS7 signaling link.

The following examples describe how a periodic report is first created before SS7 Links (C7LINK) are selected as the collection points:

```
RDPRI:REPORT=1,PRTYPE=MSC7,PERIOD=01:00:00,RDC1=4,
       RESET=Y,LABEL=C7LINK;
```

The RDPRI command creates report number 1 that is of type MSC7. The RDPRI command creates report number 1 that is of type MSC7. The contents of the report is transferred to the RDC once each period.

RDC number 4 is the primary RDC; no secondary RDC is identified in the example. Reports are transferred to the C7LINK directory on the RDC. Because the RESET parameter has been set to ‘Y’, data for each circuit group associated with this report is reset following each file transfer.

Once the periodic report has been initialized, existing SS7 links can be dynamically associated with it using the RDPDI command or removed with the RDPDE command, for example:

```
RDPDI:REPORT=1,C7LINK=2&3;
RDPDE:REPORT=1,C7LINK=3;
```

The RDPDI command identifies SS7 links 2 and 3 as collection points for report 1. The RDPDE command removes SS7 link 3 from the report.

PCM Traffic Measurements

Periodic reports conveying PCM performance data can be configured using the RDPRI command. PCMs are associated with the report using the RDPDI command. PCMs can be removed from the report using the RDPDE command.

The PRTYPE parameter should be **MSPCM**.

SIGTRAN Link Traffic Measurements

Periodic reports conveying SIGTRAN link performance data can be configured using the RDPRI command. SIGTRAN Links (SNLINK) are associated with the report using the RDPDI command. SIGTRAN Links can be removed from the report using the RDPDE command.

The PRTYPE parameter should be **MSSL**.

Ethernet Port Traffic Measurements

Periodic reports conveying Ethernet performance data can be configured using the RDPRI command. ETH ports are associated with the report using the RDPDI command. ETH ports can be removed from the report using the RDPDE command.

The PRTYPE parameter should be **MSEP**.

System Measurements

Periodic reports conveying system performance data can be configured using the RDPRI command. There are no associated data types for use with this command.

The PRTYPE parameter should be **MSSY**.

9.5.4 Software Update

See Section 4.11.1, “Software Update from a Remote Data Centre” on page 24 for example MML that upgrades the Signaling Gateway software from an RDC.

9.5.5 Configuration Backup

See Section 4.12.1, “Configuration Backup to Remote Data Centre” on page 25 for example MML that upgrades the Signaling Gateway configuration from an RDC.

9.5.6 Configuration Update

See Section 4.13.1, “Configuration Update from a Remote Data Centre” on page 26 for example MML that upgrades the Signaling Gateway configuration from an RDC.

9.5.7 Software Option Installation

See Section 4.14.3, “License Update from Remote Data Centre” on page 28 for example MML that installs software options onto the Signaling Gateway from an RDC.

Chapter 10: SS7G2x SNMP MIB

The Signaling Gateway supports an SNMP version 1 managed agent to allow a remote management platform to interrogate the current alarm status of the Signaling gateway. Variables are supported from the MIB II system branch and from an enterprise MIB. The MIB provides read-only access to all variables.

The MIB II system branch provides basic information about managed node, that is, the Signaling Gateway. The Enterprise-specific branch of the MIB provides information as to the number of outstanding alarms, grouped by Category and Class (see Chapter 8, “Alarm Fault Code Listing”).

SNMP support can be activated by setting the SNMP parameter to Y using the CNSYS command as follows:

```
    CNSYS:SNMP=Y;
```

Then restart the system using:

```
MNRSI;
```

The user should then use their SNMP manager to communicate with Signaling Gateway using SNMP UDP port 161.

The content of the MIB is as follows:

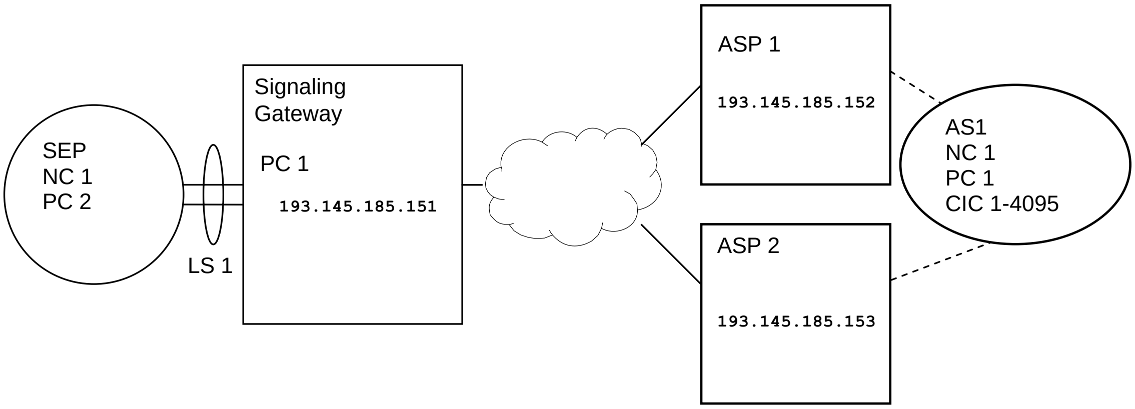
```
-- --------------------------------------------------------------------- --
-- --------------------------------------------------------------------- --
--                                                                          --
--                          The DataKinetics 4032 MIB                       --
--                                                                          --
-- --------------------------------------------------------------------- --
-- --------------------------------------------------------------------- --
--
--  Management Information Base for SNMP Network Management on DataKinetics
--  products.
--
-- Copyright (C) 1999-2007 Dialogic Corporation. All Rights Reserved.
--
--   The information in this document is subject to change without notice.
--
--   Enterprise number is 4032.
--
-- ------  ----------  ---- ------------------------------------------- --
-- Issue      Date      By    Changes                                   --
-- ------  ----------  ---- ------------------------------------------- --
-- 2          08-Jul-02 GNK - First published release
-- ------  ----------  ---- ------------------------------------------- --

DK-GLOBAL-REG DEFINITIONS ::= BEGIN

    IMPORTS
        enterprises             FROM RFC1155-SMI
        OBJECT-TYPE             FROM RFC1155-SMI;
--
-- The DataKinetics enterprise node
--
    datakinetics           OBJECT IDENTIFIER ::= { enterprises 4032 }

-- ------------------------------------------------------------------------
-- The MIB version stands alone at the top level
--
    dkMibVer OBJECT-TYPE
       SYNTAX  INTEGER
       ACCESS  read-only
       STATUS  mandatory
       DESCRIPTION
           "The current version of the MIB running on the agent. Currently
            the following values are recognised

            0 - Pre-release
            1 - Pre-release
            2 - First published release"
       ::= { datakinetics 1 }

-- ------------------------------------------------------------------------
-- ------------------------------------------------------------------------
-- Top level nodes within DK4032 MIB.
--
    dkSysInfo              OBJECT IDENTIFIER ::= { datakinetics 2 }

-- ------------------------------------------------------------------------
-- ------------------------------------------------------------------------
-- The system information branch
--

    dkSysAlarms          OBJECT IDENTIFIER ::= { dkSysInfo 4 }

-- ------------------------------------------------------------------------
-- The Alarms branch
--
    dkAlrmCategory          OBJECT IDENTIFIER ::= { dkSysAlarms 1 }

    dkAlrmPcm OBJECT-TYPE
       SYNTAX  INTEGER
       ACCESS  read-only
       STATUS  mandatory
       DESCRIPTION
           "The number of active PCM alarms"
       ::= { dkAlrmCategory 1 }

    dkAlrmSig OBJECT-TYPE
       SYNTAX  INTEGER
       ACCESS  read-only
       STATUS  mandatory
       DESCRIPTION
           "The number of active signaling alarms"
       ::= { dkAlrmCategory 2 }

    dkAlrmSys OBJECT-TYPE
       SYNTAX  INTEGER
       ACCESS  read-only
       STATUS  mandatory
       DESCRIPTION
           "The number of active system alarms"
       ::= { dkAlrmCategory 3 }

    dkAlrmClass             OBJECT IDENTIFIER ::= { dkSysAlarms 2 }

    dkClass1 OBJECT-TYPE
       SYNTAX  INTEGER
       ACCESS  read-only
       STATUS  mandatory
       DESCRIPTION
           "The number of active Class 1 alarms"
       ::= { dkAlrmClass 1 }

    dkClass2 OBJECT-TYPE
       SYNTAX  INTEGER
       ACCESS  read-only
       STATUS  mandatory
       DESCRIPTION
           "The number of active Class 2 alarms"
       ::= { dkAlrmClass 2 }

    dkClass3 OBJECT-TYPE
       SYNTAX  INTEGER
       ACCESS  read-only
       STATUS  mandatory
       DESCRIPTION
           "The number of active Class 3 alarms"
       ::= { dkAlrmClass 3 }

END

-- ------------------------------------------------------------------------
-- ------------------------------------------------------------------------
```

Chapter 11: Worked Configuration Examples

11.1 Backhaul Configuration

The following is an example of a Signaling Gateway working in a “backhaul” configuration. The Signaling Gateway is connected to a single Signaling End Point (SEP) on the TDM side. On the IP side there is a single Application Server (AS) that processes circuit-related messages. The AS exists on two ASPs for resilience. On the SS7 side, boards 2 and 3 are used to terminate two SS7 E1 PCMs. Each PCM carries 1 timeslot with SS7 signaling. The Point Code of the gateway equipment is 1, which is the same as that of the application server.

Figure 12. Example Back-Haul Configuration



The complete set of commands required to configure the entire system is as follows:

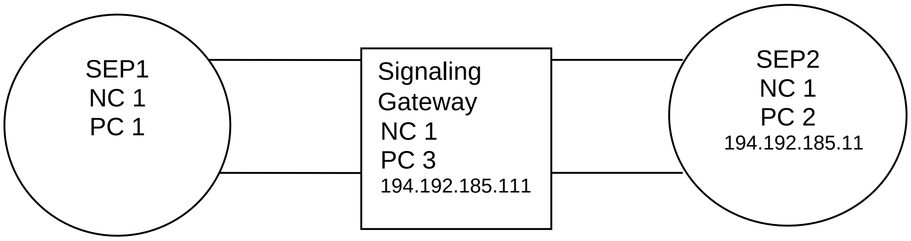
```
CNSYS:SYSID=THISSITE,IPADDR=193.145.185.151;
MNRSI;
CNBOI:BPOS=2,BRDTYPE=SPCI2S-4-2,SIGTYPE=SS7;
CNBOI:BPOS=3,BRDTYPE=SPCI2S-4-2,SIGTYPE=SS7;
CNPCI:PCM=2-3,PCMTYPE=E1,SYNCPRI=1;
CNPCI:PCM=3-3,PCMTYPE=E1,SYNCPRI=1;
C7LSI:LS=1,OPC=1,DPC=2,LSSIZE=2,SS7MD=ITU14,NC=1,NI=2;
C7SLI:C7LINK=1,EQU=2-1,TS=2-3-16,LS=1,SLC=0;
C7SLI:C7LINK=2,EQU=3-1,TS=3-3-16,LS=1,SLC=1;
C7RTI:C7RT=1,NC=1,DPC=2,LS1=1;
SNSLI:SNLINK=1,SNTYPE=SGM3UA,END=S,SS7MD=ITU14,NC=1,
      IPADDR=193.145.185.152,LABEL=ASP1;
SNSLI:SNLINK=2,SNTYPE=SGM3UA,END=S,SS7MD=ITU14,NC=1,
       IPADDR=193.145.185.153,LABEL=ASP2;
SNAPI:AS=1,NC=1,DPC=1,RC=1,LABEL=AS1;
SNALI:AS=1,SEQ=1,SNLINK=1;
SNALI:AS=1,SEQ=2,SNLINK=2;
SGDPI:DEST=1,AS=1,RTPRI=NONE,LABEL=AS1;
SGDPI:DEST=2,RTPRI=MTP,LABEL=TDM_SEP;
SGRKI:RKI=1,RKTAB=1,NC=1,DPC=1,BCIC=1,RANGE=4095,DEST=1;
SGRKI:RKI=2,RKTAB=1,NC=1,DPC=2,DEST=2;
SGIRI:IR=1,RKTAB=1,NC=1,DOMAIN=MTP;
SGIRI:IR=2,RKTAB=1,NC=1,DOMAIN=IP;
MNBLE:BPOS=2&&3;
MNBLE:SNLINK=1&&2;
MNBLE:C7LINK=1&&2;
MNBLE:AS=1;
```

11.2 M2PA Longhaul Configuration

The following is an example of a Signaling Gateway offering the longhaul of SS7 signalling over M2PA. The Signaling Gateway is connected to a Signaling End Point (SEP) on the TDM side and an SEP on the IP side. Each SEP treats the Signaling Gateway as an STP to reach its destination SEP. On the TDM side, board 1 is used to terminate two SS7 E1 PCMs with clock being taken from SEP 1. Each PCM carries 1 timeslot with SS7 signaling to SEP 1. On the SIGTRAN IP side, two M2PA associations are used to convey two SS7 signaling links to SEP 2. The Point Code of the gateway equipment is 3; the SEPs are Point Codes 1 and 2 respectively.

Note: Potentially routing keys are not required in this scenario, the user could simply configure a the incoming route to go directly to the TDM destination. Routing keys are present since they allow the Signaling Gateway to validate the DPC in the received data message.

Figure 13. M2PA Longhaul Configuration

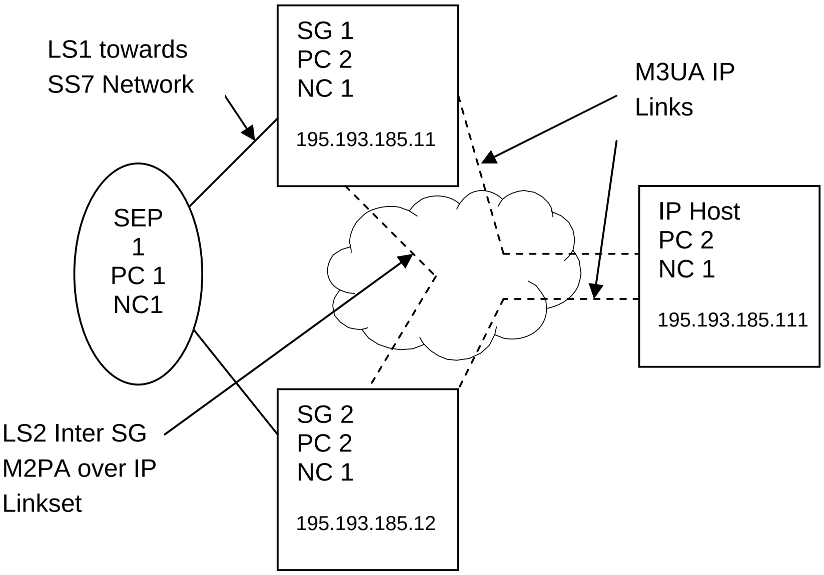


The complete set of commands required to configure the entire system is as follows:

```
CNSYS:SYSID=SGW1,IPADDR=194.192.185.111;
MNRSI;
CNBOI:BPOS=1,BRDTYPE=SPCI2S-4-2,SIGTYPE=SS7;
CNBOI:BPOS=2,BRDTYPE=SPCI2S-4-2,SIGTYPE=SS7;
CNPCI:PCM=1-3,PCMTYPE=E1,SYNCPRI=1;
CNPCI:PCM=2-3,PCMTYPE=E1,SYNCPRI=1;
SNSLI:SNLINK=1,SNTYPE=M2PA,END=C,IPADDR=194.192.185.11,      HPORT=3565,PPORT=3565,LABEL=SEP2-1;
SNSLI:SNLINK=2,SNTYPE=M2PA,END=C,IPADDR=194.192.185.11, HPORT=3566,PPORT=3566,LABEL=SEP2-2;
C7LSI:LS=1,OPC=3,DPC=1,LSSIZE=2,SS7MD=ITU14,NC=1,NI=2;
C7LSI:LS=2,OPC=3,DPC=2,LSSIZE=2,SS7MD=ITU14,NC=1,NI=2;
C7SLI:C7LINK=1,EQU=1-1,TS=1-3-16,LS=1,SLC=0;
C7SLI:C7LINK=2,EQU=2-1,TS=2-3-16,LS=1,SLC=1;
C7SLI:C7LINK=3,SNLINK=1,LS=2,SLC=0;
C7SLI:C7LINK=4,SNLINK=2,LS=2,SLC=1;
C7RTI:C7RT=1,NC=1,DPC=1,LS1=1;
C7RTI:C7RT=2,NC=1,DPC=2,LS1=2;
SGDPI:DEST=1,RTPRI=MTP,LABEL=SEP1-2;
SGRKI:RKI=1,RKTAB=1,NC=1,DPC=1,DEST=1;
SGRKI:RKI=2,RKTAB=1,NC=1,DPC=2,DEST=1;
SGIRI:IR=1,NC=1,RKTAB=1;
MNBLE:BPOS=1&2;
MNBLE:SNLINK=1&2;
MNBLE:C7LINK=1&&4;
```

11.3 Dual Resilient Configuration

Figure 14. Example Dual Resilient Configuration



The following configuration commands are for SG1 and SG2, where SG1 and SG2 are in DUAL operation and SG1, SG2 and the IP host are acting as a single Point Code. Note the configuration of LS2 between the two SGs and the use of this link set for routes to the SS7 network.

> ***Note:*** While this example shows a linkset with M2PA SS7 links over IP between the two Signaling Gateways, the linkset could equally contain SS7 links utilizing timeslots on a PCM between the two Signaling Gateways.

11.3.1 SG 1 Configuration

```
CNSYS:SYSID=SS7G2x 1,IPADDR=194.192.185.11;
CNBOI:BPOS=1,BRDTYPE=SPCI2S-4-2,SIGTYPE=SS7;
CNPCI:PCM=1-3,PCMTYPE=E1,SYNCPRI=1;
C7LSI:LS=1,OPC=2,DPC=1,LSSIZE=2,SS7MD=ITU14,NC=1,NI=2;
C7LSI:LS=2,OPC=2,DPC=2,LSSIZE=2,SS7MD=ITU14,NC=1,NI=2;
C7RTI:C7RT=1,DPC=1,LS1=1,LS2=2;
C7RTI:C7RT=2,DPC=2,LS1=2;
SNSLI:SNLINK=1,SNTYPE=M2PA,END=C,IPADDR=194.192.185.12,
LABEL=INTER-SG;
C7SLI:C7LINK=1,EQU=1-1,TS=1-3-16,LS=1,SLC=0;
C7SLI:C7LINK=2,SNLINK=1,LS=2,SLC=0;

SNSLI:SNLINK=2,SNTYPE=SGM3UA,END=S,SS7MD=ITU14,NC=1,
IPADDR=194.192.185.111,LABEL=IP Host;
SNAPI:AS=1,NC=1,DPC=2,RC=1,LABEL=IP Host;
SNALI:AS=1,SEQ=1,SNLINK=2;
SGDPI:DEST=1,AS=1,LABEL=IP Host;
SGDPI:DEST=2,RTPRI=MTP,LABEL=SS7 Net;
SGRKI:RKI=1,RKTAB=1,NC=1,DPC=2,DEST=1;
SGRKI:RKI=2,RKTAB=1,NC=1,DPC=1,DEST=2;
SGIRI:IR=1,RKTAB=1,NC=1;
MNBLE:BPOS=1;
MNBLE:SNLINK=1&2;
MNBLE:C7LINK=1&&2;
MNBLE:AS=1;
```

11.3.2 SG 2 Configuration

```
CNSYS:SYSID=SS7G2x 2,IPADDR=194.192.185.12;
CNBOI:BPOS=1,BRDTYPE=SPCI2S-4-2,SIGTYPE=SS7;
CNPCI:PCM=1-3,PCMTYPE=E1,SYNCPRI=1;
C7LSI:LS=1,OPC=2,DPC=1,LSSIZE=2,SS7MD=ITU14,NC=1,NI=2;
C7LSI:LS=2,OPC=2,DPC=2,LSSIZE=2,SS7MD=ITU14,NC=1,NI=2;
C7RTI:C7RT=1,DPC=1,LS1=1,LS2=2;
C7RTI:C7RT=2,DPC=2,LS1=2;
SNSLI:SNLINK=1,SNTYPE=M2PA,END=C,IPADDR=194.192.185.11,
LABEL=INTER-SG;
C7SLI:C7LINK=1,EQU=1-1,TS=1-3-16,LS=1,SLC=0;
C7SLI:C7LINK=2,SNLINK=1,LS=2,SLC=0;
SNSLI:SNLINK=2,SNTYPE=SGM3UA,END=S,SS7MD=ITU14,NC=1,
IPADDR=194.192.185.111,LABEL=IP Host;
SNAPI:AS=1,NC=1,DPC=2,RC=1,LABEL=IP Host;
SNALI:AS=1,SEQ=1,SNLINK=2;
SGDPI:DEST=1,AS=1,LABEL=IP Host;
SGDPI:DEST=2,RTPRI=MTP,LABEL=SS7 Net;
SGRKI:RKI=1,RKTAB=1,NC=1,DPC=2,DEST=1;
SGRKI:RKI=2,RKTAB=1,NC=1,DPC=1,DEST=2;
SGIRI:IR=1,RKTAB=1,NC=1;
MNBLE:BPOS=1;
MNBLE:SNLINK=1&2;
MNBLE:C7LINK=1&&2;
MNBLE:AS=1;
```

Chapter 12: Command Summary

Alarm Commands

- ALCLS - Alarm Class Set
- ALCLP - Alarm Class Print
- ALFCP - Alarm Fault Code Print
- ALLIP - Alarm List Print
- ALLOP - Alarm Log Print
- ALREI - Alarm Reset Initiate
- ALTEI - Alarm Test Initiate
- ALTEE - Alarm Test End

Configuration Commands

- CNBOI - Configuration Board Initiate
- CNBOE - Configuration Board End
- CNBOP - Configuration Board Print
- CNBUI - Configuration Back Up Initiate
- CNMOI - Configuration Monitor Initiate
- CNMOE - Configuration Monitor End
- CNMOP - Configuration Monitor Print
- CNPCI - Configuration PCM Initiate
- CNPCC - Configuration PCM Change
- CNPCE - Configuration PCM End
- CNPCP - Configuration PCM Print
- CNRDI - Configuration Remote Data Centre Initiate
- CNRDC - Configuration Remote Data Centre Change
- CNRDE - Configuration Remote Data Centre End
- CNRDP - Configuration Remote Data Centre Print
- CNSWP - Configuration Software Print
- CNSYS - Configuration System Set
- CNSYP - Configuration System Print
- CNTDS - Configuration Time and Date Set
- CNTDP - Configuration Time And Date Print
- CNTOS - Configuration Timeout Value Set
- CNTOP - Configuration Timeout Value Print
- CNTSP - Configuration Timeslot Print
- CNUPI - Configuration Update Initiate
- CNXCI - Configuration Cross Connect Initiate
- CNXCE - Configuration Cross Connect End
- CNXCP - Configuration Cross Connect Print

CCS SS7 Signaling Commands

- C7LSI - CCS SS7 Link Set Initiate
- C7LSC - CCS SS7 Link Set Change
- C7LSE - CCS SS7 Link Set End
- C7LSP - CCS SS7 Link Set Print

- C7RTI - CCS SS7 Route Initiate
- C7RTC - CCS SS7 Route Change
- C7RTE - CCS SS7 Route End
- C7RTP - CCS SS7 Route Print
- C7SLI - CCS SS7 Signaling Link Initiate
- C7SLC - CCS SS7 Signaling Link Change
- C7SLE - CCS SS7 Signaling Link End
- C7SLP - CCS SS7 Signaling Link Print

IP Commands

- IPEPS - Set Ethernet Port Speed
- IPEPP - Display Ethernet Port Speed
- IPGWI - Internet Protocol Gateway Initiate
- IPGWE - Internet Protocol Gateway End
- IPGWP - Internet Protocol Gateway Print

MML Commands

- MMLOI - MML Log Off Initiate
- MMLOP - MML Log Off Print
- MMLOS - MML Log Off Set
- MMPTC - MML Port Change
- MMPTP - MML Port Print

Maintenance Commands

- MNBLI - Maintenance Blocking Initiate
- MNBLE - Maintenance Blocking End
- MNINI - Maintenance Inhibit Initiate
- MNINE - Maintenance Inhibit End
- MNRSI - Maintenance Restart System Initiate

Measurement Commands

- MSC7P - Measurements SS7 Print
- MSPCP - Measurements PCM Print
- MSSLP - Measurements SIGTRAN Link Print
- MSSYP - Measurements System Print

Remote Data Centre Commands

- RDCRI - Remote Data Centre Continuous Record Initiate
- RDCRC - Remote Data Centre Continuous Record Change
- RDCRE - Remote Data Centre Continuous Record End
- RDCRP - Remote Data Centre Continuous Record Print
- RDPDI - Remote Data Centre Periodic Data Initiate
- RDPDE - Remote Data Centre Periodic Data End
- RDPDP - Remote Data Centre Periodic Data Print
- RDPRI - Remote Data Centre Periodic Report Initiate
- RDPRC - Remote Data Centre Periodic Report Change
- RDPRE - Remote Data Centre Periodic Report End

- RDPRP - Remote Data Centre Periodic Report Print

Signaling Gateway Commands

- SGDPI - Signaling Gateway Destination Point Initiate
- SGDPC - Signaling Gateway Destination Point Change
- SGDPE - Signaling Gateway Destination Point End
- SGDPP - Signaling Gateway Destination Point Print
- SGIRI - Signaling Gateway Incoming Route Initiate
- SGIRC - Signaling Gateway Incoming Route Change
- SGIRE - Signaling Gateway Incoming Route End
- SGIRP - Signaling Gateway Incoming Route Print
- SGRKI - Signaling Gateway Routing Key Initiate
- SGRKE - Signaling Gateway Routing Key End
- SGRKP - Signaling Gateway Routing Key Print

SIGTRAN Commands

- SNALI - SIGTRAN Application Server List Initiate
- SNALE - SIGTRAN Application Server List End
- SNALP - SIGTRAN Application Server List Print
- SNAPI - SIGTRAN Application Server Initiate
- SNAPE - SIGTRAN Application Server End
- SNAPP - SIGTRAN Application Server Print
- SNNAI - SIGTRAN Network Appearance Initiate
- SNNAE - SIGTRAN Network Appearance End
- SNNAP - SIGTRAN Network Appearance Print
- SNSLI - SIGTRAN Signaling Link Initiate
- SNSLC - SIGTRAN Signaling Link Change
- SNSLE - SIGTRAN Signaling Link End
- SNSLP - SIGTRAN Signaling Link Print

Status Commands

- STALP - Status Alarm Print
- STAPP - Status Application Server Print
- STBOP - Status Board Print
- STCRP - Status C7 Route Print
- STC7P - Status C7 Link Print
- STEPP - Status Ethernet Port Print
- STIPP - Status IP Print
- STPCP - Status PCM Print
- STRDP - Status Remote Data Centre Print
- STSLP - Status SIGTRAN Link Print

Glossary

AS	Application Server. A logical entity serving a specific Routing Key. An example of an AS is a virtual switch element handling all call processing for a unique range of PSTN trunks, identified by an SS7 SIO/DPC/OPC/CIC_range. Another example is a virtual database element, handling all HLR transactions for a particular SS7 DPC/OPC/SCCP_SSN combination. The AS contains a set of one or more unique Application Server Processes (ASPs), of which one or more is normally actively processing traffic. Note that there is a 1:1 relationship between an AS and a Routing Key.
ASP	Application Server Process. A process instance of an Application Server (AS). An ASP serves as an active or backup process of an Application Server (for example, part of a distributed virtual switch or database). Examples of ASPs are processes (or process instances) of MGCs, IP SCPs or IP HLRs. An ASP contains an SCTP endpoint and may be configured to process signaling traffic within more than one Application Server.
AIS	Alarm Indication Signal
ANSI	American National Standards Institute
BER	Bit Error Rate
CCITT	Consultative Committee on International Telegraphy and Telephony
CCS	Common Channel Signaling
CIC	Circuit Identification Code
CPU	Central Processing Unit
DC	Direct Current
DSC	Digital Signaling Converter
DSR	Data Set Ready
DTE	Data Terminal Equipment
DTR	Data Terminal Ready
FTP	File Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU	International Telecommunication Union
LIU	Line Interface Unit
M2PA	MTP 2 Peer to Peer Adaptation Layer
M3UA	MTP3 User Adaptation Layer
MML	Man-Machine Interface Language
MTP	Message Transfer Part (of SS7 signaling)
PCM	Pulse Code Modulation
PSU	Power Supply Unit
RDC	Remote Data Centre
SCTP	Stream Control Transmission Protocol
SIGTRAN	Signaling Transport
SS7	Signaling System Number 7
SSH	Secure Shell
STP	Signaling Transfer Point

SEP	Signaling End Point
SNM	Signaling Network Management
TDM	Time-Division Multiplexing

Index