Carrier VoIP

Session Server Trunks Basics

NN10333-111

Document status: Standard
Document version: 04.02
Document date: 20 October 2006

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.

Contents

New in this Release

The following sections list what's new in Session Server Trunks Basics for (I)SN09U.

- Features
- "Other changes" (page 6)

Features

Session Server Fault Handling Enhancements (A00012735)

This activity extends the coverage of hardware faults handled by the Session Server Nortel Carrier Grade Linux (NGCL) Platform Manager software, thereby increasing platform reliability. This activity involves the detection and reporting of hardware faults.

For more information, see "Fault management" (page 20) and *Nortel Session Server Trunks Fault Management* (NN10332-911).

Support for SIP DID Trunks on Session Server (A00011533)

This feature provides Carrier Voice over IP networks with additional Internet Engineering Task Force (IETF) compliance and interoperability with the session initiation protocol (SIP) and SIP for telephones (SIP-T) standards. The enhancements improve interworking between CS 2000 switches and with other third-party SIP servers.

Support for SIP direct inward dialing (DID) trunk types on SST provides the following improvements:

- Preserves existing SIP-T functionality provided by virtual router distribution node (VRDN) in CS 2000
- Supports the mobile telephone exchange (MTX) DID trunk type on the Session Server
- Provides enhanced ANSI ISUP parameter mapping to SIP to support SIP interfacing to remote CS 2000 and third-party SIP servers.
- The Session Timer extension (RFC4028) enables SIP servers and endpoints to know if an endpoint is no longer in a session, such as in case of a crash, and to limit the duration of a session. An endpoint that

has the Session Timer extension activated sends periodic keep-alive messages to notify that it is active or to extend the duration of the session.

For more information, see "Configuring Remote SIP Servers" in *Nortel Session Server Trunks Configuration Management* (NN10338-511).

Mapping of prefix digits to in incoming DPT trunk group (168398)

This feature allows the CS2K-SST to process SIP to TDM calls with multiple trunk groups on the core from signaling on a single SIPLINK. This functionality allow the SST application to interpret the leading digits (digits prefixed on the called DN) and, based on these digits, select an incoming DPT trunk group in the CS 2000. These digits are mapped to a SIPLINK in the SST, and therefore a trunk group in the CS 2000 in the same manner as the mapping of an x-nortel-profile header.

For details, see *Nortel Session Server Trunks Configuration Management* (NN10338-511).

Other changes

There are no other changes in SST Basics for (I)SN09U.

Functional description

The Nortel Session Server Trunks (SST) is a call media and signaling interoperability component. The SST is made up of a high capacity, carrier grade hardware platform based on the Session Application Module-eXtreme Thin Server (SAM-XTS, used also for STORM IA) along with software consisting of a Nortel Carrier Grade Linux (NCGL) base and shared SIP-T layers. The component is deployed as two redundant hardware units housed in the SAM-F frame or SAM-CCF frame.

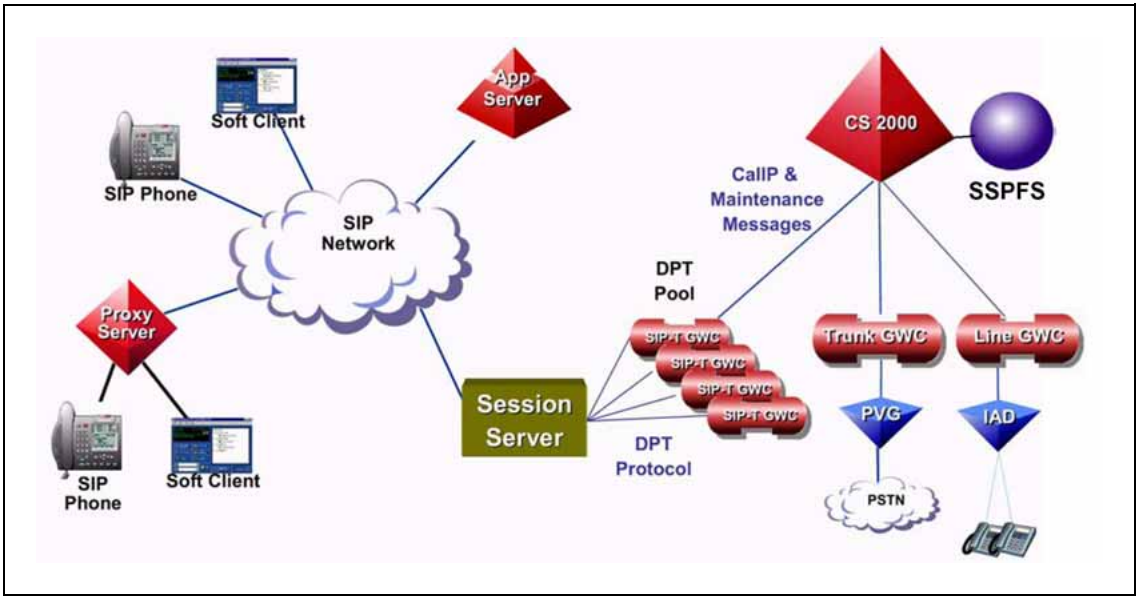
The primary application introduced on the SST platform is the SIP Gateway application which facilitates interoperability between the CS 2000 network and third-party SIP-based call servers and media application servers, such as Multimedia Communication Server (MCS). This capability enables SIP-based call servers to access the PSTN through the CS 2000 network and eliminates the need for a slower VRDN GWC for call routing.

SST supports interoperability for the following VoIP environments:

- Call Server-to-Call Server using SIP-T including CS 2000-Compact
- Full interoperability between MCS 5100 (Enterprise) and MCS 5200 (Carrier) and the CS 2000 for all SIP-T supported services and functionality supported for the MCS application server
- Open Standard Interop with Third-Party Call Servers, Proxy Servers and Application Servers
- Support for multi-vendor environments

The following diagram illustrates the role of the SST in the CS 2000 network of components.

Relationship of Session Server Trunks to other CS 2000 network components



The main components with respect to SIP and SIP-T call processing on the Call Server LAN are described briefly:

Node	Function
CS 2000	Contains the XA-Core call processing engine which connects to the IP network through the SIP-T dynamic packet trunks (DPT) gateway controllers (GWCs).
Trunk and Line GWCs	Function as the interface between the XA-Core and gateways such as the Media Gateway 7480/15000 (formerly PVG) or integrated access line devices (IADs)
SIPT GWCs	Sometimes referred to as a DPT GWC, functions as an interface between a DPT trunk GWC and the VRDN GWC by providing SIP call processing functions.
VRDN GWCs	Functions as a router to direct incoming/outgoing calls between SIP-T and line or trunk GWCs.
Server Platform Foundation Software (SPFS)	Acts as the general OAM&P platform for the CS 2000 Management Components and the Integrated Element Management System (IEMS). It provides web proxy services for web-based component managers, including those on the SST, the CS 2000 Session Server Trunks Manager and the CS 2000 NCGL Platform Manager.

Supported configurations

The following configurations are supported in (I)SN09U, using the SST in call server-to-call server communication:

- (I)SN09FF SST and (I)SN09FF SST

- (I)SN09FF SST and (I)SN08 SST

The following configurations are supported in (I)SN09U, using the SST in call server-to-application server communication:

- (I)SN09FF SST and MCS 5200 3.0
- (I)SN09FF SST and MCS 5200 4.0
- (I)SN09FF SST and (I)SN09FF SST
- (I)SN09FF SST and (I)SN08 SST

SST hardware platform

The SST chassis are deployed in a rack-mounted configuration house containing processing hardware, hard drives, Ethernet interface ports, and redundant power supplies. Two Ethernet interface ports are reserved for inter-SST communication for fault tolerance.

With two chassis working together to provide carrier-grade level fault tolerance, this hardware configuration provides the platform for the SIP Gateway application.

This hardware platform uses Network Equipment Building Standards (NEBS) Level 3 compliant hardware designed for telecommunications central offices or data centers, based on the Hewlett Packard™ cc3310 carrier-grade server.

Features of each hardware platform unit include:

- Dual 2.4 GHz Xeon processors
- 4-GB DDR memory
- Dual 73-GB hot-swappable disk drives
- CD-RW/DVD-R drive
- Dual hot-swappable power supplies
- Dual GbE interface network interface cards
- SAM-XTS platform, used with other Carrier VoIP components such as the STORM and Policy Controller, is based on the compact HP cc3310 carrier-grade server.

Configuring multiple SST nodes in the call server network

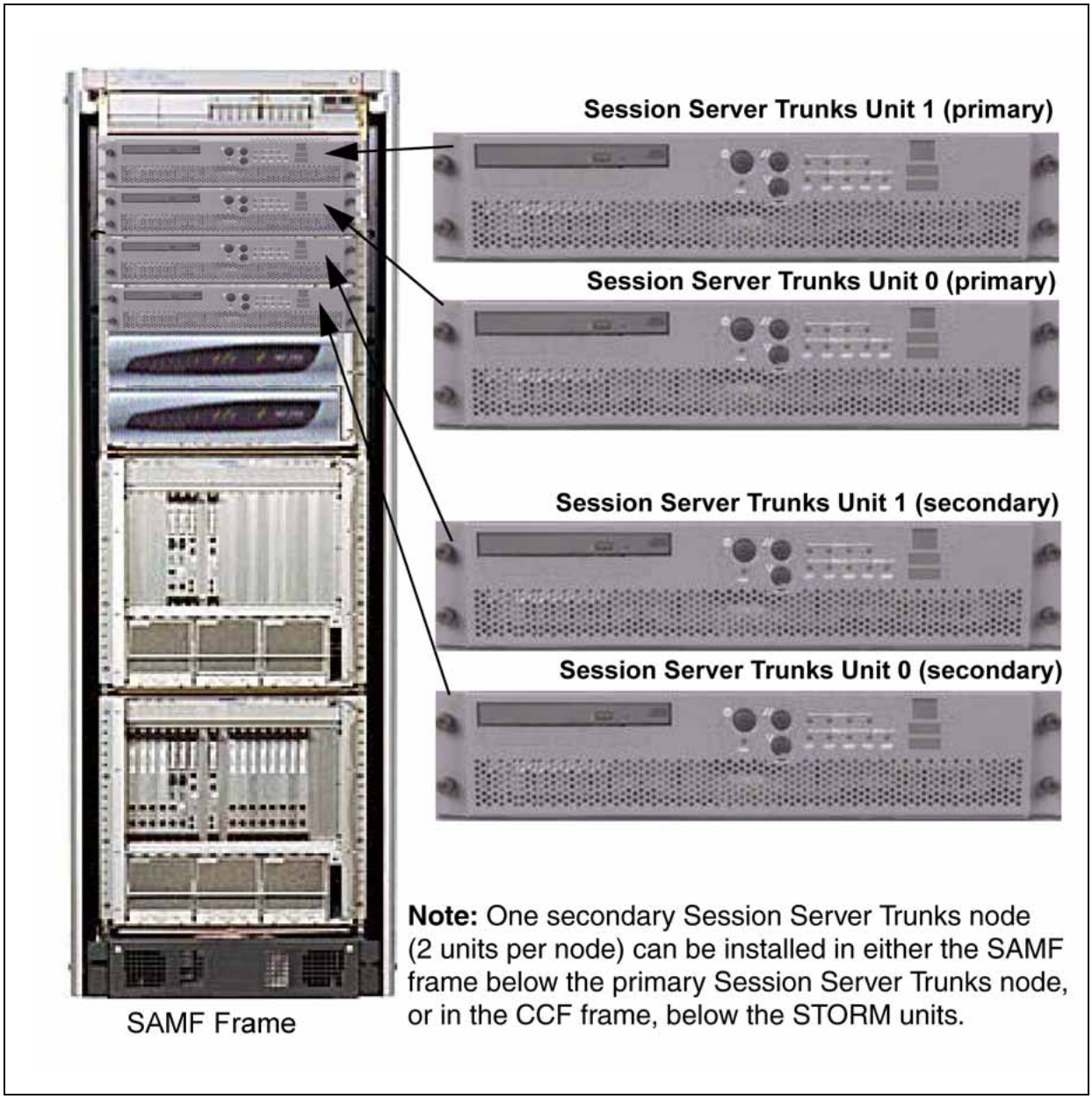
In (I)SN09U, one or more SST nodes are installed in the SAMF and Call Control (CCF) frames. On the SAMF frame (NTRX51HA), the primary SST node, made up of two hardware units, is mounted below the BIP power distribution unit. A secondary SST node comprised of two additional hardware units can be mounted below the primary node in the SAM-F frame. As an option, the secondary SST node can be mounted in the CCF frame

(NTRX51TA), below the STORM units. A maximum of two nodes, four units total, are allowed in a single CS 2000 call server network. Do not confuse SST units with Policy Controller or STORM units, which can appear identical.

Typically, each SST unit is labeled for identification to distinguish it from other units in the frame and to distinguish it from Policy Controller or STORM units. The naming identification may be similar to the hostname of the node, made during commissioning of the node.

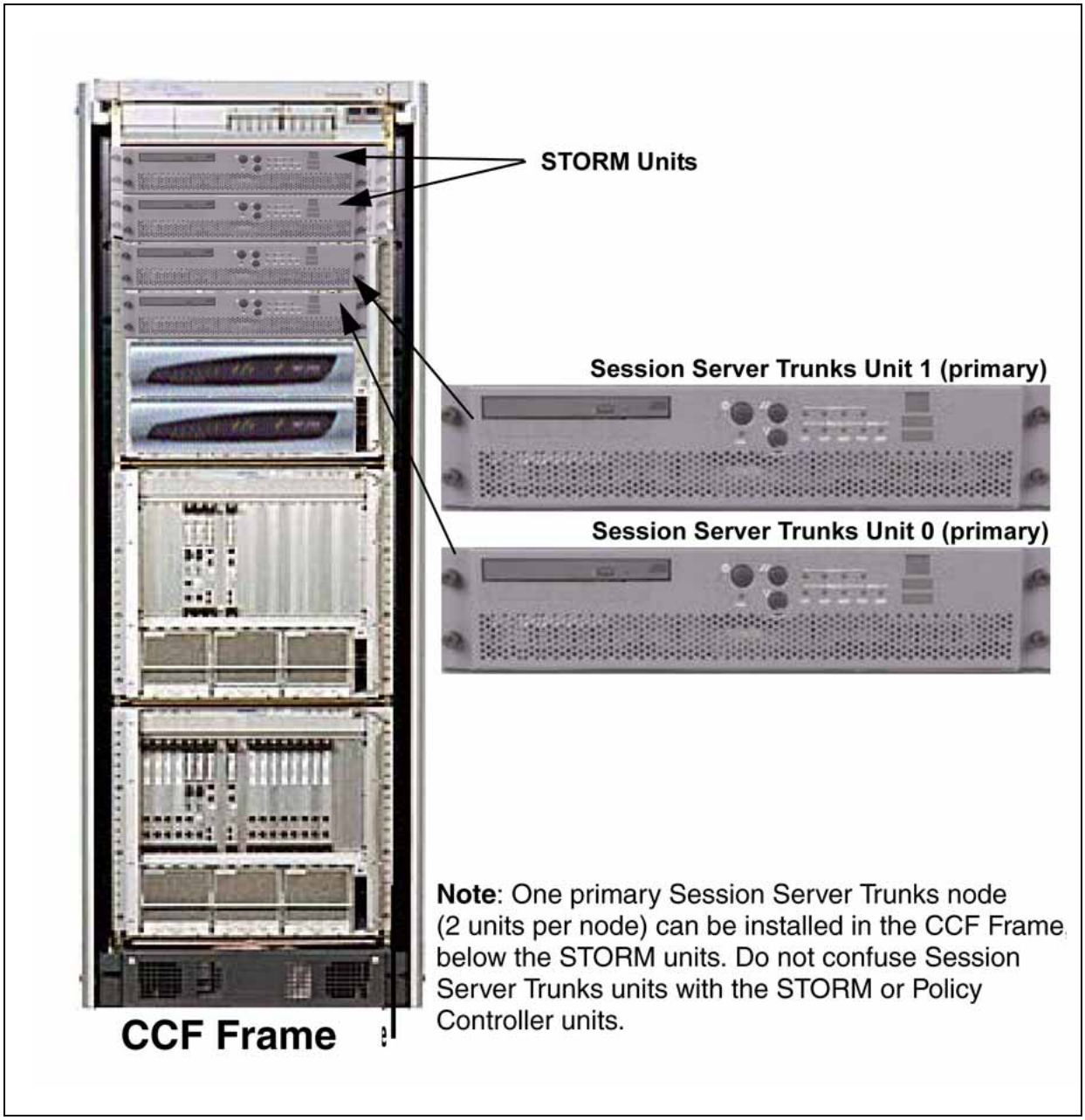
The following diagram shows the location of the primary and secondary SST hardware units in the SAM-F frame.

Identifying SST units in the SAMF frame (NTRX51HA)



The following diagram shows the location of the primary SST hardware units in the CCF frame.

Identifying SST primary units in the CCF frame (NTRX51TA)



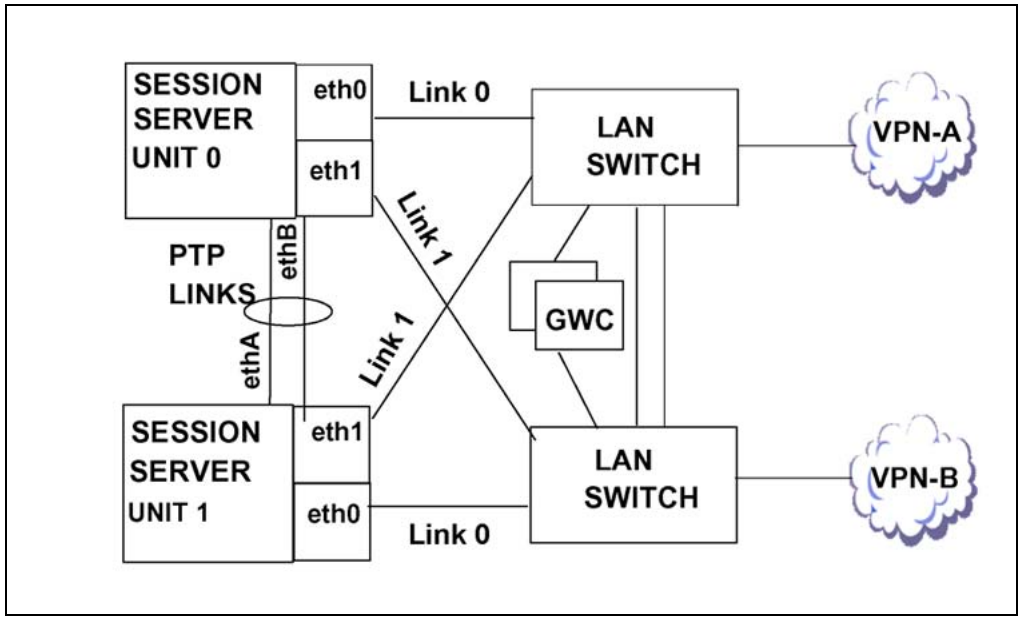
Network interfaces and connectivity

Each SST unit has two GbE Ethernet interfaces, configured as link 0 and link 1, to communicate with CS-LAN switch. In addition, two additional Ethernet interfaces interconnect the two hardware units in a Point-To-Point (PTP) link.

This configuration allows the SST to operate like the Gateway Controller in that it supports maintaining active calls over a Warm Switch of Activity (SWACT) from an active to a standby unit. SWACTs can be manually executed or may automatically execute when callp auditing processes determine that there is sufficient cause to SWACT units.

For more detailed information about managing Ethernet links for the SST, See *Session Server Trunks Security and Administration* (NN10346-611).

Link Configuration of the SST with the CS-LAN

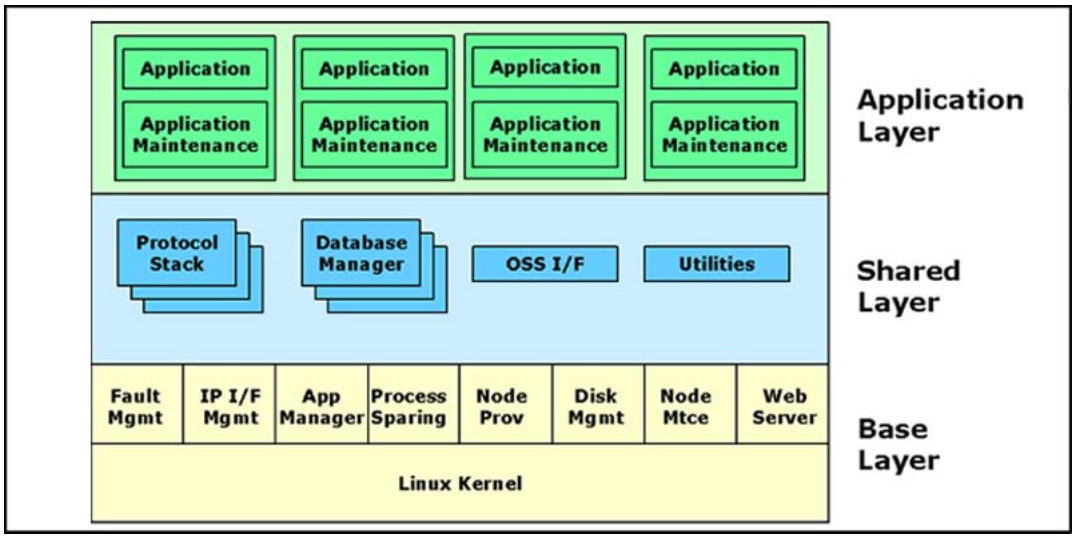


Software architecture

The SST software utilizes a layered architecture, which consists of the following:

- The base Nortel Carrier Grade Linux (NCGL) layer, which includes the Linux kernel along with a carrier-grade software platform that supports fault management, interface management, hardware management and application management
- A shared application layer which contains reusable components, such as the SIP protocol stack, used by higher level applications such as the SIP Gateway application
- An application layer, which includes a maintenance process for each application, which in turn manages the associated SIP gateway application processes.

SST Software Architecture

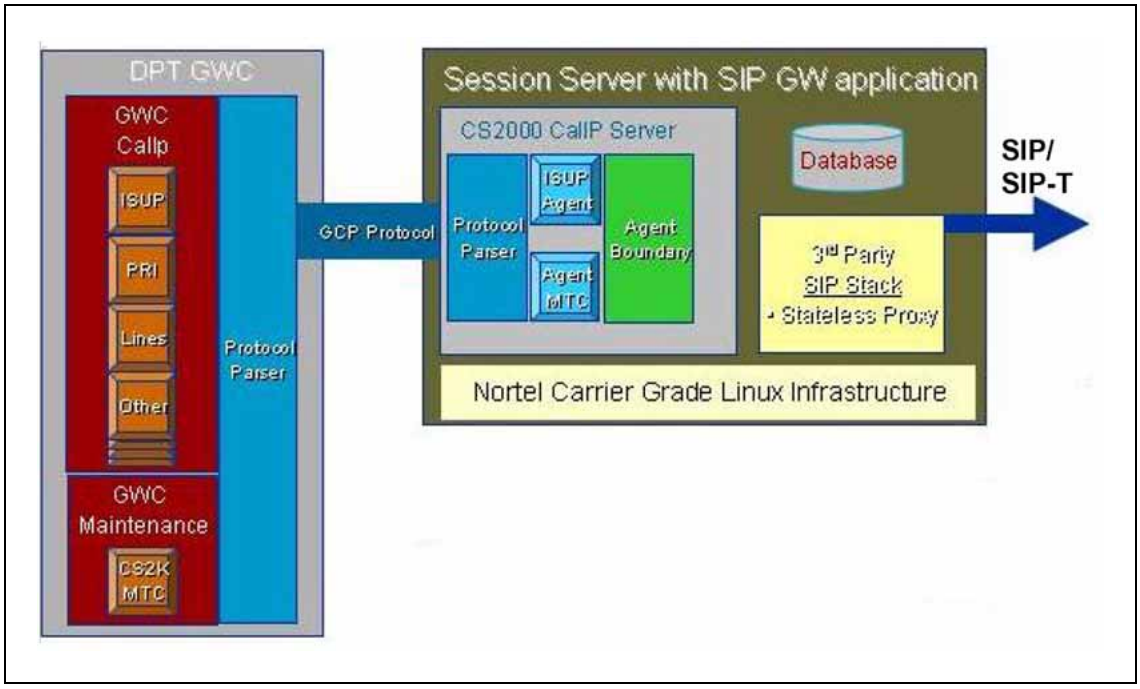


SIP Gateway application software

The SIP Gateway application (also referred to as the SIP application) is the application primarily responsible for call processing activities such as setting-up and tearing-down SIP calls, maintaining accessibility between SIP-T (DPT) GWCs (gateway controllers) and remote SIP servers.

The application runs on the SST platform and communicates indirectly with the CS 2000 through SIP-T GWCs. Using Generic Call Processing (GCP) protocol to interface with the GWCs, SST integrates DPT call processing, managed by the CS 2000 by providing a direct trunking interface between the TDM interface on the CS 2000 and a SIP domain that contains a SIP-based application server. It maps ISUP or PRI signaling to SIP signaling and SIP signaling to ISUP/PRI signaling.

SIP Gateway application interface protocols



SIP Application Maintenance, part of the application layer, is responsible for the following:

- initializing and managing SIP Application processes
- tracking the SIP Application maintenance state and callp states
- relaying provisioning changes to the SIP Application database from the CS 2000 SST Manager
- generating maintenance related logs and alarms

About CS 2000 SIP implementation

The Session Initiation Protocol (SIP), used by the SST is a protocol designed for multimedia communication. The current CS 2000 SIP implementation is a proprietary implementation of SIP for telephony (SIP-T) used to allow interoperation with third-party proxy servers and application servers, in compliance with the IETF SIP specifications.

Because SIP implementation is migrating to an Open Interop standard, the CS 2000 has evolved to implement a SIP Gateway to convert Open Interop SIP messaging into messages understandable by the CS 2000.

Client web browser requirements

For provisioning and maintaining the SST the following client web browsers are supported:

Windows 2000, Windows XP, or Office 2003 based PC

- Internet Explorer 6.0 SP1 and above
- Netscape 6.2.3 and 7.1+

Solaris 2.8 and 2.9-based Sun workstations

- Netscape 6.2.3
- Firefox/Mozilla 1.4+

For more information about supported browsers, see *Session Server Trunks Configuration Management* (NN10338-511).

Software ordering and delivery

See the Basics NTP applicable to your Carrier VoIP solution, for more information about software ordering and support options.

SST software loads

The SST uses a single load for North America and International markets and all supported IP solutions.

Maintenance release upgrades and patching

Patching and in-service maintenance release upgrades are supported for SST. For details, see *Nortel Carrier Voice over IP Upgrade and Patches* (NN10440-450).

For more information about release compatibility between SST and other Carrier VoIP software, consult your *Carrier Voice over IP Network Upgrade Overview* (NN10440-450).

Upgrading a CS 2000 network to support SST

Upgrading a CS 2000 network-based office to include the SST and migrating existing SIP-T traffic from the VRDN architecture to the SST is not covered in the SST NTPs. Procedures related to migration may be included in the NTPs for other reasons.

For initial installation and provisioning of a SST into an existing network, contact your Nortel service representative.

Operations, administration, maintenance and provisioning strategy

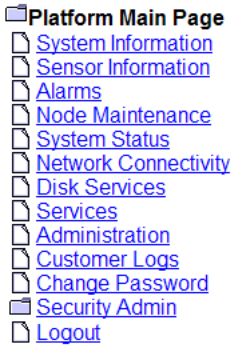
Since the SST is a component in the CS 2000 network, it uses operations, administration, maintenance and provisioning (OAM&P) functions for handling fault, configuration, accounting, performance and security (FCAPS) management activities in similar fashion to other components in the CS 2000 network.

Tools, utilities and user interfaces

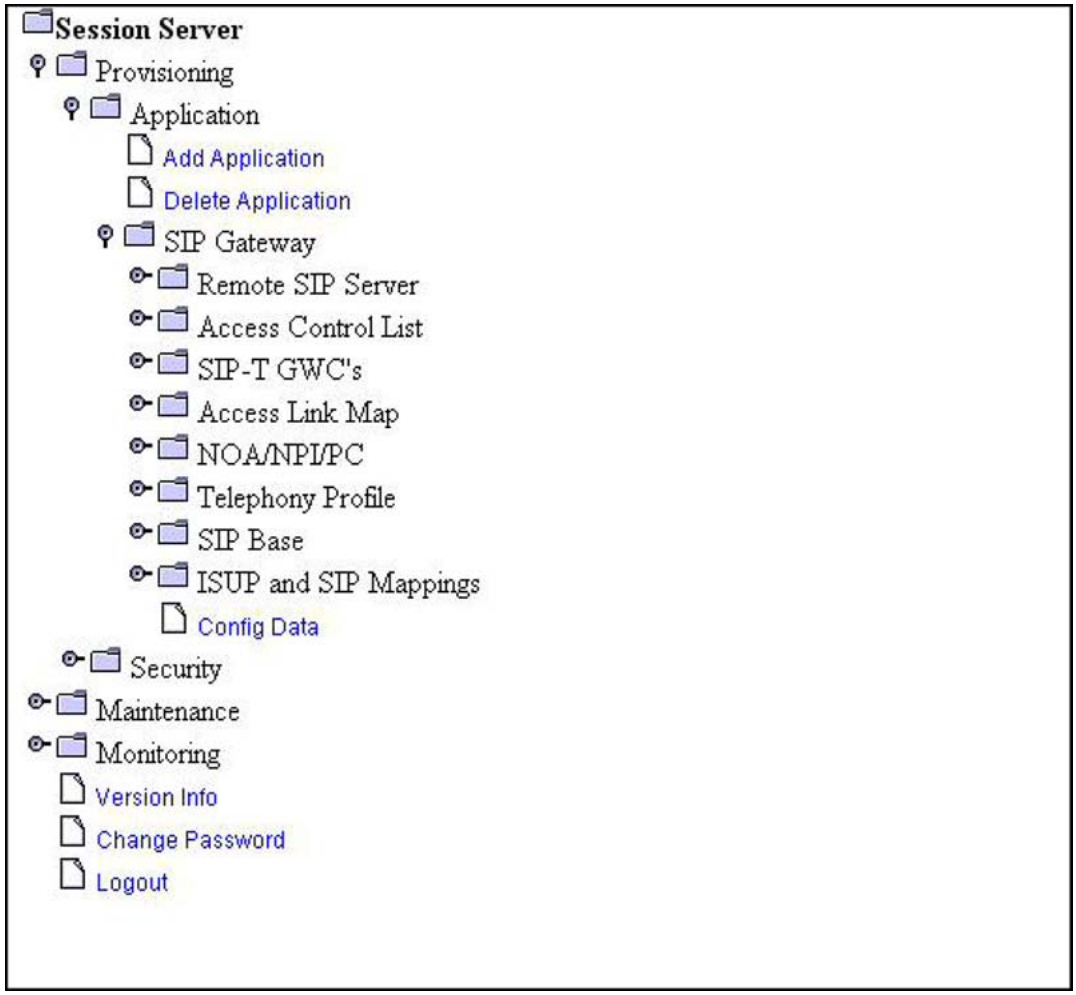
All OAM&P activity on the SST is performed using one or more of the following user interface tools, accessed through the IEMS system:

- the CS 2000 SST Manager GUI, a client web browser application
- the CS 2000 NCGL Platform Manager GUI, a client web browser application
- the NCGL command line interface (CLI)

CS 2000 NCGL Manager main menu used for platform OAM and P



The CS 2000 SST Manager main menu used for application OAM and P



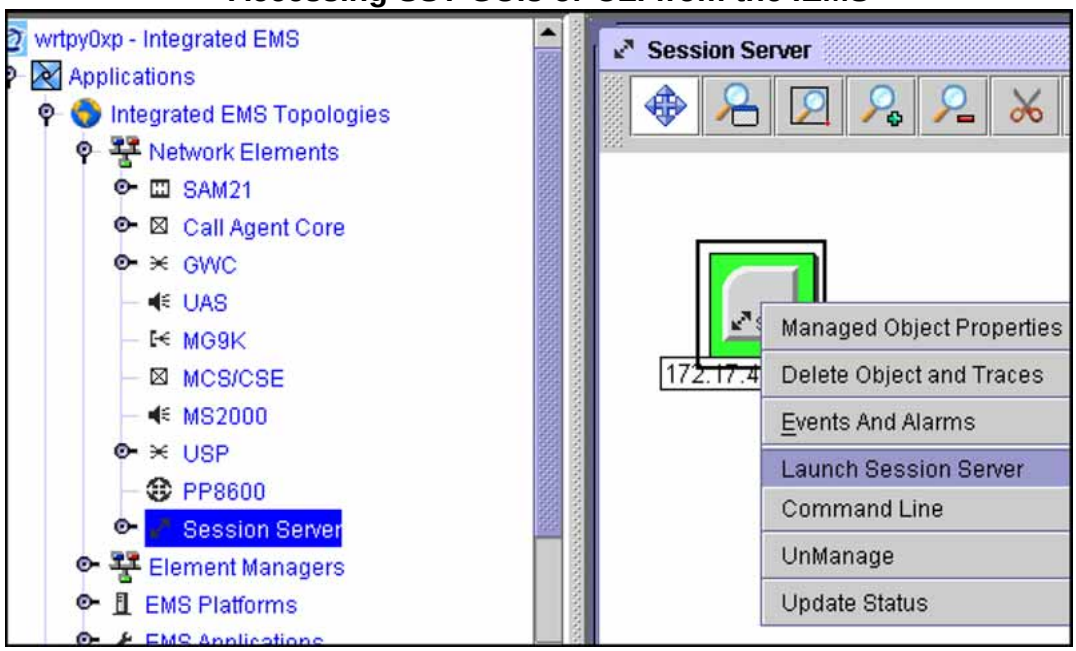
Accessing SST GUIs and CLIs

The SST user interfaces are usually configured to be accessed through the IEMS. It can also be configured without the IEMS because SST uses its own element manager interface. This means that provisioning for a SST takes place directly on the SST node itself. This is possible because SST uses a web-based interface that consists of a web server, running on both SST units, providing web pages for performing OAM&P activities.

There are three primary methods for accessing SST user interfaces:

- All GUI and CLI interfaces to the SST GUI can be accessed by selecting and right-clicking on the active SST element from the IEMS expanded Network Elements view, as shown below.

Accessing SST GUIs or CLI from the IEMS



For more information, see "Accessing Session Server Trunks/NCGL GUIs or CLI using the IEMS," in *Session Server Trunks Security and Administration* (NN10346-611).

- All GUI interfaces to the SST can be accessed from a remote system known to the CS 2000 Management Tools proxy server on the CS-LAN.
- The CLI interface can be accessed through a secure shell (SSH) connection from a remote client to the SST by way of SSH/telnet access through the SPFS server.

For commissioning purposes, the CLI can also be accessed using a console connected to the rear of the SST active unit.

Upgrading the SST

In-service, major release upgrades of existing Session nodes from (I)SN08 to (I)SN09 and (I)SN09 to (I)SN09U are provided in *Nortel Carrier Voice over IP Upgrade and Patches* (NN10440-450).

The NCGL platform software can be patched as well as upgraded by regular maintenance releases (RMRs). The SIP Gateway application is upgraded by way of an RMR. For more information, see *Nortel Carrier Voice over IP Upgrade and Patches* (NN10440-450).

Fault management

The SST uses self-testing, automated diagnostics, and log reporting systems to support maintenance activities and to manage and report faults. These systems raise alarms and generate logs when the following types of hardware or software events occur:

- fault or failure conditions
- correction or resolution of fault or failure conditions
- a preset operating performance or resource capacity threshold such as CP usage is crossed or exceeded
- a transient condition
- a condition that cannot be repaired and causes a system SWACT

Fault management for the SST platform encompasses:

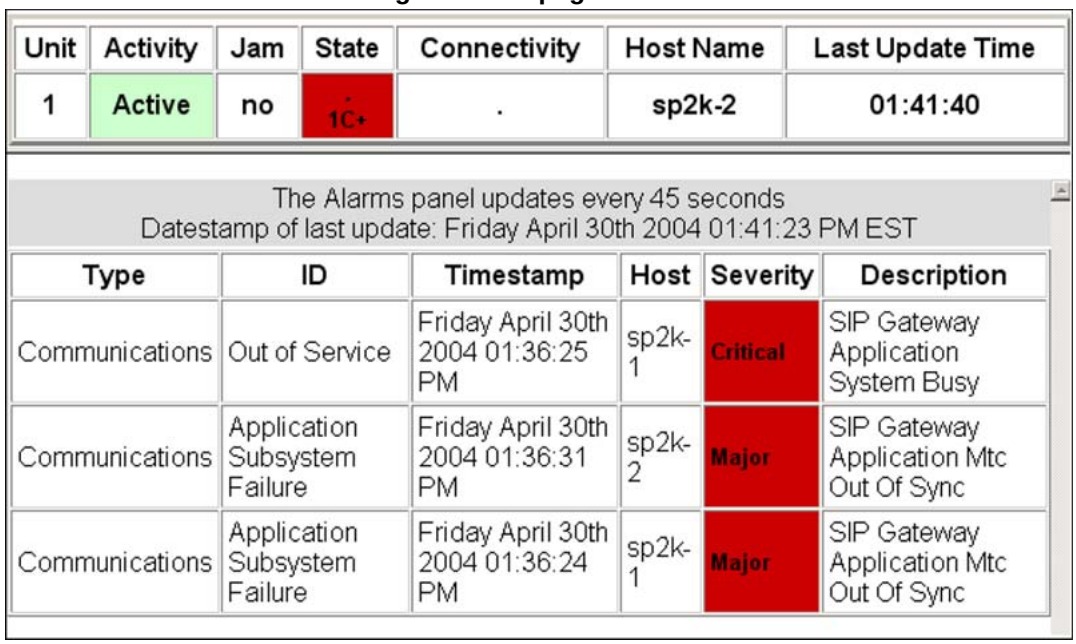
- setting up and managing resource thresholds such as monitoring disk usage and file system usage
- monitoring alarms at either the CS 2000 NCGL Platform Manager or CS 2000 SST Manager GUIs
- reviewing log reports using the CS 2000 NCGL Platform Manager or CS 2000 SST Manager GUIs or view the logs directly from their log files using the NGCL CLI (command line interface)

  If SST is configured to transfer log reports to the OSS network rather than the SST GUIs, log reports may only be available to IEMS or other third-party OSS applications rather than on the logs view of the SST GUIs. Regardless of the type of log configuration, they are always directly accessible on the disk drives of either unit.
- performing routine maintenance and preventative maintenance tasks
- replacing faulty equipment as needed

Monitoring and managing alarms

The SST has the capability for SIP Gateway application or the system itself to generate alarms. These alarms can be viewed on the SST Alarm web page available from either web-based GUI (see "Tools, utilities and user interfaces" (page 17)). Information about alarms includes alarm type, identifier, time stamp, the unit generating the alarm, severity, and a description of the alarm. See the following figure for a view of the alarms page.

View of the CS 2000 SST Manager alarms page



Unit	Activity	Jam	State	Connectivity	Host Name	Last Update Time
1	Active	no	1C+	.	sp2k-2	01:41:40

The Alarms panel updates every 45 seconds
Datestamp of last update: Friday April 30th 2004 01:41:23 PM EST

Type	ID	Timestamp	Host	Severity	Description
Communications	Out of Service	Friday April 30th 2004 01:36:25 PM	sp2k-1	Critical	SIP Gateway Application System Busy
Communications	Application Subsystem Failure	Friday April 30th 2004 01:36:31 PM	sp2k-2	Major	SIP Gateway Application Mtc Out Of Sync
Communications	Application Subsystem Failure	Friday April 30th 2004 01:36:24 PM	sp2k-1	Major	SIP Gateway Application Mtc Out Of Sync

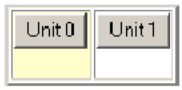
Alarm severity codes indicate the impact of events on the SST or other network elements. There are three levels of alarm: critical, major, and minor. Based on the alarm severity, each alarm has a specific color. Critical and major alarms are red and minor alarms are orange.

For details on SST alarms as well as procedures on viewing alarms and associated logs, see the *Session Server Trunks Fault Management* (NN10332-911).

Sensor information The following figure shows an extract of the Sensor Information page, which displays status and alarm information for hardware sensors. Readings are collected from the platform servers for the following:

- power supplies
- fan speeds
- system temperature
- system voltage
- miscellaneous hardware elements

By default, sensor information appears for the platform server you are logged into. Switch between servers by clicking Unit 1 or Unit 0.



Sensor Group		Sensor Status
Unit 0 Chassis Sensors		minor
Fan Speed	80mm,Left	2958.00 RPM Low Minor/Major = 1989.00/1836.00 RPM
	80mm,Right	2856.00 RPM Low Minor/Major = 1989.00/1836.00 RPM
	40mm,Left	6834.00 RPM Low Minor/Major = 3774.00/3264.00 RPM
	40mm,Right	7191.00 RPM Low Minor/Major = 3774.00/3264.00 RPM
System Temp	Baseboard	35.00 C Low Minor/Major = -5.00/-10.00 C High Minor/Major = 60.00/65.00 C
	Processor1	33.00 C Low Minor/Major = -5.00/-10.00 C High Minor/Major = 75.00/80.00 C
	Processor2	27.00 C Low Minor/Major = -5.00/-10.00 C High Minor/Major = 75.00/80.00 C
	Front Panel	22.00 C Low Minor/Major = -5.00/-10.00 C High Minor/Major = 40.00/45.00 C
	Other	OK
	3.3V	3.38 volts Low Minor/Major = 3.08/2.99 volts High Minor/Major = 3.54/3.64 volts

For more information, see the following sensor log report topics:

- XTS382
- XTS383
- XTS682
- XTS683

Monitoring Logs

SST applications or the platform can generate logs associated with alarms. Customer logs are written to the local custlog file. Stored as ASCII-based text, in CSV format, the log data can be reviewed, copied, printed, saved to a remote system and loaded into a spreadsheet application for further analysis.

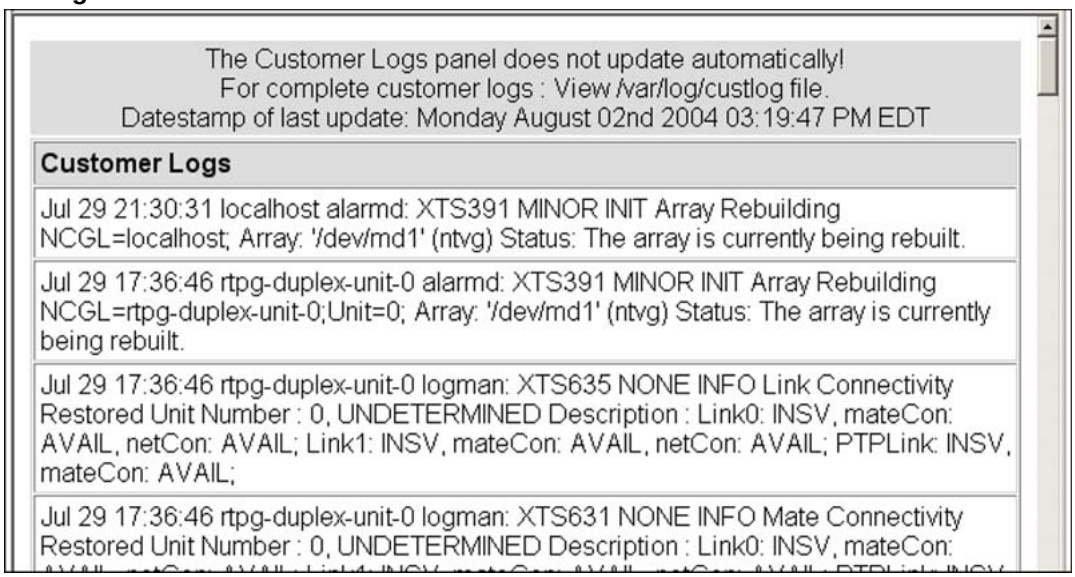
The SST can be configured to alter what log information is written to the local custlog file by redirecting log information to a remote log server and SNMP server using the NCGL commissioning tool.

If the SST is configured to transfer SNMP alarm traps to an OSS network, log reports related to raising or clearing alarms is only available on the IEMS or other third-party OSS application, rather than on the logs view of the SST GUIs.

If the SST is configured to transfer logs to a remote log server, all logs that are ordinarily viewable from the SST GUI or local log file on the disk drive are sent to the log server.

The following sample logs view is displayed by the CS 2000 SST Manager. This view displays a maximum of the most recent 2000 line entries from the current custlog file. When viewing logs from an IEMS system, log headers may differ slightly from what is shown in this view.

Sample customer logs viewed from the CS 2000 Session Server Trunks Manager GUI



Customer log histories can only be viewed by directly accessing the custlog file using the SST CLI (command line interface). Log files can also be downloaded using FTP to a PC or other system capable of connecting to the SST on the secure CS-LAN.

For log reports, see *Carrier Voice over IP Fault Management Logs Reference Volume 1* (NN10275-909v1). For procedures about viewing logs, see the *Session Server Trunks Fault Management* (NN10332-911).

Configuration

Initial installation and provisioning of the SST is provided by Nortel installation personnel or its contracted agents. System configuration management and configuring for expansion can be completed by the customer and is documented in the *Session Server Trunks Configuration Management* (NN10338-511).

Configuration management activities can include:

- configuring access for remote SIP application servers
- managing SIP-T GWCs associated with the SST
- managing ISUP-to-SIP mapping, SIP-to-ISUP mapping, variant mappings and redirection mappings
- provisioning TLS for specific remote SIP servers
- recommissioning a replacement SST unit
- modifying the NCGL platform provisioning on a unit
- reconfiguring SST unit BIOS settings
- reinstalling or reconfiguring the SIP Gateway application
- creating, modifying, monitoring and removing file systems
- adding SIP-T DPT trunk groups and managing other XA-core tables on the CS 2000
- managing the web proxy settings on the CS 2000 Management Tools server used for accessing the SST GUI by proxy

Accounting and Billing

The billing process on the SST generates billing records, formats them using the IPDR format, and writes them to the local hard drive. An end user can access these records by using a secure shell (SSH).

Performance management

Like other components in the Carrier VoIP environment, the SST records operational measurements (OMs) for various performance related events. These OMs are essential information sources for determining preventive and corrective maintenance actions, as well as identifying provisioning problems or capacity limitations. Currently, all OMs are related to activities and processes in the SIP Gateway application, running on the SST.

OMs are viewed through the IEMS, using the command line interface (CLI) to the SST, or through a direct, secure shell (SSH) connection to the SST. OMs cannot be viewed directly from the IEMS.

OM data recorded on one unit of a SST node is completely independent of OM data recorded on its mate unit. Data is not transferred from one unit to another during SIP Gateway application database synchronization activities.

When more than one SST node is installed in the network, OM data recorded by the first node is independent of that recorded by other SST nodes.

Monitoring SIP-T DPT callp traffic levels

Operational measurements, related to SIP-T DPT call capacity limits, capacities are collected on the core. These OMs show the call processing load for each SIP-T DPT trunk group. This data can be used to forecast future equipment loading and determines future equipment requirements.

Service monitoring

Some operational measurements can indicate service level degradation for the SST when combined with alarms, indicating that resources are running low. This information helps to determine the corrective action which may include equipment repair.

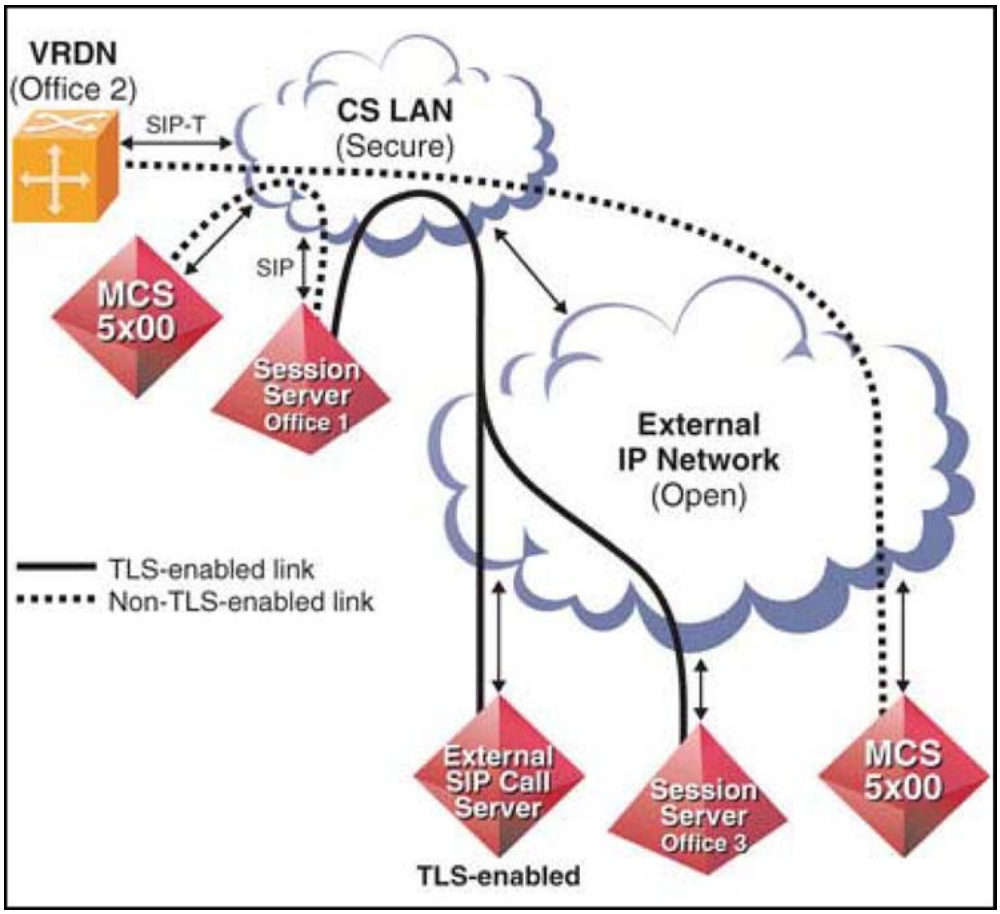
Security monitoring

Some operational measurements can indicate security degradation or possible intrusion. When combined with alarms, this information helps to determine the corrective action which may include generating new security certificates or disconnecting suspicious remote SIP servers.

Security for SST SIP messaging

The Transport Layer Security (TLS) security feature provides security for SIP connections using the TLS protocol. This protocol enables secure data transmission for inter-call server communication, such as between the SST and a remote SIP application server.

The TLS feature will allow the SST to establish TLS sessions with a remote Call Server or SIP application server that is TLS aware. With the support of TLS on the SST, connections to a SIP-enabled server can be secured over non-secure networks like the internet, allowing SIP-based client/server applications to communicate with privacy and integrity.



Provisioning options enable non-TLS UDP, non-TLS TCP, or TLS connections to be set up and utilized. For instructions on configuring TLS, see *Session Server Trunks Configuration Management* (NN10338-511).

The TLS feature also provides security-related logs, OMs, and alarms for monitoring security failures, attacks, and session establishment. For instructions on monitoring security-related logs and alarms, see the *Session Server Trunks Fault Management* (NN10332-911). For instructions on monitoring security-related operational measurements, see *Session Server Trunks Performance Management* (NN10342-711).

Operational administration

User administration is controlled though both the SST GUIs and the CLI. Procedures for managing users are found in *Session Server Trunks Security and Administration* (NN10346-611).

Customer documentation

The SST customer documentation suite consists of the following NTPs:

- *Nortel Session Server Trunks Basics* (NN10333-111) (this NTP)
- *Nortel Carrier Voice over IP Upgrade and Patches* (NN10440-450)
- *Nortel Session Server Trunks Fault Management* (NN10332-911)
- *Nortel Session Server Trunks Configuration Management* (NN10338-511)
- *Nortel Session Server Trunks Performance Management* (NN10342-711)
- *Nortel Session Server Trunks Security and Administration* (NN10346-611)

Customer support

See the Basics NTP applicable to your Carrier VoIP solution to find information about support options and to order SST software.

Terminology

The following terms and acronyms are commonly used in Carrier VoIP networks and by SST.

ANSI
American National Standards Institute

APG
Anchor Packet Gateway

APS
Audio Provisioning Server

ARP
Address Resolution Protocol

ASPEN
a call control protocol

ATM
Asynchronous Transfer Mode

BICC
Bearer Independent Call Control

CCF
Call Control Frame

CallP
Call Processing

CICM
Centrex IP Client Manager

CISM
Cabinetized Integrated Service Module

CLLI
Common-language Location Identifier

CMTS
Cable Modem Termination System

CM
Computing Module; also known as the core or XA-Core

CODEC
Encoder-decoder

Contivity 600 VPN switch
Contivity 600 Virtual Private Network switch

COPS
Common Open Policy Service

CORBA
Common Object Request Broker Architecture

cPCI
compact Peripheral Component Interconnect

CSAM
Cabinetized Services Application Module

CS 2000
Communication Server 2000:

CS LAN
Communication Server (or Call Server) Local Area Network: is the integrated component within Nortel Networks Carrier VoIP CS 2000 and CS 2000-Compact that provides a secure environment for mission critical processing of message traffic between the CS 2000 components and other key network elements.

CSV
Comma Separated Values

DID
Direct Inward Dialing

DPT
Dynamic Packet Trunking

DMS
Digital Multiplex Switch

DNS
Domain Name Service

DPT
Dynamic packet trunking

DSM-CC
Digital Storage Media - Command and Control; used to manage universal port gateways, such as a trunk gateway which can connect TDM terminations.

DQoS
Dynamic Quality of Service feature: assigns (on demand) resources for each communication, depending on the QoS requested

DS0
Digital Signal Level 0: the 64 Kbit/s channel that is the basic building block for a North American T1 transmission line

DS0A
Refers to a process where a sub-rate signal (2.4, 4.8, or 9.6 Kbps) is repeated 20, 10, or 5 times respectively to make a 64 Kbps DS0 channel

DS1
Digital Signal Level 1: the North American Digital Hierarchy signaling standard for transmission at 1.544 MB/s.

DS30
Digital Signal Level 30: is the equivalent of 30 DS1s

DSL
Digital Subscriber Line

ESA
Emergency Standalone Support

FCAPS
Fault, Configuration, Accounting, Performance, Security

FCM
Fabric Control Message

FLPP
Fiberized Link Peripheral Processor

FQDN
Fully-qualified Domain Name

FTP
File Transfer Protocol

GUI
Graphical User Interface

GWC
Gateway Controller

GWCEM
CS 2000 Gateway Controller (element) Manager

HIOP
High performance Input Output Processor; provides the XA-Core with Ethernet access to the IP-based telco network and supports communication between the core and the GWC

HTML
Hypertext Markup Language; used in creating web pages

HTTP
Hypertext Transfer Protocol

HTTPS
Secure Hypertext Transfer Protocol

ICMP
Internet Control Message Protocol

IETF
Internet Engineering Task Force

IEMS or Integrated EMS
Integrated Element Management System

INSV
In-service

I/O
Input/Output

IP
Internet Protocol

ISUP
Integrated Services (Digital Network) User Part

ITU
International Telecommunications Union

JAAS
Java™ Authentication Authorization Service

JRE
Java™ Runtime Environment

JWS
Java™ Web Start

LAN
Local Area Network

LMM
Line Maintenance Manager

LPP
Link Peripheral Processor; the core switch's link to the SS7 network. In the IP topology, works with the GWC to supply signaling to the destination switch

MANB
Manual Busy

MAPCI
Maintenance And Administration Position Command Interface

Mate; Mate Unit
the complementary, back-up or redundant SST unit

MCS
Multimedia Communications Server; a multimedia application server

MEGACO
Media Gateway Control; an IETF standard for peripheral messaging protocols promulgated originally as H.248

MGC
Media Gateway Controller

MGCP
Media Gateway Control Protocol

MTA
Multimedia Terminal Adapter

MTX
Mobile Telephone Exchange

NAS
Network Access Service

NCS
Network based Call Signaling

NAT
Network Address Translation

NAPT
Network Address And Port Translator

NCGL
Nortel Carrier-Grade Linux; a version of the Linux™ operating system that has been enhanced to operate in a NEBS compliant telecommunications environment

NEBS
North American New Equipment Building Standard

NFS
Network File System

NGSS
Next Generation SST; another name for SST, a name sometimes seen in GUI or CLI outputs from the SST or Policy Controller

NOCs
Network Operations Centers

NPM
Network Patch Manager

NTP
Network Time Protocol; also Nortel Technical Publication

OAM&P
Operations, Administration, Maintenance, And Provisioning

OC-3
Optical Carrier Level 3 is the SONET transmission rate of 155.52 Mbit/s

OM
Operational Measurement

OSI
Open Systems Interconnection

OSS
Operations Support System

OSSGate
is an application that provides a machine interface for provisioning components within Carrier VoIP

PM Poller
Performance Measurements Poller

PDF
Adobe™ Portable Document Format

PEP
Policy Enforcement Point

PRI
primary rate interface

QCA
Quality of Service Collector Application

QoS
Quality Of Service

QoSCA
Quality of Service Collector Application

RAID
redundant array of inexpensive disks

RAS
Remote access server

RMGC
Redirecting Media Gateway Controller

RMON
Remote MONitoring specification is a simple network management protocol

RMR
Regular maintenance release

RTP
real-time transport protocol

SAM-XTS
Session Application Module eXtreme Thin Server

SC
Shelf Controller

SCP
secure copy (a flavor of the Unix/Linux cp command)

SCCP
Signaling Connection Control Part Protocol

SCTP
Simple Control Transmission Protocol

SDM
SuperNode Data Manager

SDP
signal distribution point or Session Description Protocol

SESM
Succession Element Sub-Network Manager is a software package that includes several CS 2000 Management Tools applications

SFT
Secure File Transfer

SIP
Session Initiation Protocol

SIP-T
Session Initiation Protocol for Telephony

SNMP
Simple Network Management Protocol (SNMP)

SQL
System Query Language; used in many databases

SS7
Signaling System Number 7: is a family of signaling protocols used to set up, manage, and tear down connections, as well as to exchange non-connection associated information.

SPFS
Server Platform Foundation Software: is the NCL software package that contains base operating system and common tools, libraries and server functions used by element-management-level applications.

STORM
Storage Manager

STP
Signaling Transfer Point: a node in the SS7 network

Succession
The former brand name for Carrier VoIP or Nortel Networks

SWIM
CS 2000 Core Manager Software Inventory Manager

SYSB
System Busy

TCP
Transmission Control Protocol

TDM
Time Division Multiplexing

TFTP
Trivial File Transfer Protocol

TLS
Transport Layer Security; a protocol used in peer-to-peer SIP communications to secure a session

TMM
Trunk Maintenance Manager

UAS
Universal Audio Server or User Agent Server

UDP
User Datagram Protocol

Unit
a single SST SAM-XTS hardware platform, where two units are configured to create a single, fault-tolerant node

USP
Universal Signaling Point

VDRN
Virtual Routing Distribution Node: is a type of GWC

VoIP
Voice over Internet Protocol

VPN
Virtual Private Network

XA-Core
Extended Architecture Core

XML
Extensible Markup Language

XTS
eXtreme Thin Server

Carrier VoIP

Session Server Trunks Basics

Publication: NN10333-111
Document status: Standard
Document version: 04.02
Document date: 20 October 2006

To provide feedback or report a problem in this document, go to www.nortel.com/documentfeedback.

The information in this document is sourced in Canada, the United States of America, and the United Kingdom.