Session Server Basics

What’s new in the (I)SN08 release?

The following new features and activities are covered in the Session Server NTP suite for the (I)SN08 release:

- Features A00008383 and A00007275 - Support for Multiple HTTPS connection to the Session Server through SSPFS. This feature provides support for multiple proxy https connections from IEMS/SSPFS and allows multiple Session Server nodes to reside on the CS-LAN. This feature is documented in the Session Server Configuration Management NTP.
- Feature A00006893 - provides for configuring TLS (transport layer security) on the signaling paths (but not the call content) between the Session Server and a similarly configured remote SIP application server or call server. Configuring TLS support is documented in the Session Server Configuration Management NTP. OMs supporting TLS security are also now available and documented in the Session Server Performance Management NTP. Security certificate management is also enhanced and covered in the Session Server Security and Administration NTP.
- Feature A00007268 - This OM enhancement activity enhances the existing OM subsystem to support a dynamic number of tuples. It is documented in the Session Server Performance Management NTP.
- Feature A00007270 - Provides for Overload Controls on the Session Server SIP Gateway application. Most of this feature is not customer visible; however, significant changes to log SIPC310 in the Session Server Fault Management NTP have been made to support this feature.
- An in-service, major release upgrade activity, supporting upgrades of existing Session Server-SIP application nodes from SN07 to SN08 is provided in the Session Server Upgrades NTP.

Session Server customer documentation

The Session Server customer documentation suite consists of the following NTPs:

- Session Server Basics, NN10333-111, (this NTP)
- Session Server Configuration Management, NN10338-511
- Session Server Fault Management, NN10332-911
- Session Server Performance Management, NN10342-711
- Session Server Security and Administration, NN10346-611
- Session Server Upgrades, NN10349-461

Functional description and role of the Session Server

The Session Server is a call media and signaling interoperability component. It is made up of a high capacity, carrier grade hardware platform based on the SAM-XTS (used also for STORM IA) along with software consisting of an NCGL (Nortel Carrier Grade Linux) 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.

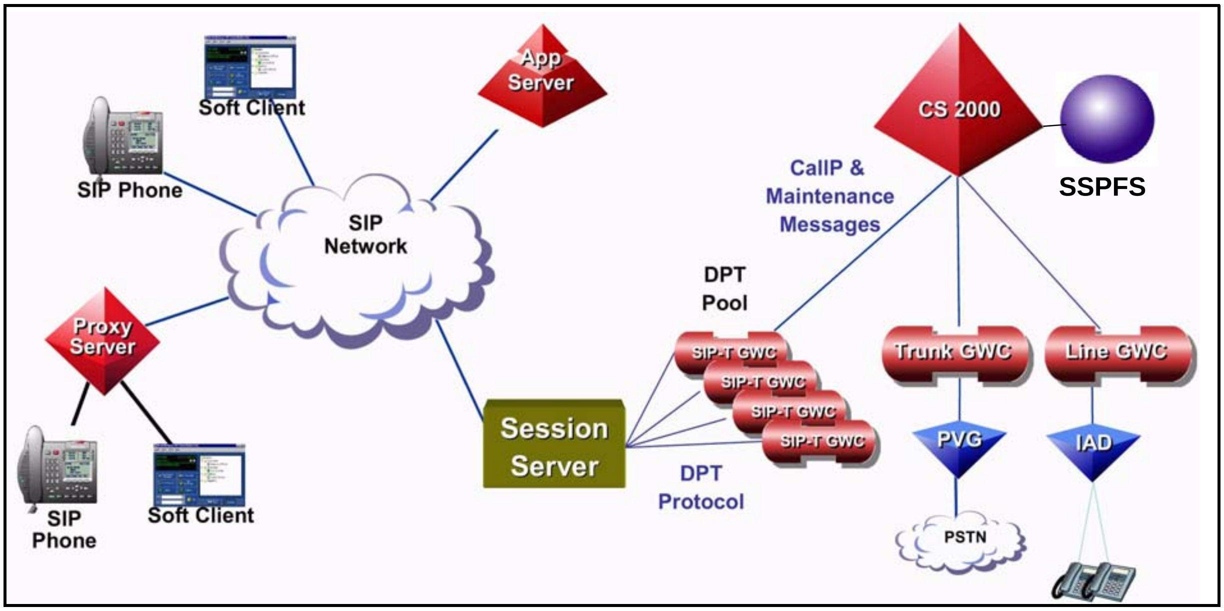
The primary application introduced on the Session Server platform is the SIP Gateway application which facilitates interoperability between the CS 2000 network and 3rd party SIP-based Call Servers and Media Application Servers (such as MCS). This capability enables SIP-based call servers to access the PSTN through the CS 2000 network and eliminates the need for a (slower) VRDN GWC for call routing.

Session Server 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 5200 (Carrier) and the CS 2000 for all SIP-T supported services and functionality supported for the MCS application server
- Open Standard Interop with 3rd Party Call Servers, Proxy Servers and Application Servers
- Support for multi-vendor environments

The following diagram illustrates Session Server’s role in the CS 2000 network of components.

Relationship of Session Server 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 DPT GWCs.
Trunk and Line GWCs	Function as the interface between the XA-Core and gateways such as the Media Gateway 7480/15000 (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	Function as a router to direct incoming/outgoing calls between SIP-T and Line or Trunk GWCs.
SSPFS	SSPFS (Succession Server Platform Foundation Software) Acts as 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 Session Server, the CS 2000 Session Server Manager and the CS 2000 NCGL Platform Manager.

Supported configurations

The following configurations are supported in SN08, using the Session Server in call server-to-call server communication:

- SN08 Session Server and SN08 Session Server
- SN08 Session Server and SN07 Session Server
- SN08 Session Server and SN07/SN08 GWC-VRDN
- SN08 Session Server and SN06.0/6.2 GWC-VRDN

The following configurations are supported in SN08, using the Session Server in call server-to-application server communication:

- SN08 Session Server and MCS5200 3.0
- SN08 Session Server and MCS5200 4.0

Session Server hardware platform

The Session Server chasses deployed in a rack-mounted configuration house processing hardware, hard drives, ethernet interface ports (two currently reserved for inter-Session Server communication for fault tolerance), and redundant power supplies. 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^{TM} cc3310 carrier-grade server. With two chassis working together to provide carrier-grade level fault tolerance, this hardware configuration provides the platform for the SIP Gateway application.

Features of each hardware platform unit include:

- Dual 2.4GHz Xeon Processors
- 4GB DDR Memory
- Dual 73GB Hot Swappable Disk Drives
- CD-RW/DVD-R Drive
- Dual Hot Swappable Power Supplies
- Dual GigE 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.

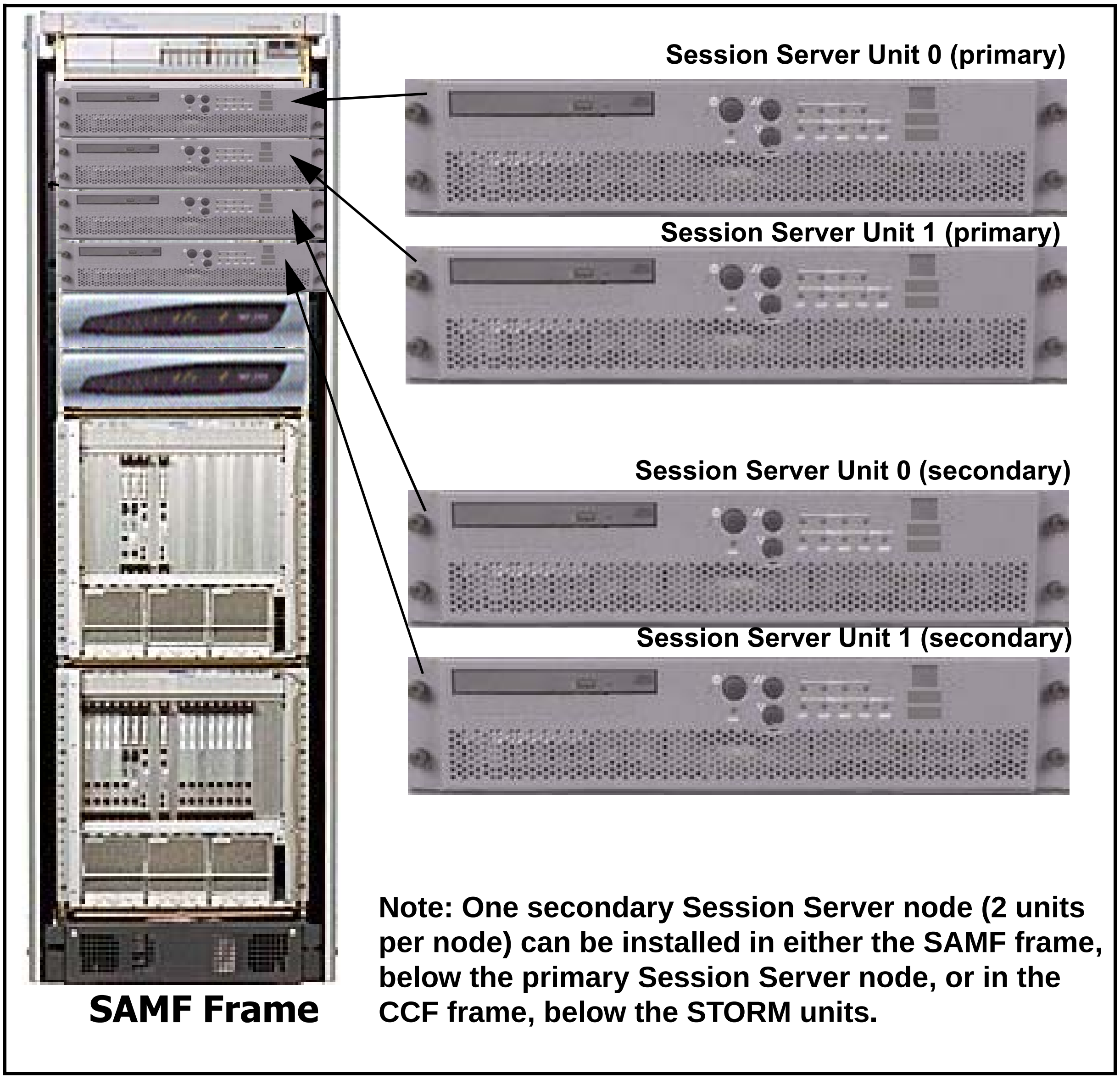
Configuring multiple Session Server nodes in the call server network

In SN08, one or more Session Server nodes are installed in the SAMF and Call Control (CCF) frames. On the SAMF frame (NTRX51HA), the primary Session Server node (made up of two hardware units) is mounted below the BIP power distribution unit. A secondary Session Server node (2 additional hardware units) can be mounted below the primary node in the SAM-F frame. As an option, the secondary Session Server node can be mounted in the CCF frame (NTRX51TA), below the STORM units. A maximum of 2 nodes (four units total) are allowed in a single CS 2000 call server network. Do not confuse Session Server units with Policy Controller or STORM units, which can appear identical.

Typically, each Session Server 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 Session Server hardware units in the SAM-F frame.

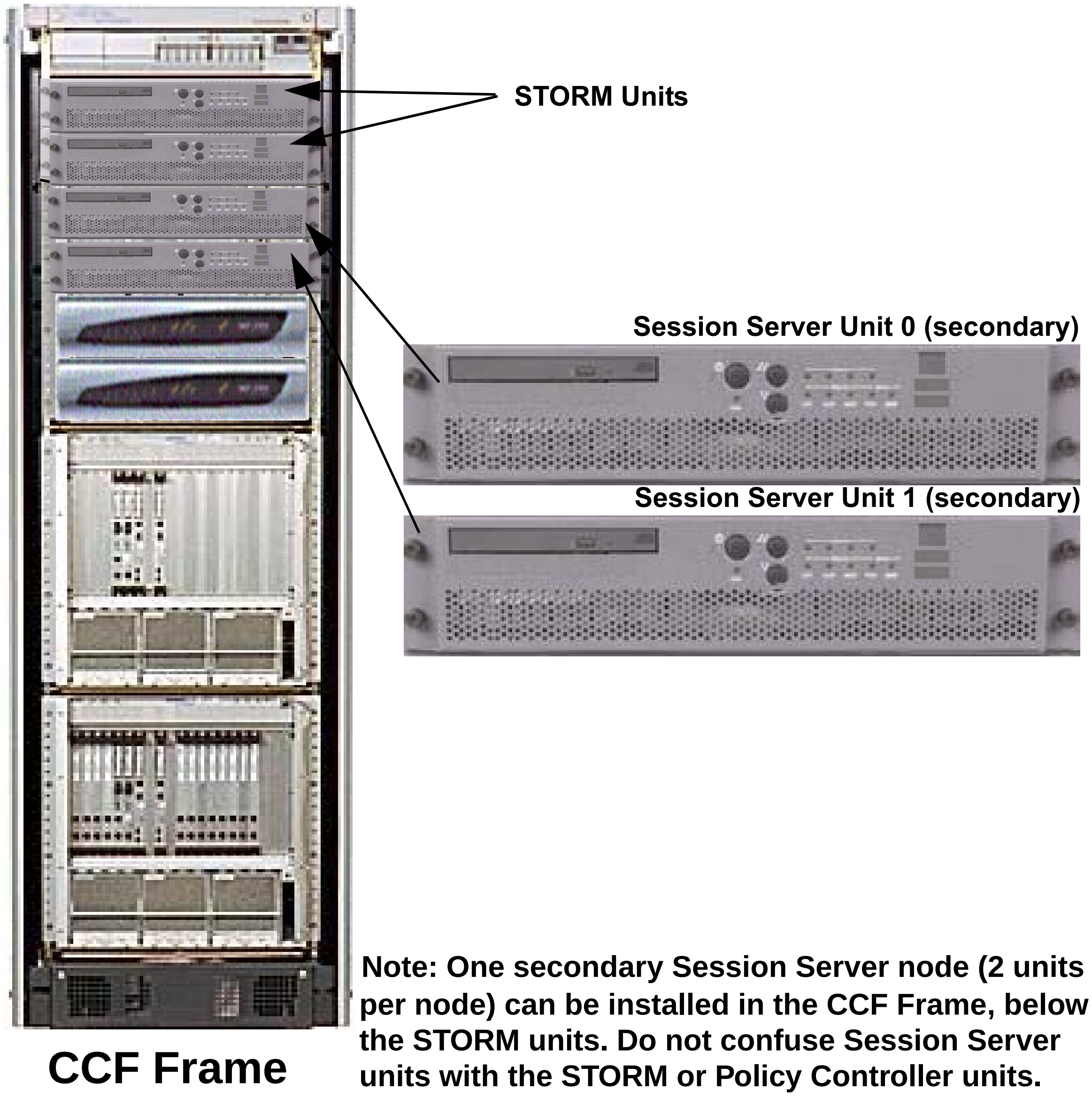
Identifying Session Server units in the SAMF frame (NTRX51HA)


Session Server Unit 0 (primary)
Session Server Unit 1 (primary)
Session Server Unit 0 (secondary)
Session Server Unit 1 (secondary)
SAMF Frame

Note: One secondary Session Server node (2 units per node) can be installed in either the SAMF frame, below the primary Session Server node, or in the CCF frame, below the STORM units.

The following diagram shows the location of the secondary Session Server hardware units in the CCF frame.

Identifying Session Server secondary units in the CCF frame (NTRX51TA)


STORM Units
Session Server Unit 0 (secondary)
Session Server Unit 1 (secondary)
CCF Frame

Note: One secondary Session Server node (2 units per node) can be installed in the CCF Frame, below the STORM units. Do not confuse Session Server units with the STORM or Policy Controller units.

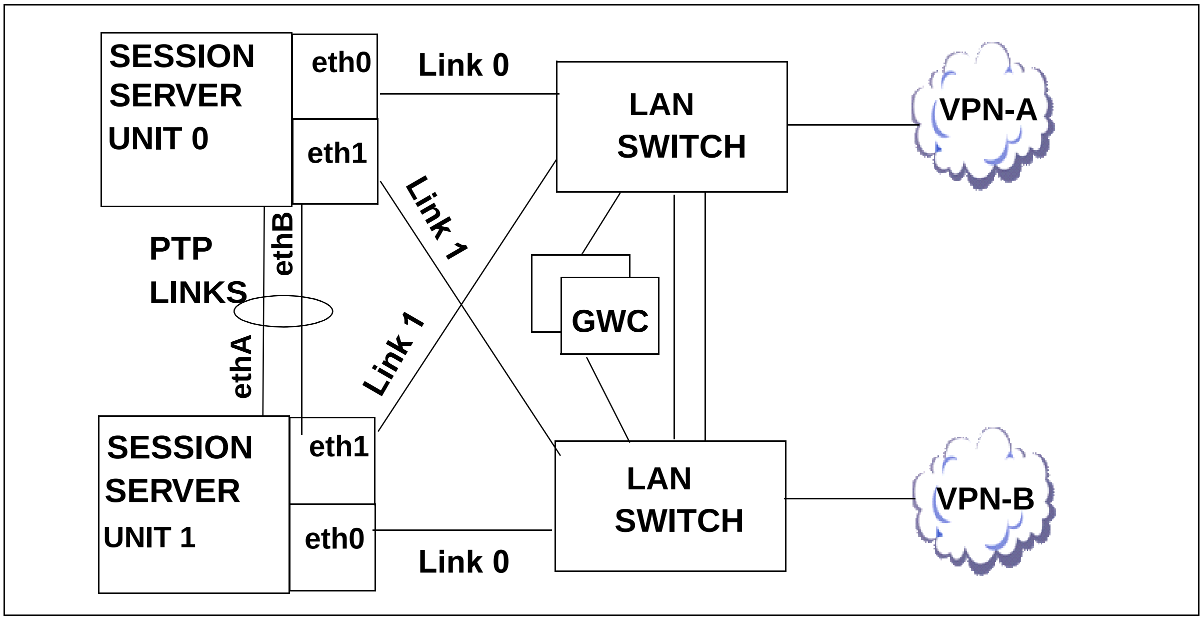
Network interfaces and connectivity

Each Session Server unit has two GigE 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 Session Server 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 Session Server, refer to the Session Server Security and Administration NTP, NN10346-611.

Link Configuration of the Session Server with the CS-LAN



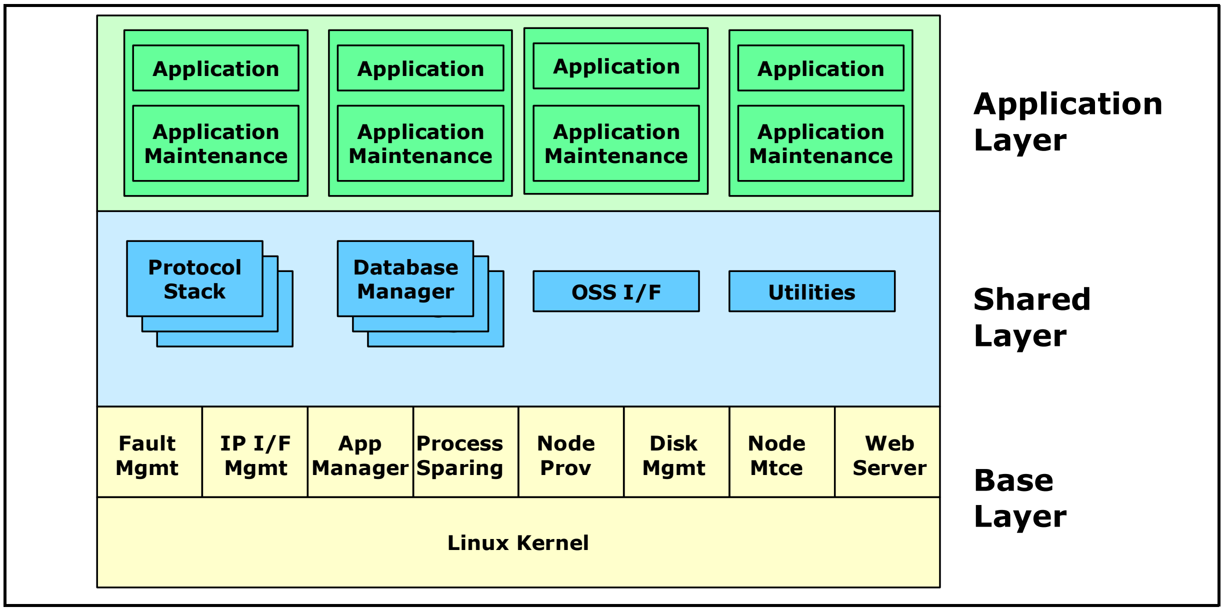
Software architecture

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

- The base NCGL (Nortel Carrier Grade Linux) 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, that are 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 application processes, in this case the SIP Gateway application processes.

Session Server Software Architecture

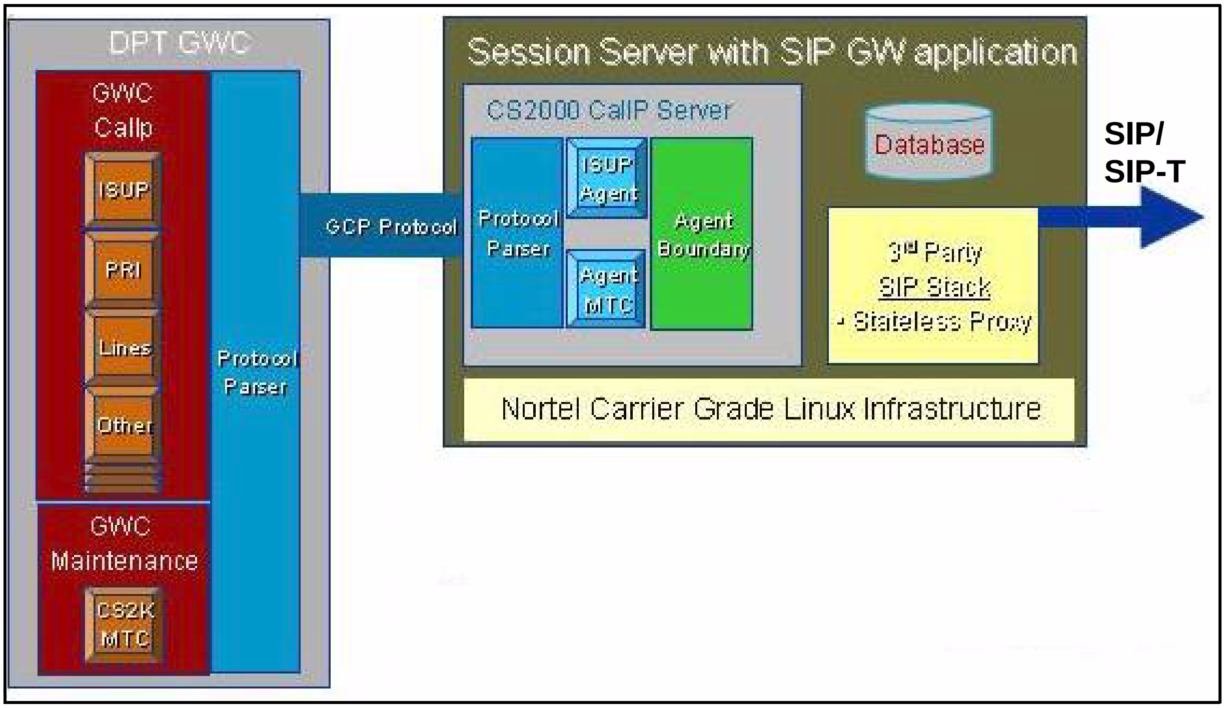


SIP Gateway application software

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 Session Server platform and communicates indirectly with the CS2000 through SIP-T GWCs. Using Generic Call Processing (GCP) protocol to interface with the GWCs, Session Server integrates DPT call processing, managed by the CS 2000 by providing a direct trunking interface between the TDM interface on the CS2000 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.

Figure 1 SIP Gateway application interface protocols



SIP Application Maintenance, part of the application layer, is responsible for 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 Session Server Manager, and generating maintenance related logs and alarms.

About CS 2000 SIP implementation

The Session Initiation Protocol (SIP), used by the Session Server is a protocol designed for multimedia communication. The current CS 2000 SIP implementation is a proprietary implementation of SIP-T (SIP for telephony) used to allow interoperation with 3rd party Proxy Servers and Application Servers, in compliance with the IETF (Internet Engineering Task Force) 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 Session Server the following client web browsers are supported:

Supported web clients on a Windows 2000, XP, or 2003-based PC:

- Internet Explorer 6.0 SP1and above
- Netscape 6.2.3 and 7.1+

Supported web clients on a Solaris 2.8 and 2.9-based Sun workstations:

- Netscape 6.2.3
- Mozilla 1.4+

Consult the Session Server Configuration Management NTP, NN10338-511, for more information about supported browsers.

Software ordering and delivery

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

Session Server software loads

The Session Server 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 Session Server. Consult the Session Server Upgrades NTP, NN10349-461, for details.

Session Sever was first released in SN07. Therefore, backwards compatibility of Session Server with other Carrier VoIP releases has limited support for to releases 6.0 and 6.2, for some IP solutions. For more information about release compatibility between Session Server and other Carrier VoIP loads, consult your Carrier Voice over IP Network Upgrade Overview NTP, NN10440-450.

Upgrading a CS2000 network to support Session Server

Upgrading a CS 2000 network-based office to include the Session Server and migrating existing SIP-T traffic from the VRDN architecture to the Session Server is not covered in the Session Server NTPs, although some procedures related to migration may be included in the NTPs for other reasons, For initial installation and provisioning of a Session Server into an existing network, consult your Nortel service representative for information about installing the Session Server component into a call server network.

Operations, administration, maintenance and provisioning strategy

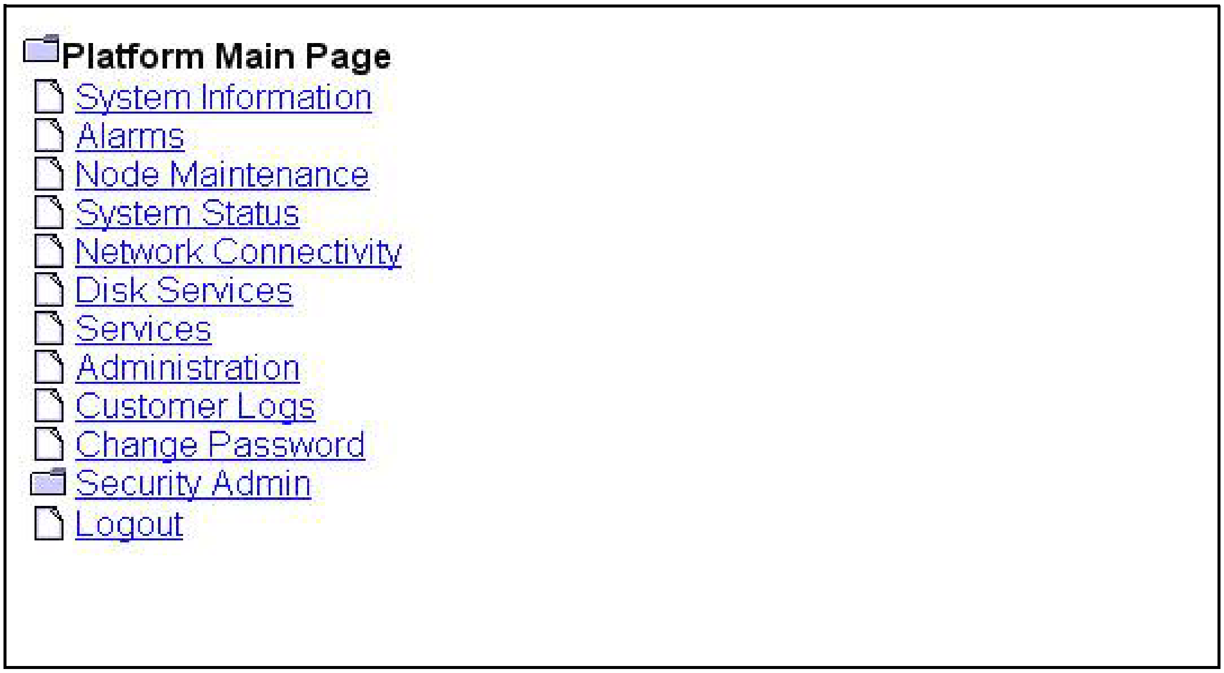
Since the Session Server is a component in the CS 2000 network, it uses operations, administration, maintenance and provisioning (OAM&P) functions for handling fault, configuration, accounting, performance and security (FCAPS) management activities in similar fashion to other components in the CS 2000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

Tools, utilities and user interfaces

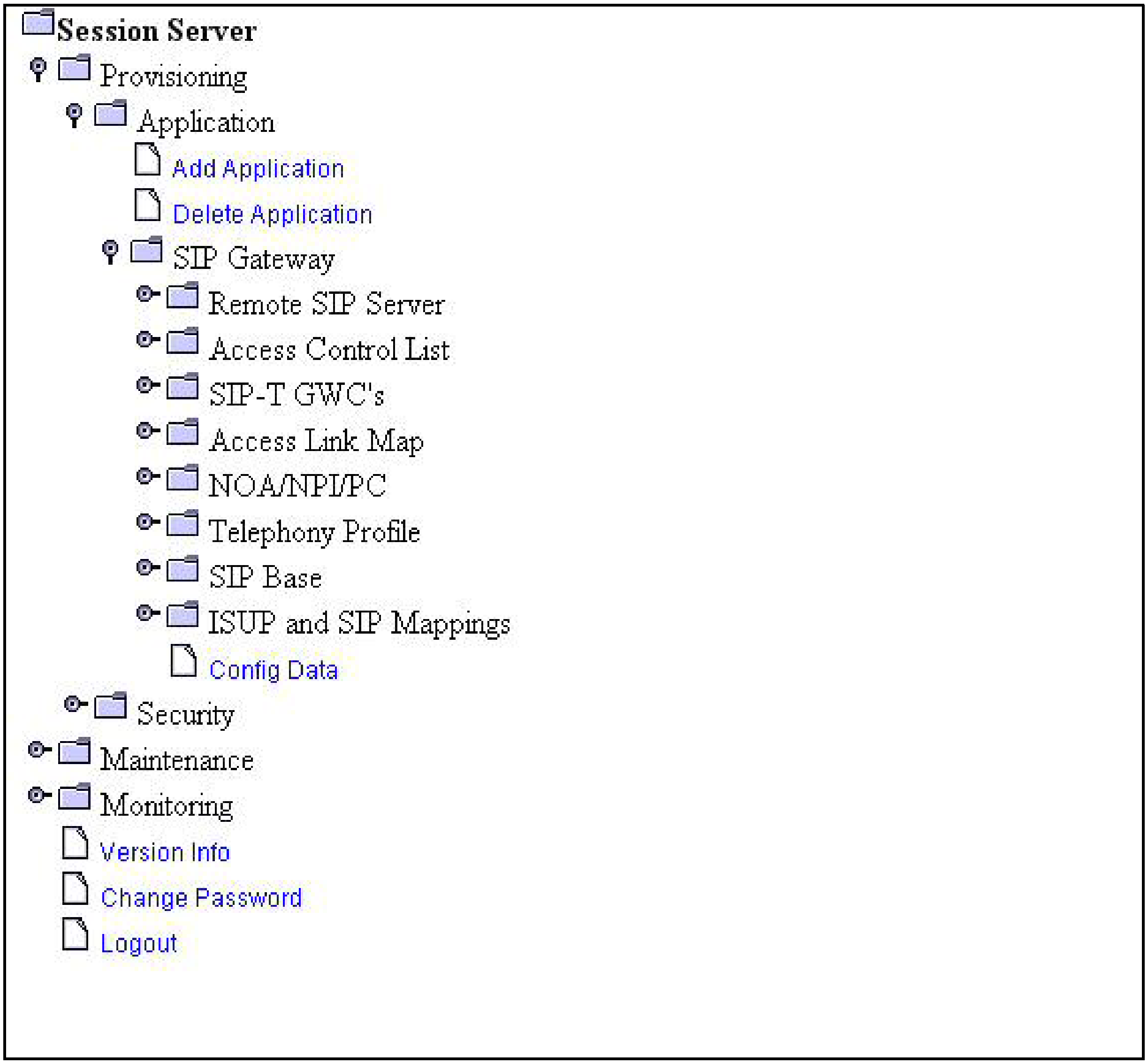
All OAM&P activity on the Session Server is performed using one or more of the following user interface tools, accessed through the Integrated EMS system:

- the CS 2000 Session Server 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)

The CS 2000 NCGL Manager main menu used for platform OAM&P



The CS 2000 Session Server Manager main menu used for application OAM&P



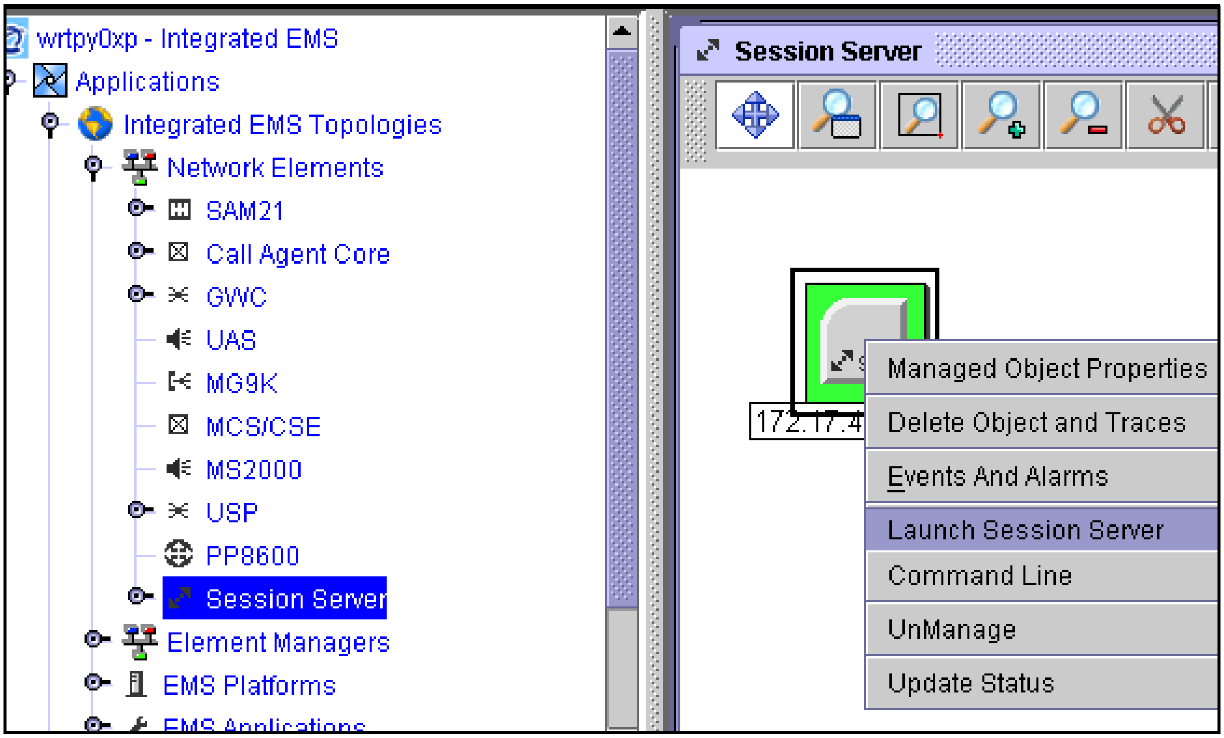
Accessing Session Server GUIs and CLIs

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

There are three primary methods for accessing Session Server user interfaces:

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

Accessing Session Server GUIs or CLI from the Integrated EMS



For more information, refer to procedure *Access the CS 2000 Session Server GUIs from the Integrated EMS*, found in the Session Server Security and Administration NTP, NN10346-611. For more information about using the Integrated EMS service, refer to the Integrated EMS Basics NTP, NN10329-111.

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

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

Configuration

Initial installation and provisioning of the Session Server 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 Configuration Management NTP, NN10338-511.

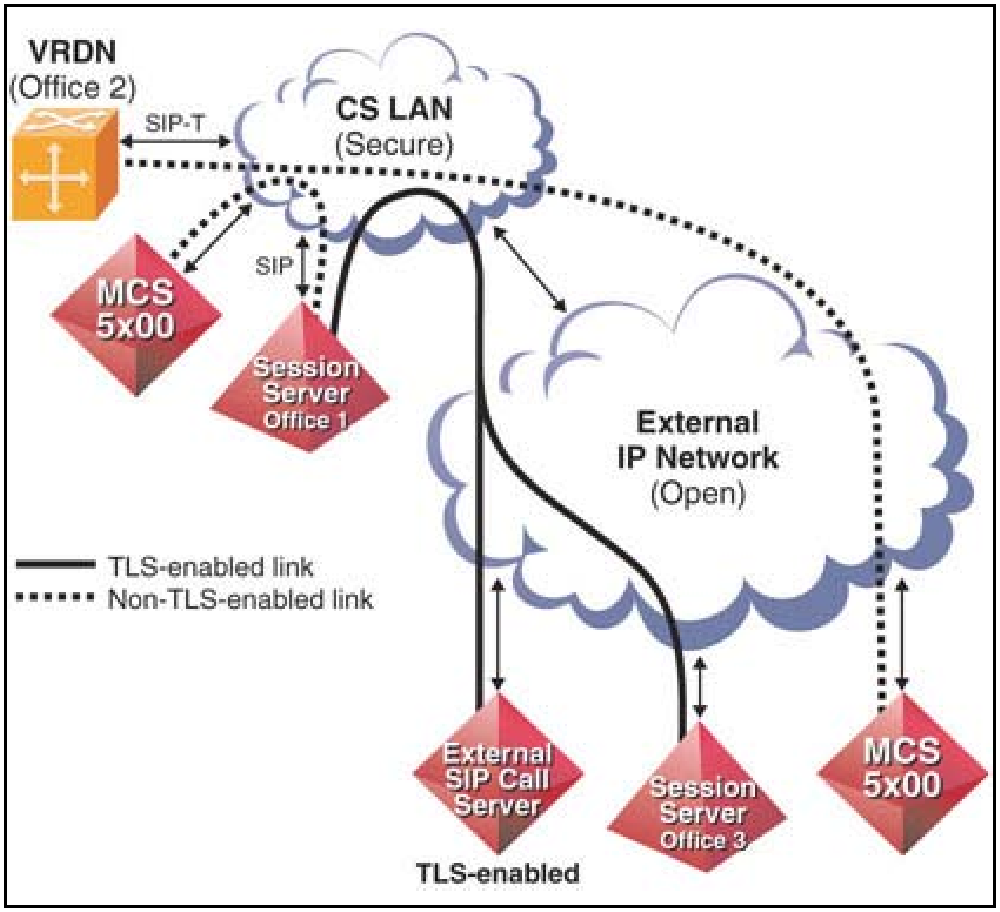
Configuration management activities can include:

- configuring access for remote SIP application servers
- managing SIP-T GWCs associated with the Session Server
- managing ISUP-to-SIP mapping, SIP-to-ISUP mapping, variant mappings and redirection mappings
- provisioning TLS for specific remote SIP servers
- recommissioning a replacement Session Server unit
- modifying the NCGL platform provisioning on a unit
- reconfiguring Session Server 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 Session Server GUI by proxy

Security for Session Server SIP messaging

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

The TLS feature will allow the Session Server to establish TLS sessions with a remote Call Server or SIP application server that is TLS aware. With the support of TLS on the Session Server, connections to a SIP enabled server can be secured over a non-secure network, 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. Refer to the Session Server Configuration Management NTP, NN10338-511, for instructions on configuring TLS security. The TLS Security feature also provides security-related logs, OMs, and alarms for monitoring security failures, attacks, and session establishment. Refer to the Session Server Fault Management NTP, NN10332-911, for instructions on monitoring security-related logs and alarms. Refer to the Session Server Performance Management NTP, NN10342-711, for instructions on monitoring security-related operational measurements.

Accounting and Billing

The billing process on the Session Server 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).

Fault management

The Session Server 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
- when a preset operating performance or resource capacity threshold such as CP usage is crossed or exceeded
- a condition occurs that is transient or cannot be repaired and causes a system SWACT

Fault management for the Session Server 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 Session Server Manager GUIs
- reviewing log reports using the CS 2000 NCGL Platform Manager or CS 2000 Session Server Manager GUIs or view the logs directly from their log files using the NGCL CLI (command line interface)

  Note: If Session Server is configured to transfer log reports to the OSS network rather than the Session Server GUIs, log reports may only be available to Integrated EMS or other 3rd party OSS applications rather than on the logs view of the Session Server GUIs. Regardless of logs configuration, logs are always directly accessible from the log files located on the disk drives of either unit.

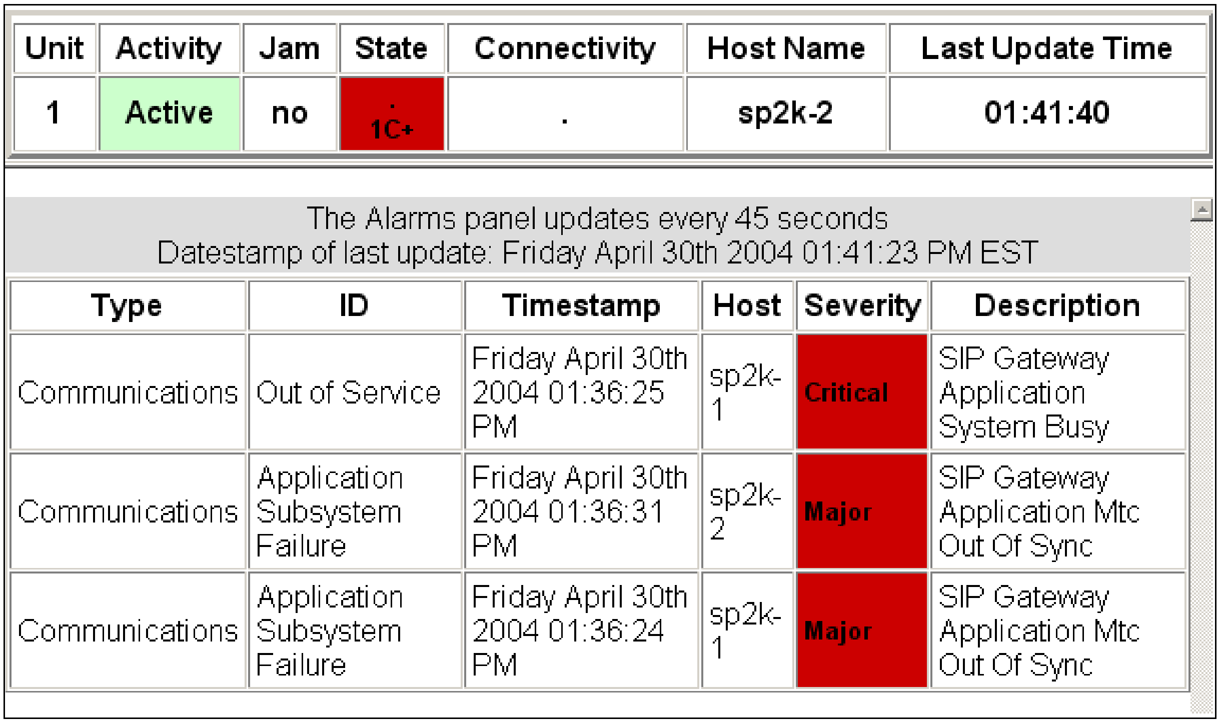
- performing routine maintenance and preventative maintenance tasks
- replacing faulty equipment as needed

Monitoring and managing alarms

The Session Server has the capability for SIP Gateway application or the system itself to generate alarms. These alarms can be viewed on the Session Server’s Alarm web page available from either web-based

GUI (see section Tools, utilities and user interfaces on page 12). Information about alarms includes the alarm type, identifier, time-stamp, the unit generating the alarm, the severity and description of the alarm. Refer to the following figure for a view of the alarms page.

View of the CS 2000 Session Server 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 Session Server 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 Session Server alarms as well as procedures on viewing alarms and associated logs, refer to the Session Server Fault Management NTP, NN10332-911.

Monitoring Logs

The Session Server has the capability for its applications or the platform itself to generate logs associated with alarms. There are five types of customer logs (CTRM, SIPS, SIPC, SIPM, DBSE, STGW and XTS logs) that 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.

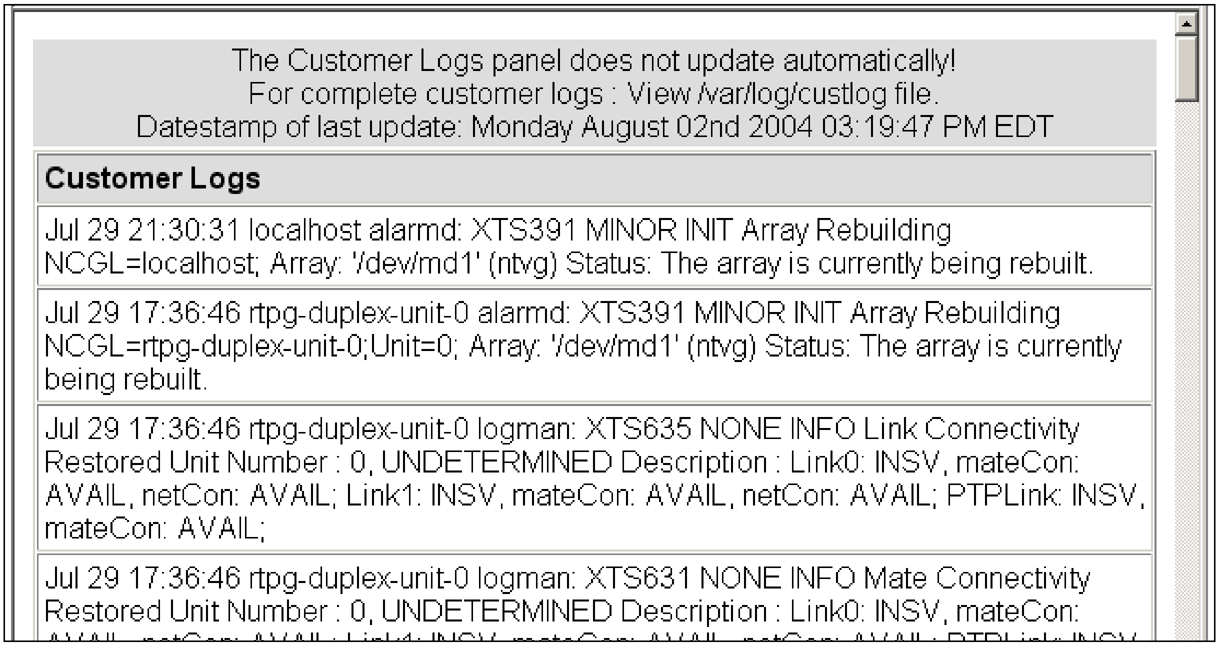
The Session Server can be configured to alter what log information is written to the local custlog file by redirecting log information to a remote log server and SNMP server using the NCGL commissioning tool.

If the Session Server is configured to transfer SNMP alarm traps to an OSS network, log reports related to the raising or clearing of alarms is only available on the Integrated EMS or other 3rd party OSS application, rather than on the logs view of the Session Server GUIs.

If the Session Server is configured to transfer logs to a remote log server, all logs that are ordinarily viewable from the Session Server 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 Session Server Manager. This view displays a maximum of the most recent 2000 line entries from the current custlog file. When viewing logs from an Integrated EMS system, log headers may differ slightly from what is shown in this view.

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



The Customer Logs panel does not update automatically!
For complete customer logs : View /var/log/custlog file.
Datestamp of last update: Monday August 02nd 2004 03:19:47 PM EDT

Customer Logs

```
Jul 29 21:30:31 localhost alarmd: XTS391 MINOR INIT Array Rebuilding NCGL=localhost; Array: '/dev/md1' (ntvg) Status: The array is currently being rebuilt.

Jul 29 17:36:46 rtpg-duplex-unit-0 alarmd: XTS391 MINOR INIT Array Rebuilding NCGL=rtpg-duplex-unit-0;Unit=0; Array: '/dev/md1' (ntvg) Status: The array is currently being rebuilt.

Jul 29 17:36:46 rtpg-duplex-unit-0 logman: XTS635 NONE INFO Link Connectivity Restored Unit Number : 0, UNDETERMINED Description : Link0: INSV, mateCon: AVAIL, netCon: AVAIL; Link1: INSV, mateCon: AVAIL, netCon: AVAIL; PTPLink: INSV, mateCon: AVAIL;

Jul 29 17:36:46 rtpg-duplex-unit-0 logman: XTS631 NONE INFO Mate Connectivity Restored Unit Number : 0, UNDETERMINED Description : Link0: INSV, mateCon:
```

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

For details about Session Server logs as well as procedures on viewing logs, refer to the Session Server Fault Management NTP, NN10332-911.

Performance management

Like other components in the Carrier VoIP environment, the Session Server 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 Session Server.

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

OM data recorded on one unit of a Session Server 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 Session Server node is installed in the network, OM data recorded by the first node is independent of that recorded by other Session Server 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 Session Server 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.

Operational administration

User administration is controlled though both the Session Server GUIs and the CLI. Procedures for managing users are found in the Session Server Security and Administration NTP, NN10346-611.

Upgrading the Session Server

In-service, major release upgrades of existing Session nodes from SN07 to SN08 is provided in the Session Server Upgrades NTP, NN10349-461

The NCGL platform software can be patched as well as upgraded by MR (maintenance release). The SIP Gateway application is upgraded by way of an MR. Refer to the Session Server Upgrades NTP, NN10349-461, for more information.

Customer support

Refer to the Basics NTP applicable to your Carrier VoIP solution to find information about support options and to Session Server order software.

Glossary of terms

The following terms and acronyms commonly, used in Carrier VoIP Networks and the Session Server component, are defined:

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 Succession 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

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 Mbit/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^{TM} Authentication Authorization Service

JRE
Java^{TM} Runtime Environment

JWS
Java^{TM} 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 Session Server 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

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$^{\text{TM}}$ operating system that has been enhanced to operate in a NEBS compliant telecom environment

NEBS
North American New Equipment Building Standard

NFS
Network File System

NGSS
Next Generation Session Server; another name for Session Server, a name sometimes seen in GUI or CLI outputs from the Session Server 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

PVG
Packet Voice Gateway

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

RTP
real-time transport protocol

SAM
System Application Module; SAM16 or SAM21

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.

SSPFS
Succession 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
an obsolete term for describing the Carrier VoIP or Nortel Networks brand

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

USP
Universal Signaling Point

VDRN
Virtual Routing Destination Node: is a type of GWC

VoIP
Voice over Internet Protocol

VPN
Virtual Private Network

XA-Core
Extended Architecture Core

XML
Extensible Markup Language