555-4031-903

Nortel Communication Server 2100

Session Initiation Procotol

Service Implementation Guide

SE08 Standard 01.03 May 2005

NORTEL

Nortel Communication Server 2100

Session Initiation Protocol

Service Implementation Guide

Publication number: 555-4031-903
Product release: SE08
Document release: Standard 01.03
Date: May 2005

Publication history

May 2005

Issue 01.03, Standard SE08.

January 2005

Issue 01.02, Draft SE08. Updated after internal review comments.

September 2004

Issue 01.01, Draft SE08. This is the first version of the document for internal review purposes.

Contents

About this document

Purpose and audience

This document describes the fundamentals behind the Session Initiation Protocol (SIP) and how to configure the protocol in a Communication Server 2100 network.

How to check the version and issue of this document

The version and issue of the document are indicated by numbers (for example, 01.01).

The first two digits indicate the version. The version number increases each time the document is updated to support a new software release. For example, the first release of a document is 01.01. In the next software release cycle, the first release of the same document is 02.01.

The second two digits indicate the issue. The issue number increases each time the document is revised but re-released in the same software release cycle. For example, the second release of a document in the same software release cycle is 01.02.

FOR MORE INFORMATION

To determine whether you have the latest version of this document and how documentation for your product is organized, check the release information in the *Meridian SL-100 Master Index of Publications*.

References in this document

Refer to the following documents for further information relevant to the topics discussed in this document:

- *Meridian SL-100/Communication Server 2100 Product Guide*, 555-4001-806
- *Meridian SL-100/Communication Server 2100 Application Planning Guide*, 555-4001-108

Introducing SIP on the Communication Server 2100

Overview

What is the Session Initiation Protocol?

The Session Initiation Protocol, or SIP, is an Internet Engineering Task Force (IETF) signaling protocol for establishing real-time calls and conferences over Internet Protocol networks. The Communication Server 2100 implementation is designed to be compliant with RFC3261. Each session can include different types of data such as audio and video, although currently most of the SIP extensions address audio communication. As a traditional text-based Internet protocol, it resembles the HyperText Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). SIP uses the Session Description Protocol (SDP) for media description (for more information about SDP, see "Appendix A: Session Description Protocol" on page 43).

SIP is independent of the packet layer. The protocol is an open standard and is scalable. It has been designed to be a general-purpose protocol.

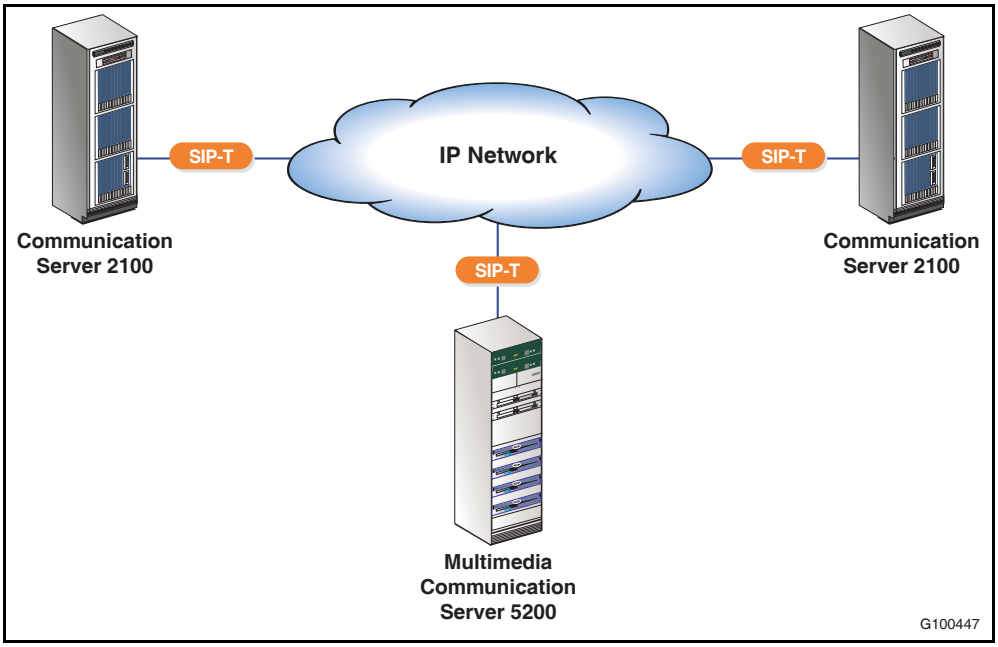
SIP implementation on the Communication Server 2100

SE08 introduces the ability to use SIP to connect a Communication Server 2100 to another Communication Server 2100 or a Nortel Multimedia Communication Server 5200 (MCS 5200).

Note: SIP lines are not supported in SE08.

SIP session characteristics are enabled through the use of network hosts to which users can transmit session information. Figure 1 on page 12 shows a sample Communication Server 2100 Session Initiation Protocol network configuration.

Figure 1
Communication Server 2100 SIP-based network



The Session Initiation Protocol implementation on the Communication Server 2100 provides the ability to integrate with other application servers, such as the Nortel Multimedia Communication Server 5200.

Note: In SE08, SIP can only be used between two Communication Server 2100s.

The software application offering this solution resides on the Communication Server 2100, Session Server platform. The Session Server provides a highly-available hardware, operating system and Operations, Administration, Maintenance and Provisioning (OAM&P) platform giving applications the reliability required by large enterprises. The application contains an interface that enables the platform to function with its Element Management System (EMS).

Session Initiation Protocol trunking

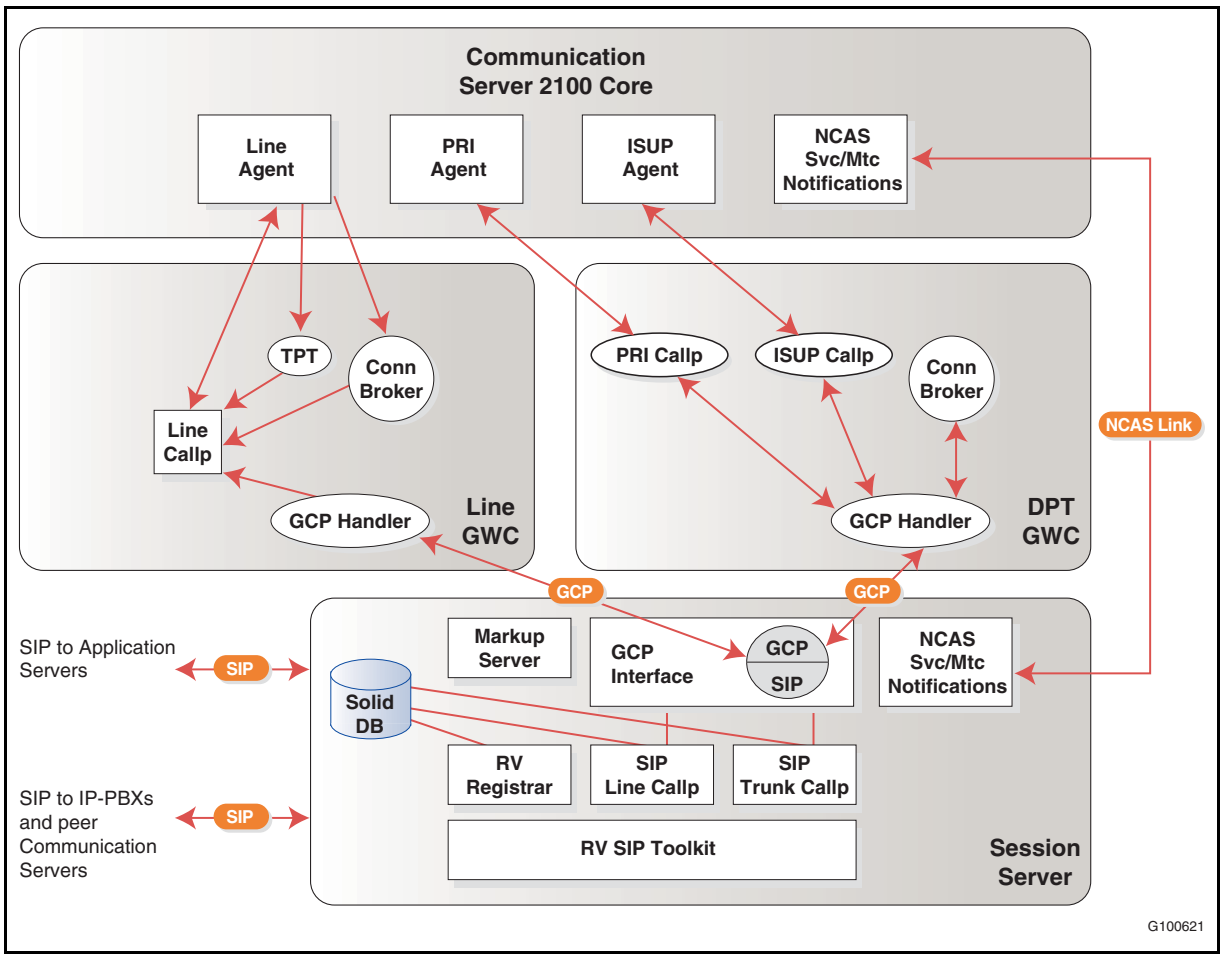
The Session Initiation Protocol virtual trunking application provides a direct speechpath between end users. This direct media approach eliminates unnecessary coding/decoding along the path, which was used in a traditional trunk world, and thus improves end-to-end voice quality.

Currently, IP-peer networking implemented on the Gateway Controller platform uses the H.323 protocol. However, in order to interwork with other latest SIP-enabled Nortel products, such as the Multimedia Communication Server 5200, a SIP-PRI gateway is required. However, the introduction of a SIP-PRI gateway increases network cost. Therefore, the Communication Server 2100 solution eliminates this interface and connects with other Nortel or third-party SIP applications directly. This section describes the modified IP-Peer Networking feature that is used to create this direct SIP interface.

The SIP trunking User Agent application consists of two hardware and software platforms. The first component resides on a Gateway Controller to tap into the translations and routing power of the Communication Server 2100 and provide an interface for the second component, the Session Server, to complete the User Agent interface. The second component is the Session Server which resides on a Hewlett Packard cc3310. The Hewlett Packard cc3310 is same platform as the Persistent Data Storage used for the Compact Communication Server 2100.

Figure 2 provides a logical view of the Communication Server 2100 hardware components.

Figure 2
Communication Server 2100 SIP components



This Session Server provides the following functions within the Session Initiation Protocol:

- User Agent
- registrar server
- presence server

SIP User Agent support for SS7

Overview

Starting in Release SE08, the Communication Server 2100 uses the Session Initiation Protocol (SIP) or SIP for Telephony (SIP-T) to support peer-to-peer signaling with other Communication Server 2100s and with SIP-enabled Media Gateway Controllers (MGCs), such as the Multimedia Communication Server 5200. The difference between SIP and SIP-T is that SIP-T messages convey encapsulated SS7 messages, while SIP messages do not. SIP-T, therefore, supports SS7 signaling directly, by enabling SS7 messages to be inserted in and extracted from SIP-T messages. SIP does not provide direct SS7 support, but SIP messages can be interworked with SS7 equivalents to provide indirect SS7 support. In this document, references to SIP should be taken to include SIP-T, unless this is otherwise indicated.

Typically, SIP-T is used for signaling between Communication Server 2100s, while SIP is used for signaling between the Communication Server 2100 and the Multimedia Communication Server 5200.

The Communication Server 2100 support for SIP functionality is provided by the Session Server, while SS7 functionality is provided by Dynamic Packet Trunk (DPT) Gateway Controllers. Session Server support for Session Initiation Protocol signaling and SS7 encapsulation is designed to be compliant with RFC 3261, which defines a SIP interface for open interoperability between communication servers and other network elements.

Communication Server 2100 support for Dynamic Packet Trunks

Dynamic Packet Trunks for inter-Communication Server signaling are supported by Dynamic Packet Trunk Gateway Controllers with no subtending units. DPTs are so called because trunk characteristics such as the ISUP protocol variant to be used are determined on the basis of the telephony profile of the selected route, which is downloaded to the DPT Gateway Controller during call establishment. For SIP-T, the telephony profile indicates the protocol characteristics of encapsulated SS7 signaling messages, which can be those of any supported ISUP variant. For SIP, the telephony profile indicates the SS7 protocol that is to be interworked with SIP. The telephony profile itself is selected on the basis of the far-end host name, as determined by translations and routing for an originating Communication Server 2100 or as indicated by the first incoming message for a terminating Communication Server 2100.

The DPT Gateway Controllers on a Communication Server 2100 provide a pool of resources that can be used for connections to any peer Communication Server 2100 or compatible Media Gateway Controller (MGC). The softswitch selects a DPT Gateway Controller and allocates it only for the duration of a given call, after which the Communication Server 2100 returns it to the pool for re-use. The fact that trunk group data for a selected DPT is downloaded to its DPT Gateway Controller only when the DPT is selected and allocated promotes efficiency in two ways:

- It is not necessary to provision inter-Communication Server trunks statically, which would involve estimating the proportion of traffic to be handled by each type of trunk, with the consequent risks of under-provisioning (leading to unnecessary congestion) or over-provisioning (with wasted capacity).
- It is not necessary for a Communication Server 2100 or peer Media Gateway Controller to know the IP addresses of all the DPT Gateway Controllers on another Communication Server 2100 with which it may need to communicate. Only a single target IP address on each remote Communication Server 2100 is required.

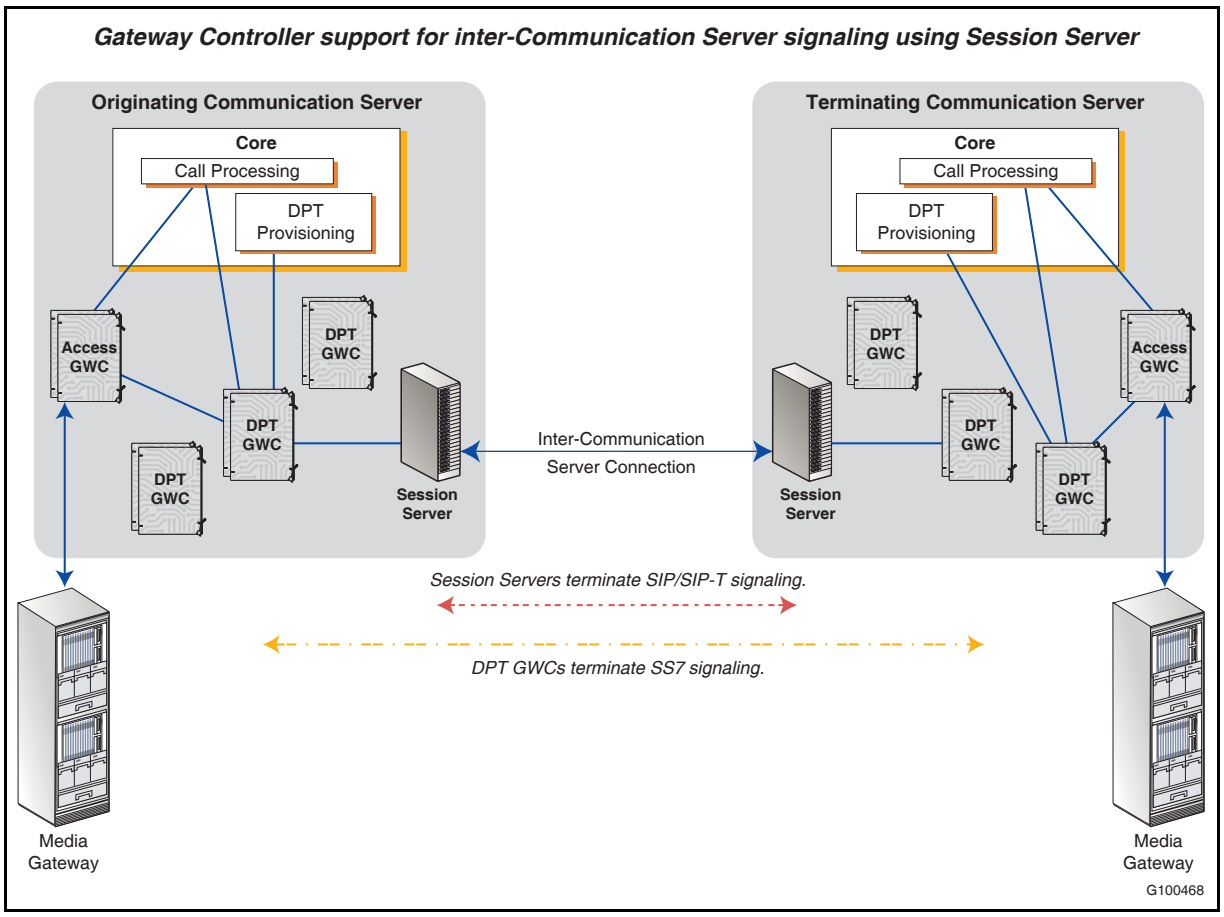
To support inter-Communication Server signaling, the operation of DPT Gateway Controllers is coordinated based on DPT Gateway Controllers interacting with the Session Server. In this implementation, SIP functionality is provided entirely by the Session Server. Specifically, the Session Server terminates SIP signaling and extracts SS7 signaling for the use of the DPT Gateway Controller.

Once a DPT Gateway Controller has been selected and provisioned, that Gateway Controller can communicate directly with the following:

- Session Server (co-ordination of messages with the Gateway Controller is through call ID).
- Call processing, which can identify the trunk using a standard terminal ID (as if it had been statically provisioned).
- The appropriate access Gateway Controller.

Figure 3 on page 17 shows how DPT Gateway Controllers interact with these other units to support inter-Media Gateway Controller communication using SIP/SIP-T.

Figure 3
DPT GWC interaction with other units to support peer-to-peer SIP signaling

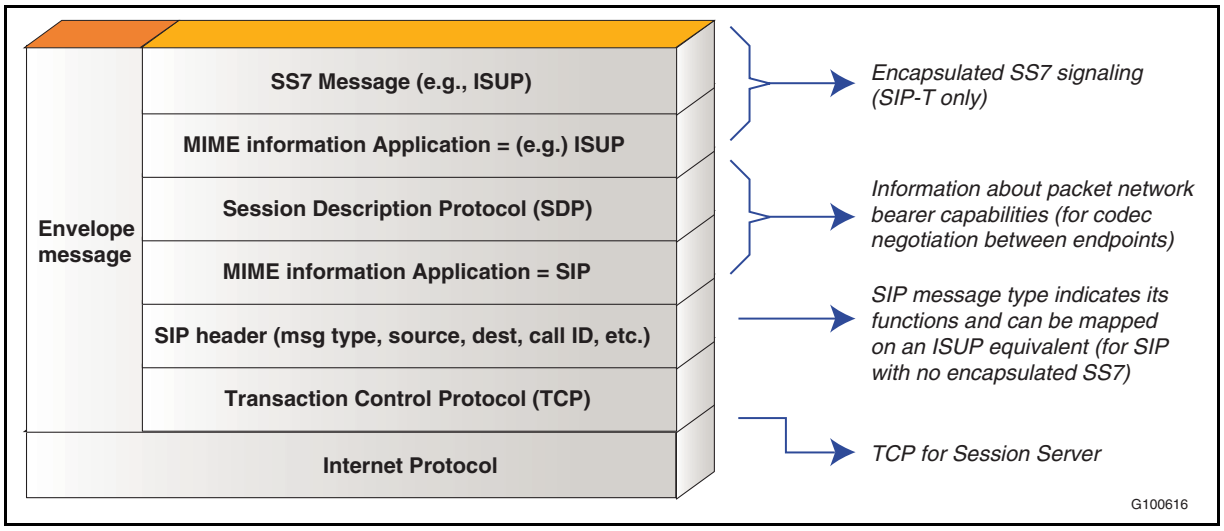


Session Initiation Protocol messages

Introduction

Figure 4 shows the structure of a complete GWC-to-GWC message, showing how SIP fits into the protocol stack and how a SIP/SIP-T message is used as an envelope for other types of signaling.

Figure 4
Structure of a complete SIP/SIP-T inter-CS message



The characteristics of SIP-T can be summarized as follows:

- SIP conveys information primarily by means of the message type used, which depends on the current state of the call and the call event being initiated or reported. Message content is kept to a minimum. SIP-T relies on the encapsulated SS7 user part message to convey all the signaling information needed for call processing.
- SIP and SIP-T both rely on the Session Description Protocol (SDP) to convey information about the media streams to be used in a session (call or conference) and the IP addresses of the participants.

- SIP-T messages are potentially able to convey any suitable user part messaging (for example, ISUP).
- SIP-T cannot convey SS7 Transaction Capabilities Application Part (TCAP) signaling across the packet network. The Communication Server 2100 supports TCAP Non Call Associated Signaling (NCAS) over an IP network by means of a TCAP/SCCP/MTP3/M2PA/SCTP/IP protocol stack terminated on the Universal Signaling Point (USP).
- SIP uses the Multipurpose Internet Mail Extensions (MIME) protocol defined in RFC 2046 to identify other protocols conveyed in SIP messages. The Communication Server 2100 supports the following combinations of media type and sub-type:

  — application/sdp

  — application/isup

  — application/tup

  — multipart/mixed

  The multipart/mixed payload type allows both SDP and SS7 information to be separately encapsulated in a single SIP-T message. In this case, the “application/sdp” and “application/isup” payload information is delimited by STANDARD BOUNDARY lines within the command body, as appears in the INVITE message.

  The MIME type specifies which SS7 protocol is being used, but a mechanism outside the SS7 protocol is required to convey the sort of additional information associated with trunk groups in the existing TDM telephony network (for example, customer group). This information is provided by the proprietary X-Nortel-Profile header in the SIP INVITE message. This header contains a text string (maximum 32 bytes) that represents a set of trunk characteristics (that is, maps to a trunk group). If this header does not appear in the message, a default trunk group will be selected, based on the SS7 protocol being used and the source Communication Server 2100.
- SIP messages are conveyed using the Transaction Control Protocol over IP for the Session Server implementation.

Message formats

The Communication Server 2100 implements format and length restrictions for SIP messages and parameters that support the capacity and performance required for a large-scale Media Gateway Controller. The Communication Server 2100 also implements extensions to the basic SIP-T message and header set.

General message rules

Communication Server 2100 conventions establish the following rules for SIP messages:

- Use the two ACSII characters “CR” (decimal value 13) and “LF”, in that order, for line breaks within a SIP message.
- Ignore unrecognized headers, whether or not defined in RFC 3542, when parsing a message.

  Note: This rule applies only if the unrecognized header complies with the general header field format.

- Do not exceed 143 characters (excluding the terminating CRLF) in the value length of individual headers.
- Do not use more that 20 headers in a single SIP message.

  Note: Notwithstanding this maximum, the SIP header block cannot exceed 2048 characters.

- Do not repeat headers within a SIP message.

  Note: In the case of a repeated header, the Communication Server 2100 only uses the first instance of the header.

- Do not use more than three message payloads in an individual SIP message.

  Note: A message payload cannot exceed 300 bytes.

Uniform Resource Identifiers

The Session Initiation Protocol Uniform Resource Identifier (URI) supports user, password, host and port fields using the following format:

“sip:”[user[“;”password]”@”]host[“:”port]

The user, password and host fields are character arrays with a maximum of 32 bytes each. The port field uses an unsigned integer. Escaped characters (escape+ character) are not supported.

The Communication Server 2100 implementation of the Session Initiation Protocol Uniform Resource Identifier only uses the host field. This reduces the format to the following main body:

“sip:”host

Communication Server message parsing discards any parameters following the main body of the Uniform Resource Identifier, including semi-colon delimiters.

Start line requirements

Support for the start line requirements is different between request messages and response messages. The requirements for the start line of a request message depend on the methods supported and the restrictions set by the Session Initiation Protocol Uniform Resource Indicator. The length of the **<progress-indication>** string determines the limitations for the start line of a response message.

Header requirements

Table 1 describes the header types and requirements that Communication Server 2100 Session Initiation Protocol messages use.

Table 1
SIP message header types (Sheet 1 of 3)

Header	Description
To	This mandatory header contains the identity of the destination Media Gateway Controller in Session Initiation Protocol Uniform Resource Identifier format. The Communication Server 2100 discards any additional parameters when parsing the To header.
From	This mandatory header contains the identity of the source Media Gateway Controller in Session Initiation Protocol Uniform Resource Identifier format. The Communication Server 2100 discards any additional parameters when parsing the From header.

Table 1
SIP message header types (Sheet 2 of 3)

Header	Description
Call-ID	This mandatory header provides a unique identification for a call leg. The header value is a character array with a length that cannot exceed 64 bytes. The header value consists of the following three segments: • An ASCII character string that acts as a unique identifier for the hardware unit that generated the call. This string cannot exceed 16 characters and can use any printable US ASCII character, except for the dash. ***Note:*** The dash is a reserved character that separates the first segment from the second. • A timestamp consisting of five two-digit fields each, separated by a colon. These fields represent the day, hour, minute, second and centisecond respectively. • A character string that gives the local host name. The character string cannot exceed 32 characters. ***Note:*** An @ must precede this string. ***Example:*** **0057.4002-17:10:22:59.99@wst.nortelnetorks.com**
Call Sequence	This mandatory header contains the request method and a single decimal sequence number that is unique within a call leg. The Communication Server 2100 supports Call Sequence (CSeq) headers that do not contain method information.
Content-Length	This header is mandatory when the SIP message contains a MIME body. In this case, the Content-Type header describes the MIME body content. The Communication Server 2100 supports the following media types and sub-types: • application/sdp • application/isup • application/tup • multipart/mixed • The Communication Server 2100 implements the multipart/mixed payloads in accordance with IETF RFC 2046.

Table 1
SIP message header types (Sheet 3 of 3)

Header	Description
Content-Length (continued)	The Communication Server 2100 Content-Type header also supports the following parameters: • For session description payloads, the “Charset” parameter specifies the character set in use. ***Example:*** **text/html;charset=ISO-8859-4** • For user part payloads (for example, ISUP), the following parameters specify particular variants: — base parameter — version parameter • For multipart message bodies, a string unique to the message body content separates the different payloads. The boundary parameters specify this string. ***Note:*** In every case, the parameter value is a character array that cannot exceed 20 bytes.
Require	This general header describes the options that the client expects the User Agent server to support in order to process the request properly. The header value is a character array that cannot exceed 32 bytes.
Supported	This general header lists User Agent capabilities. The header value is a character array that cannot exceed 32 bytes.
Unsupported	This response header lists capabilities that the server does not support. The header value is a character array that cannot exceed 32 bytes.
X-Nortel-Profile	This Nortel-specific extension header describes the telephony trunk group information within the SIP INVITE message. The header value is a character array that cannot exceed 16 bytes.

SIP-T variant

SIP for Telephony (SIP-T) is a collection of internal drafts from the SIP working group in the IETF that extend the Session Initiation Protocol to support inter Media Gateway Controller communications. One of the main requirements for SIP-T is to support “SIP bridging” or PSTN signaling transparency. SIP-T directly negotiates a media connection between gateways. Endpoint information is carried in Session Description Protocol form which can describe the IP endpoints.

SIP-T uses the following two methods:

- Maps ISUP message contents to fields in the SIP header for interworking with pure SIP agents.
- Encapsulates ISUP messages within the SIP message body for SIP bridging.

SIP-T message example

Figure 5 shows an example of a SIP-T message.

Figure 5
Example SIP-T INVITE message

```
INVITE sip:15068324444@hampt.nb.com SIP/2.0
From: sip:15068321234@hampt.nb.com SIP/2.0
To: sip:15068324444@hampt.nb.com
Call-ID: 0094.4609-28-17-05-18.82@hampt.nb.com
Content-Type: Application/Multipart
Content-Length: 327
User-agent: CS 2100/8.0
Mime-Version: 1.0
Content-Type: multipart/mixed ;boundary=unique-boundary-1

--unique-boundary-1
Content-Type: application/sdp; charset=ISO-10646

v=0
o=ehampton 1890844526 1890844526 IN IP4 47.174.73.241
s=SDP Seminar
c=IN IP4 MG122.nb.com
t=2873397496  2873404696
m=audio 9092 RTP/AVP 0 3 4

--unique-boundary-1
Content-Type: application/isup; version=etsi356

01 00 60 00 0a 00 02 0a 08 03 90 53 02 18 60 00 f4 0a 07 03 13 81
81 01 06 10 3d 01 1f 31 02 00 00 39 04 3d c0 31 c0
--unique-boundary-1
```

SIP-T messages build on SIP messages with the following enhancements:

- Multipart MIME types are used to allow both an SDP payload and an ISUP payload to appear in the same message.
- The application/isup MIME type identifies the ISUP version being carried.
- In this example, the To and From headers contain a SIP URI with both the PSTN subscriber number and the name of the Media Gateway Controller where the call is routed.

Session Server

Description

The Session Server is a software application that provides inter operability with third-party application servers and softswitches. The Communication Server 2100 uses the Session Server to interact with Dynamic Packet Trunk Gateway Controllers to support peer-to-peer communication across the packet backbone network using SIP/SIP-T signaling. Session Server support for SIP signaling and SS7 encapsulation is designed to be complaint with RFC 3261, which defines a SIP interface for open inter operability between communication servers and other network elements.

The Communication Server 2100 supports peer-to-peer signaling with other Communication Server 2100s and with other compatible Media Gateway Controllers such as the Multimedia Communication Server 5200.

Dynamic Packet Trunks for inter-Communication Server signaling are supported by Dynamic Packet Trunk Gateway Controllers with no subtending units. Dynamic Packet Trunks are so called because trunk characteristics such as the ISUP protocol variant to be used are determined on the basis of the telephony profile of the selected route. The telephony profile is downloaded to the Dynamic Packet Trunk Gateway Controller during call establishment. For SIP-T, the telephony profile indicates the protocol characteristics of encapsulated SS7 signaling messages, which can be any ISUP or TUP variant. The telephony profile is selected on the basis of the far-end host name, as determined by translations and routing of an originating Communication Server 2100 or as indicated by the first incoming message for a terminating Communication Server 2100.

The role of the Session Server is to terminate SIP signaling and present SS7 signaling to the Dynamic Packet Trunk selected for a given call. See Figure 3 on page 17 for an illustration of the interaction between Dynamic Packet Trunk Gateway Controllers and the Session Server.

The Session Server consists of a Network Equipment Building Systems (NEBS) Level 3 compliant hardware platform, plus a software framework and architecture for developing carrier-grade applications and services. The hardware platform is the Hewlett Packcard HP-CC3310, which provides processing, memory and disk capacity for Call Agent card Storage Management (STORM), SIP and SIP applications. The base layer of Session Server software uses the Nortel Carrier Grade Linux (NCGL) layer which includes the Linux kernel.

The architecture of the Session Server consists of a mated pair of Services Application Module Extreme Thin Server (XTS) with a configuration similar to that of a Gateway Controller. The Session Server consists of an active and inactive unit. Each unit in reality is a fully-functional Session Server that is interconnected using a gigabit Ethernet LAN as shown in Figure 6 on page 29. Each server provides processor capacity, local disk storage and high-bandwidth network connectivity.

Each server is equipped with the following:

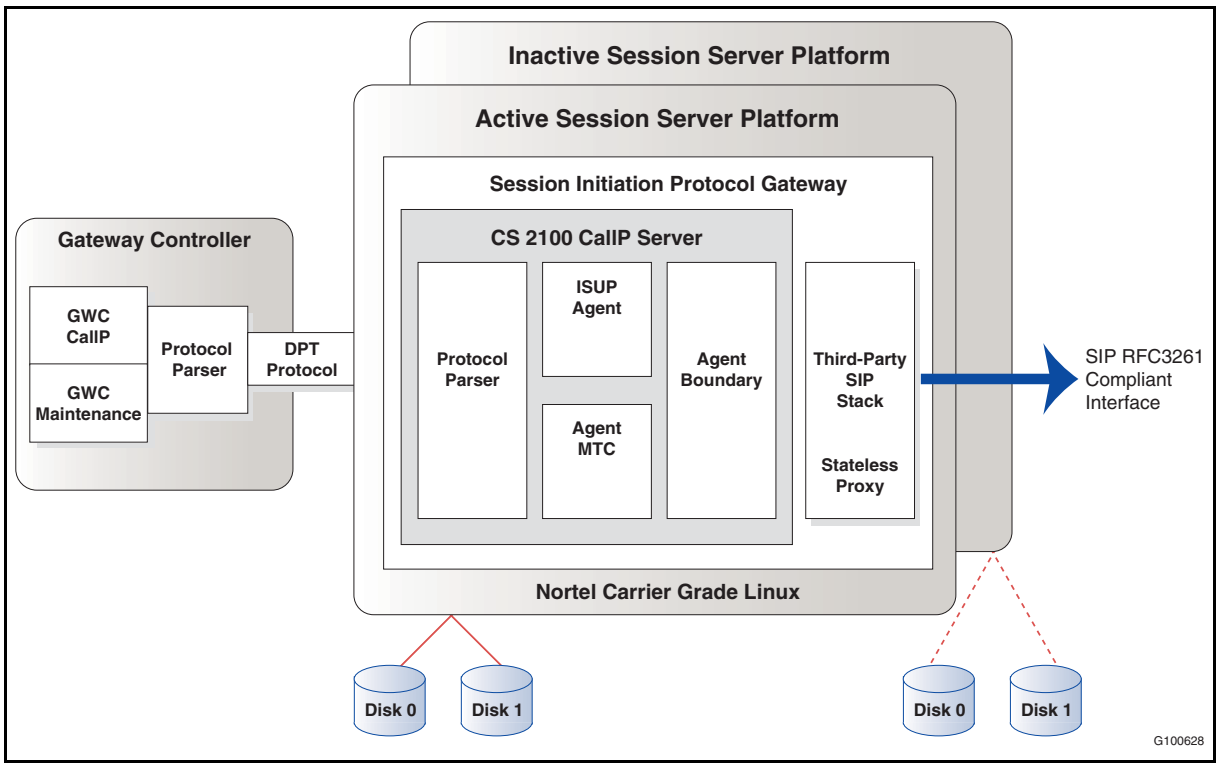
- One or two GHz Pentium 4 Xeon processors with 512 Kbyte integrated cache.
- Support for a maximum of 12 Gbytes of memory using up to six memory modules.
- Support for up to two Small Computer System Interface (SCSI) hard disk drives with 36/73/146 Gbytes storage.
- Multiple GigE copper interfaces; two on board and two-port Network Interface Card (NIC).
- Two 10/100/1000BaseT Ethernet ports for LAN connections.

The field replaceable components on the Session Server are as follows:

- hard disk
- power supply
- CD drive

Figure 6 on page 29 provides a high-level logical view of the Session Server's role in the Communication Server 2100 network.

Figure 6
Mated pair Session Server logical configuration

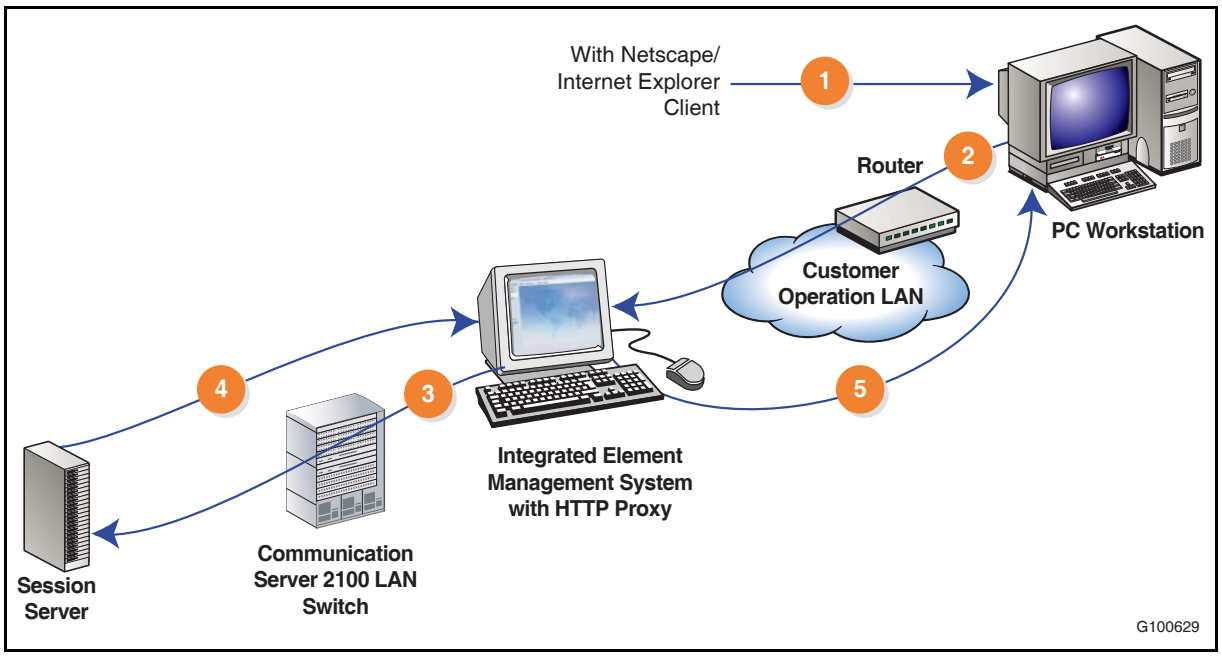


Management platform

The Session Server Manager is a web-based interface residing on the Session Server to perform the provisioning and maintenance activities. This interface consists of a web system running on the Session Server Manager that provides provisioning web pages, as well as maintenance related web pages.

The Session Server can be configured to use the Integrated Element Management System (IEMS) between the customer operation LAN and the Communication Server 2100 LAN or it can be configured without the Integrated Element Management System. Figure 7 on page 30 shows a sample configuration with Integrated Element Management System, where the HyperText Transfer Protocol (HTTP) configured on the IEMS redirects the web browser to the Session Server.

Figure 7
Session Server managed by Integrated Element Management System



Configuration steps for the sample configuration in Figure 7 include the following:

1 The user points the browser to web link on the Integrated Element Management System.

2 The Integrated Element Management System invokes HTTP.

3 HTTP on the Integrated Element Management System redirects the link to the Session Server.

4 The Session Server replies back to the Integrated Element Management System.

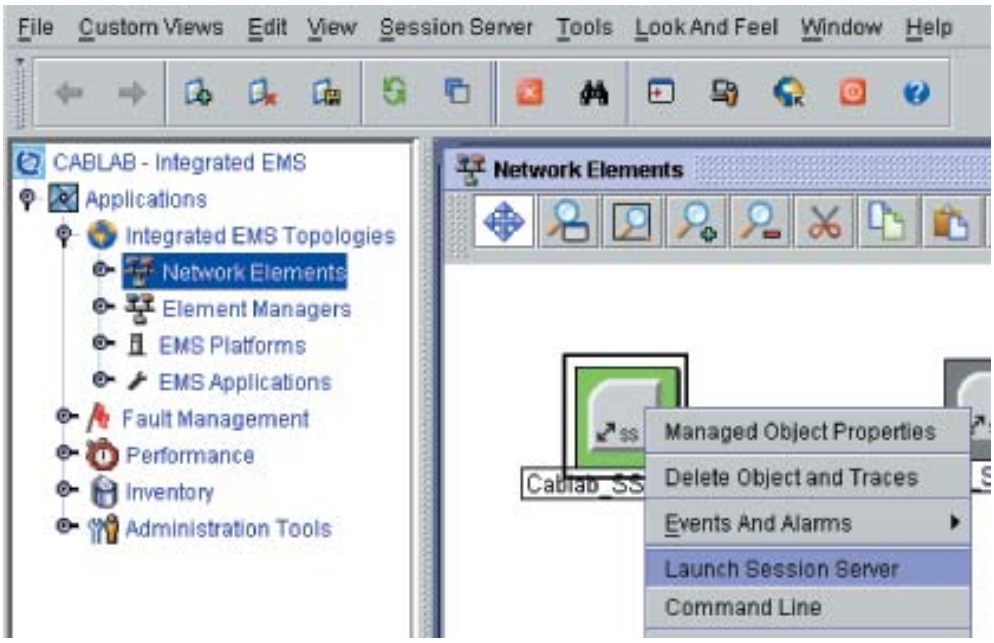
5 The Integrated Element Management System responds to the user request.

FOR MORE INFORMATION

See the *Meridian SL-100/Communication Server 2100 Product Guide* for additional information about the Integrated Element Management System.

Figure 8 on page 31 shows where to access the Session Server Manager from the IEMS Graphical User Interface.

Figure 8
Launching the Session Server from the IEMS



Session Server interfaces

The SAM-XTS is configured with four Gigabit Ethernet ports. Each Session Server is configured with two 1000 Mbs/100 Mbs/10 Mbs (depending on the IP router configuration) interfaces directed to the LAN switch. In addition, two interfaces connect unit 0 to unit 1.

Protocols supported by the Session Server

The Session Server supports SNMP V3 with “No Privacy” and “No Authentication” options. Additionally, the following protocols are supported to provide access to the server:

- Simple File Transfer Protocol (SFTP) or Signaling Control Protocol (SCP)
- Secure Shell (SSH), including
  - — Triple Data Encryption Standard (3DES) 168 bits
  - — Blowfish 128 bits
  - — Twofish 128 bits
  - — Advanced Encryption Standard (AES) 128 bits
- HTTP
- HyperText Transfer Protocol, Secure (HTTPS)

References

Table 2 shows where you can find more detailed information about the Session Server.

Table 2
Documentation references

Document title	Document number
Session Server Configuration Basics	NN10333-111
Session Server Upgrades	NN10359-461
Session Server Configuration Management	NN10338-511
Session Server Security and Administration	NN10346-611
Session Server Performance Management	NN103342-711
Session Server Fault Management	NN10332-911

Configuration procedures

This chapter describes the procedures for configuring the Session Initiation Protocol in a Communication Server 2100 network.

Introduction

The technician must enter the following information from the Element Management System (EMS):

- Type of server
- Network information
- Mate application information
- Supported services
- Service triggering mechanisms

Procedure references

The procedures for configuring SIP are described in several existing documents. Table 3 lists the procedures required to configure SIP and shows where you can find more detailed information about the procedures. The table also includes some maintenance and administration procedures.

Table 3
Communication Server 2100 SIP procedures (Sheet 1 of 2)

Procedure	Reference
Provisioning SIP-T DPTs in an office with a Session Server.	*Communication Server 2000 Configuration Management,* NN10193-511
Add and configure a GWC node, *or* Change the service profile of a Gateway Controller node.	*Gateway Controller Configuration Management,* NN10205-511
Disassociate a media gateway (if you want to remove a SIP node).	*Gateway Controller Configuration Management,* NN10205-511

Table 3
Communication Server 2100 SIP procedures (Sheet 2 of 2)

Procedure	Reference
Table SERVSINV.	*Succession Networks Operational Configuration: Data Schema Reference,* NN10324-509
Various procedures relating to the maintenance of the Session Server.	*Session Server Fault Management,* NN10332-911
Various procedures relating to the configuration and administration of the Session Server.	*Session Server Configuration Management,* NN10338-511
View Session Server Operational Measurements by OM Group.	*Session Server Performance Management,* NN103342-711
Session Server Installation	*CS2000 Session Server Installation and Commissioning* (SN07/SN08): Installation Method 35-0122
Engineering Guidelines	SEB-08-00-017 SN08.x *Engineering Rules CS2000 Session Server*

Application logs

Description

Table 4 provides a brief description of the Session Server/SIP logs. For mroe detailed explanations and receommeded actions, see *Succession Fault Mangement Log Reference (volume 3),* NN10275-909.

Table 4
Session Server/SIP log summary (Sheet 1 of 4)

Log ID	Description
DBSE300	Generated any time a change in database connectivity is detected.
SIPC301	Generated when the SIP Gateway Call Processing Application will not receive any incoming SIP messages.
SIPC550	Generated when a Critical alarm is generated to a loss of connectivity between the database and the CallP application.
SIPC650	Generated when the SIP Gateway Call Processing Application goes to get data from the database for a particular table and no data is found.
SIPC750	Generated when the SIP Gateway Call Processing Application drops incoming SIP messages due to Access Control List restrictions.
SIPM300	Generated by the SIP Gateway application maintenance process for a variety of unexpected reasons or conditions.
SIPM301	Generated when the SIPM301 critical alarm is raised.
SIPM302	Generated when SIP Gateway application state goes out of sync between the two Session Server units.
SIPM500	Generated with a SIP Maintenance State Change.
STGW700	Generated when callp activity is interrupted or negatively impacted.

Table 4
Session Server/SIP log summary (Sheet 2 of 4)

Log ID	Description
XTS300	Indicates that memory resources are low or near exhaustion.
XTS301	Indicates that the CPU load average for one or more time segments has exceeded a preset threshold.
XTS302	Indicates that free space on the root file system is low.
XTS303	Indicates that at least one software process has terminated abnormally and may retain system resources such as memory space or CPU usage.
XTS305	Indicates that the platform software lost time synchronization to one or more Network Time Protocol (NTP) servers, or the drift, is excessive.
XTS306	Indicates that CPU utilization has exceeded a preset threshold.
XTS309	Indicates that a peripheral hardware component has a PCI bus fault, Error Checking and Correction (ECC) memory fault, or a parity error.
XTS315	Indicates that the standby call processing application on the inactive Session Server is not ready for takeover.
XTS316	Indicates that the standby call processing application is out of service and the Session Server node is not operational.
XTS331	Indicates that the Session Server active unit cannot communicate to the mate unit through the ethernet connections.
XTS335	Indicates that one of PTP ethernet interfaces is down.
XTS336	Indicates that one or more ethernet links are unable to communicate with the network.
XTS351	Indicates a response to several CON and APL alarms.
XTS355	Indicates the inactive unit is jammed to prevent a Switch of Activity (SWACT).
XTS391	Indicates that a disk drive has certain major or minor alarms.
XTS392	Indicates a error result has been returned from regularly occurring NGCL audit testing for any of a number of conditions.
XTS395	Indicates a error result has been returned from regularly occurring NCGL file system audit tests.
XTS600	Generated by the NCGL operating system when all the conditions which raised alarm XTS300 have been cleared.

Table 4
Session Server/SIP log summary (Sheet 3 of 4)

Log ID	Description
XTS601	Generated by the NCGL operating system when all the conditions which raised alarm XTS301 have been cleared.
XTS602	Generated by the NCGL operating system when all the conditions which raised alarm XTS302 have been cleared.
XTS603	Generated by the NCGL operating system when all the conditions which raised alarm XTS303 have been cleared.
XTS605	Generated by the NCGL operating system when all the conditions which raised alarm XTS305 have been cleared.
XTS606	Generated by the NCGL operating system when all the conditions which raised alarm XTS306 have been cleared.
XTS609	Generated by the NCGL operating system when all the conditions which raised alarm XTS309 have been cleared.
XTS615	Generated by the NCGL operating system when all the conditions which raised alarm XTS315 have been cleared.
XTS616	Generated by the NCGL operating system when all the conditions which raised alarm XTS316 have been cleared.
XTS631	Generated by the NCGL operating system when all the conditions which raised alarm XTS331 have been cleared.
XTS635	Generated by the NCGL operating system when all the conditions which raised alarm XTS335 have been cleared.
XTS636	Generated by the NCGL operating system when all the conditions which raised alarm XTS336 have been cleared.
XTS651	Generated by the NCGL operating system when all the conditions which raised alarm XTS351 have been cleared.
XTS655	Generated by the NCGL operating system when all the conditions which raised alarm XTS355 have been cleared.
XTS670	Generated by the NCGL operating system when a SWACT of the system has been initiated.
XTS671	Generated by the NCGL operating system when a SWACT of the system has been completed.
XTS691	Generated by the NCGL operating system when all the conditions which raised alarm XTS391 have been cleared.

Table 4
Session Server/SIP log summary (Sheet 4 of 4)

Log ID	Description
XTS692	Generated by the NCGL operating system when all the conditions which raised alarm XTS392 have been cleared.
XTS695	Generated by the NCGL operating system when all the conditions which raised alarm XTS395 have been cleared

Operational Measurements

Session Server OM group and register descriptions

This section describes the following OM groups that a technician can use to monitor Gateway Controller performance:

- SIPGW_CALLP
- SIPGW_SERVICES
- SIPGW_MISC

The following tables offer register details for each of these OM groups.

Table 5
OM registers for group SIPGW_CALLP

Registers	Description	Register Type
IC_CALL_ATTEMPTS	Total number of incoming call attempts.	peg-type
OG_CALL_ATTEMPTS	Total number of outgoing call attempts.	peg-type
CALLS_ANSWERED	Total number of calls answered.	peg-type
CALLS_ABANDONED	Total number of calls abandoned.	peg-type
CALLS_REJECTED	Total number of calls rejected.	peg-type
CALLS_REDIRECTED	Total number of calls redirected.	peg-type

Table 6
OM registers for group SIPGW_SERVICES (Sheet 1 of 2)

Registers	Description	Register Type
REFER_ATTEMPTS	Total number of refer attempts.	peg-type
REFER_SUCCESS	Total number of successful refers.	peg-type

Table 6
OM registers for group SIPGW_SERVICES (Sheet 2 of 2)

Registers	Description	Register Type
IC_DTMF_SUBSCRIBES	Total number of incoming DTMF subscribes.	peg-type
OG_DTMF_SUBSCRIBES	Total number of outgoing DTMF subscribes.	peg-type
IC_DTMF_NOTIFYS	Total number of incoming DTMF notifies.	peg-type
OG_DTMF_NOTIFYS	Total number of outgoing DTMF notifies.	peg-type
IC_FAX_SUBSCRIBES	Total number of incoming fax subscribes.	peg-type
OG_FAX_SUBSCRIBES	Total number of outgoing fax subscribes.	peg-type
IC_FAX_NOTIFYS	Total number of incoming fax notifies.	peg-type
OG_FAX_NOTIFYS	Total number of outgoing fax notifies.	peg-type

Table 7
OM registers for group SIPGW_MISC

Registers	Description	Register Type
TCP_CALLS	Total number of TCP calls.	peg-type
UDP_CALLS	Total number of UDP calls.	peg-type
SIP_MSG_SEND_FAILURES	Total number of SIP message send failures.	peg-type
INCOMING_SDP_INCOMPATIBLE	Total number of incoming incompatible SDPs from remote SIP servers.	peg-type
OUTGOING_SDP_INCOMPATIBLE	Total number of outgoing incompatible SDPs from remote SIP servers.	peg-type

Additional Operational Measurements

There are many other Operational Measurements that can relate to SIP on the Communication Server 2100. For more information, see *Succession Performance Management Operational Measurements Reference,* NN10264-709. The following are a couple of examples:

- DPTNODE – OM group Dynamic Packet Trunk Node (DPTNODE) measures DPT usage of a Gateway Controller (GWC). DPTNODE contains registers that maintain terminal usage and failure counts. For GWC nodes, the info field contains the DPT protocol (BICC or SIP-T) associated with the GWC as data filled in the SERVSINV table.
- DPTOFCP – OM group Dynamic Packet Trunk Office Protocol (DPTOFCP) measures DPT protocol (BICC and SIP-T) performance for an entire office.

Appendix A: Session Description Protocol

The Session Initiation Protocol uses the Session Description Protocol for media description. As such, this Appendix is included in this document for background information.

Functional overview

Session Description Protocol (SDP) session description signaling is used to complement both Gateway Controller to gateway signaling and inter-Communication Server signaling by specifying media stream characteristics and address information, particularly for use in codec negotiation. SDP is an IETF protocol and conveys IP address information as specified in RFC 2327.

The Communication Server 2100 conveys Session Description Protocol information in one of the following ways:

- When used to complement GWC-gateway signaling using H.248, ASPEN, Network-based Call Signaling (NCS) or Media Gateway Control Protocol (MGCP), SDP information is provided inside the device/media control messaging.
- When used to complement SIP/SIP-T inter-Communication Server signaling, the Multi-purpose Internet Mail Extensions (MIME) mechanism used to encapsulate SS7 messages (ISUP) in SIP-T messages is used in a similar way to encapsulate SDP information. SS7 and SDP can both be conveyed (but separately packaged) within a given SIP-T message.

An SDP session description comprises the following:

- Information about the media stream(s) to be used in a call or conference such as:
  - Media type (for example, audio, video or data)
  - Transport protocol (for example, User Datagram Protocol or Real-time Protocol)
  - Media format (for example, A-law Pulse Code Modulation or MPEG-2 video)
- Address information for the sending and receiving of packets by participants, which for the Communication Server 2100 consists of IP addresses and UDP port numbers.

A session description can also include timing information (for example, start/stop times and session repetition details).

Network role

SDP session description signaling complements both GWC-gateway media control signaling and inter-CS signaling, as follows:

- **SDP with GWC-gateway media control signaling using H.248, ASPEN, NCS or MGCP**

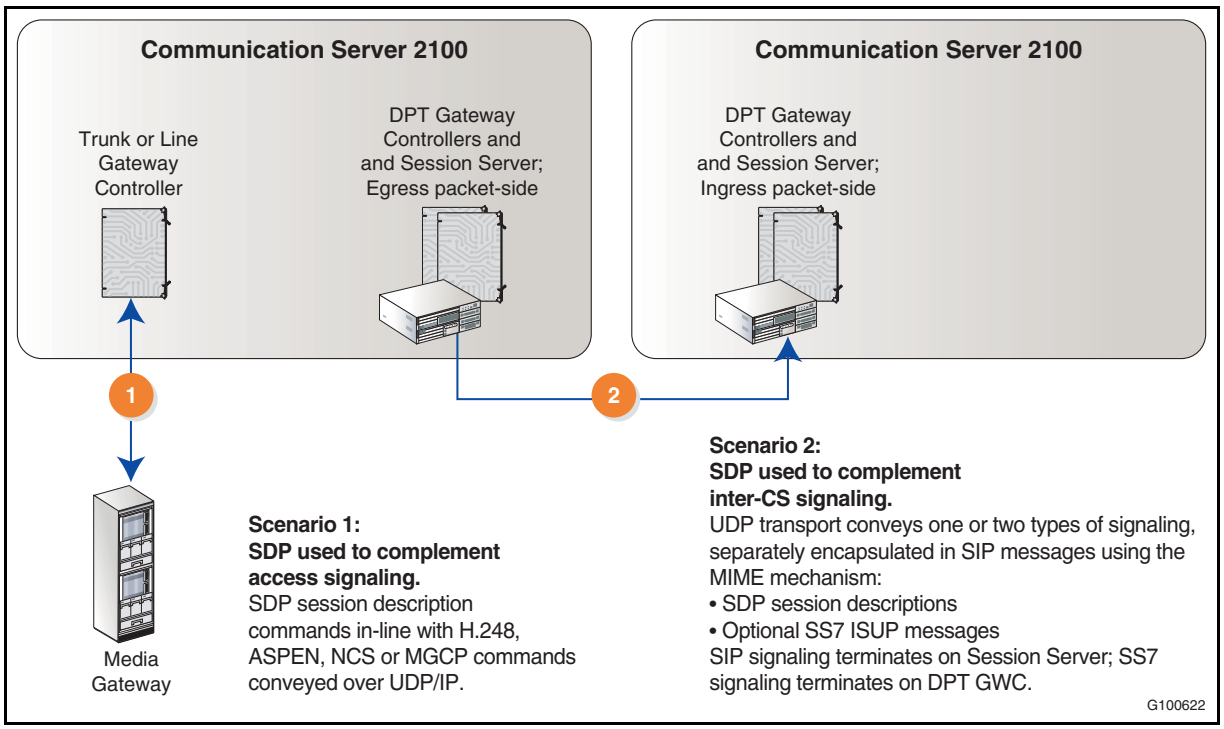
  Session Description Protocol commands are provided in-line with device/media commands sent between Gateway Controllers and media gateways. Typically, SDP commands sent by the Gateway Controller specify the requirements for a call, while SDP commands sent by the media gateway provide information about the capabilities available at the gateway.

- **SDP with inter-Communication Server signaling using SIP**

  SDP commands are encapsulated using the MIME mechanism and conveyed in SIP messages. In the case of SIP-T, SDP is conveyed along with similarly, but separately, encapsulated SS7 messages. Typically, the originating Communication Server passes on information about requirements, as provided by the ingress TDM-side Gateway Controller to the egress packet-side Gateway Controller, while the terminating Communication Server returns information about capabilities available.

Figure 9 on page 45 illustrates the two different roles of SDP session description signaling. In the handling of a given call, SDP can be involved in either or both roles.

Figure 9
Use of SDP to complement access signaling and/or inter-CS signaling



Command syntax

SDP is a text protocol consisting of text lines of the format

type = value

where

type is a single letter
value is a text string whose format depends on type

A session description consists of a session-level description (details that apply to the whole session and all media streams) and optionally several media-level descriptions (details that apply only to a single media stream and override corresponding session-level data). The session level description appears first, beginning with the v(ersion) type, and is terminated when the first (or only) media-level description appears. Each media description starts with an m(edia name).

The order of the SDP text lines in a session description is fixed. Optional lines can be omitted, but the lines included in a session description must always appear in the same order. This simplifies parsing.

Table 8
SDP session description lines and their use (Sheet 1 of 2)

Type	Meaning	Format/Content	Mandatory/ Optional
Information applicable to all media streams in a session			
v	Version	SDP version number	Mandatory
o	Originator	UserID and host address [1] of session originator	Mandatory [2]
s	Session	Session name	Mandatory [2]
i	Information	Information about session (descriptive text string)	Optional
u	URI	Universal Resource Identifier of session description	Optional
e	Email	Email address of session originator	Optional
c	Connection	Target address [1]	Mandatory
b	Bandwidth	Bandwidth information	Optional
z	Zone	Time zone information	Optional
k	Key	Encryption key	Optional
a	Attributes	Payload type (denoted by numeric identifier) and algorithm (for example, G.711a for A-law PCM)	Optional
t	Time	Start time of session (0 for immediate start)	Mandatory [2]
r	Repetition	Repetition information (for example, initiate session weekly)	Optional
Information applicable to one media stream within a session (overriding session information)			
m	Medium	Media stream description, comprising: • Media type (typically audio in SNH01) • Destination port • Transport protocol (for example, UDP or RTP) • Media format (numeric identifier of payload type)	Mandatory
i	Information	Information about media stream (descriptive text string)	Optional

Table 8
SDP session description lines and their use (Sheet 2 of 2)

Type	Meaning	Format/Content	Mandatory/ Optional
c	Connection	Target address [1]	Optional
b	Bandwidth	Bandwidth information	Optional
k	Key	Encryption key	Optional
a	Attributes	Payload type (denoted by numeric identifier) and algorithm (for example, G.711a for A-law PCM)	Optional

Note 1: Address comprises network type, address type and address. For an IP network, these are IP, IP4 and IP address respectively.

Note 2: Although defined as mandatory in the SDP specification, this is not supported by the CS 2100.

The most important SDP types are described below.

O (Originator)

Identifies the originator of the session (username and user's host address as follows:

o = username session-id version network-type address-type address

where

username is the user's login at the originating host
address is the address of the host creating the session and is of the type specified by *address-type*
network-type is IN (meaning Internet)

C (Connection)

Identifies the address to which data is to be sent as follows:

c = network-type address-type connection-address

where

network-type is IN (meaning Internet)
connection-address is the target address and is of the type specified by *address-type*

M (Medium)

Indicates the media format supported by the sender as follows:

m = media port transport format-list

where

media is the media type (for example, audio or video)
port is the port to which packets should be sent
transport is transport protocol (for example, UDP, RTP or H.323)
format-list gives the media format (for example, A-law PCM, MPEG-2 video)

List of terms

3DES	Triple Data Encryption Standard
ACM	Address Complete Message
AES	Advanced Encryption Standard
ANM	Answer Message
API	Application Programming Interface
ASPEN	Automatic System for Performance Evaluation of the Network
CallP	Call Processing
CS 2100	Communication Server 2100
CS LAN	Communication Server LAN
CSeq	Call Sequence
DPT	Dynamic Packet Trunk
EMS	Element Management System
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol, Secure
IEMS	Integrated Element Management System
IETF	Internet Engineering Task Force
IPSec	IP Security Protocol
ISDN	Integrated Services Digital Network
ISUP	Integrated Services Digital Network User Part
LAN	Local Area Network. A network that connects computers to share data storage devices and printers.
LDAP	Lightweight Directory Application Protocol
MAP	Maintenance and Administration Position
MAPCI	Maintenance and Administration Position Command Interpreter

MCS 5200	Multimedia Communication Server 5200
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIME	Multipurpose Internet Mail Extensions
MPEG	Moving Picture Experts Group
MTC	Maintenance
MTP3	Message Transfer Part layer 3 (narrowband)
NCAS	Non-Call-Associated Signaling
NCGL	Nortel Carrier Grade Linux
NCS	Network-based Call Signaling
NEBS	Network Equipment Building System
NIC	Network Interface Card
OAM&P	Operations, Administration, Maintenance and Provisioning
OM	Operational Measurement
PBX	Private Branch Exchange
PCM	Pulse Code Modulation
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request For Capability
RTP	Real-Time Protocol
SCCP	Signaling Connection Control Part
SCP	Signaling Control Protocol
SCSI	Small Computer System Interface
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SERVORD	Service Order
SFTP	Simple File Transfer Protocol
SIP	Session Initiation Protocol
SIP-T	Session Initiation Protocol for Telephony
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SS7	Signaling System # 7

SSH	Secure Shell
STORM	Storage Management
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TFTP	Trivial File Transfer Protocol
TUP	Telephone User Part
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
URI	Universal Resource Identifier
USP	Universal Signaling Point
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VRRP	Virtual Router Redundancy Protocol
XTS	Extreme Thin Server

Nortel Communication Server 2100

Session Initiation Protocol

Service Implementation Guide

Publication number: 555-4031-903
Product release: SE08
Document release: Standard 01.03
Date: May 2005
Printed in the United States of America.