AVAYA

Avaya Communication Server 1000 Communication Server 1000E Overview

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Comments? infodev@avaya.com

Chapter 1: New in this Release

The following sections detail what's new in Avaya Communication Server 1000E Overview (NN43041–110) for Avaya Communication Server 1000 (Avaya CS 1000) Release 7.6.

Navigation

Features

There are no updates to the feature descriptions in this document.

Other

Revision History

June 2014	Standard 06.02. This document is up-issued to remove references to SIP Trunk Bridge.
March 2013	Standard 06.01. This document is up-issued to support Communication Server 1000 Release 7.6.
October 2011	Standard 05.05. This document is up-issued to remove references to legacy feature and hardware content that is no longer applicable to or supported by Communication Server 1000 systems.
April 2011	Standard 05.03 and 05.04. This document is issued to include changes to SFTP application support.

January 2011	Standard 05.02. This document is up-issued to include changes to CP DC technical content.
November 2010	Standard 05.01. This document is issued to support Avaya Communication Server 1000 Release 7.5.
August 2010	Standard 04.02. This document is issued to support Avaya Communication Server 1000 Release 7.0.
June 2010	Standard 04.01. This document is issued to support Avaya Communication Server 1000 Release 7.0.
October 2009	Standard 03.04. This document is up-issued to support the Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card.
September 2009	Standard 03.03. This document is up-issued to support the Media Gateway 1010 (MG 1010).
May 2009	Standard 03.01 and 03.02. This document is issued to support Communication Server 1000 Release 6.0
December 2007	Standard 02.03. This document is issued to support Communication Server 1000 Release 5.5.
June 2007	Standard 01.02. This document is up-issued to remove the Networks Confidential statement.
May 2007	Standard 01.01. This document is issued to support Communication Server 1000 Release 5.0. This document contains information previously contained in the following legacy document, now retired: *Communication Server 1000E: Overview, 553-3041-010*.
August 2005	Standard 2.00. This document is up-issued to support Communication Server 1000 Release 4.5.
September 2004	Standard 1.00. This document is issued for Communication Server 1000 Release 4.0.

Chapter 2: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

- Getting technical documentation on page 9
- Getting product training on page 9
- Getting help from a distributor or reseller on page 9
- Getting technical support from the Avaya Web site on page 10

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, go to www.avaya.com/support. From this Web site, locate the Training link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 3: Introduction

This document is a global document. Contact your system supplier or your Avaya representative to verify that the hardware and software described are supported in your area.

Subject

This document describes Avaya Communication Server 1000E system architecture, software and hardware requirements, components, and network connections.

⚠️ **Warning:**

Before a CS 1000E system can be installed, a network assessment must be performed and the network must be VoIP-ready.

If the minimum VoIP network requirements are not met, the system will not operate properly.

For information on the minimum VoIP network requirements and converging a data network with VoIP, refer to *Converging the Data Network with VoIP Fundamentals, NN43001-260*.

Note on legacy products and releases

This document contains information about systems, components, and features that are compatible with Avaya Communication Server 1000 software. For more information on legacy products and releases, go to Avaya home page:

www.avaya.com

Applicable systems

This document applies to the following systems:

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)

Intended audience

This document is an introductory overview for individuals responsible for the sale, acquisition, planning, or installation of CS 1000E systems.

Conventions

In this document, the CS 1000E system is referred to generically as system.

The following hardware is referred to generically as Media Gateway:

- Option 11C Mini Chassis (NTDK91) and Expander chassis (NTDK92) - legacy hardware
- Option 11C Cabinet (NTAK11) - legacy hardware
- MG 1000E Chassis (NTDU14) and Expander chassis (NTDU15)
- MG 1010 Chassis (NTC310)
- Large System Universal Equipment Module (UEM) with Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card (NTDW20)

In this document, the following hardware platforms are referred to generically as Server.

- Call Processor Pentium IV (CP PIV)
- Common Processor Pentium Mobile (CP PM) card
- Common Processor Media Gateway (CP MG) card
- Common Processor Dual Core (CP DC) card
- Commercial off-the-shelf (COTS) servers
  - IBM x360m server (COTS1)
  - HP DL320 G4 server (COTS1)
  - IBM x3350 server (COTS2)
  - Dell R300 server (COTS2)

In this document, the generic term COTS refers to all COTS servers. The term COTS1 or COTS2 refers to the specific servers in the preceding list.

In this document, the following cards are referred to generically as Gateway Controller.

- Media Gateway Controller (MGC) card (NTDW60 and NTDW98)
- Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card (NTDW20)
- Common Processor Media Gateway (CP MG) card (NTDW56 and NTDW59)

The following table shows CS 1000 supported roles for common hardware platforms

Table 1: Hardware platform supported roles

Hardware platform	VxWorks Server	Linux Server	Co-res CS and SS	Gateway Controller
CP PIV	yes	no	no	no
CP PM	yes	yes	yes	no
CP DC	no	yes	yes	no
CP MG	no	no	yes (see note)	yes (see note)
MGC	no	no	no	yes
MG XPEC	no	no	no	yes
COTS	no	yes	no	no
COTS2	no	yes	yes	no

✱ Note:

> The CP MG card functions as the Co-resident Call Server and Signaling Server, and the Gateway Controller while occupying slot 0 in a Media Gateway.

In this document, the following terminology applies:

- On systems where System Manager is available, the term UCM in the documentation refers to UCM in System Manager; on systems where System Manager is not available, the term UCM in the documentation remains unchanged.

- On systems where System Manager 6.2 is available, the term Subscriber Manager in the documentation refers to User Profile Management in System Manager; on systems where System Manager 6.1 is available, the term Subscriber Manager refers to Subscriber Manager in System Manager; on systems where System Manager is not available, the term Subscriber Manager in the documentation remains unchanged.

- On systems where Session Manager is available, the term NRS in the documentation refers to Session Manager; on systems where Session Manager is not available, the term NRS in the documentation remains unchanged.

Related information

This section lists information sources that relate to this document.

Technical documents

The following Technical documents are referenced in this document:

- *Feature Listing Reference, NN43001-111*

- *Converging the Data Network with VoIP Fundamentals, NN43001-260*
- *IP Peer Networking Installation and Commissioning, NN43001-313*
- *Branch Office Installation and Commissioning, NN43001-314*
- *Features and Services Fundamentals, NN43001-106*
- *Signaling Server IP Line Applications Fundamentals, NN43001-125*
- *Telephones and Consoles Fundamentals, NN43001-567*
- *Avaya IP Deskphones Fundamentals, NN43001-368*
- *Avaya Communication Server 1000E Planning and Engineering, NN43041-220*
- *Avaya Communication Server 1000E Planning and Engineering - High Scalability Solutions, NN43041-221*
- *Avaya Communication Server 1000E Installation and Commissioning, NN43041-310*
- *Avaya Communication Server 1000E Upgrades, NN43041-458*
- *Avaya Communication Server 1000E Upgrades Hardware Upgrade Procedures, NN43041-464*
- *Avaya Communication Server 1000E Maintenance, NN43041-700*
- *Co-resident Call Server and Signaling Server Fundamentals, NN43001-509*

Online

To access Avaya documentation online, click the **Documentation** link under **Support** on the Avaya home page:

www.avaya.com

Chapter 4: Features

Contents

Introduction

⚠️ **Warning:**

> Before an Avaya CS 1000E system can be installed, a network assessment must be performed and the network must be VoIP-ready.
>
> If the minimum VoIP network requirements are not met, the system will not operate properly.
>
> For information on the minimum VoIP network requirements and converging a data network with VoIP, refer to *Converging the Data Network with VoIP Fundamentals, NN43001-260*.

The Avaya Communication Server (CS) 1000E is a robust and highly scalable Internet Protocol (IP) Private Branch eXchange (PBX) that supports traditional Meridian features as well as new IP telephony features, including Session Initiation Protocol (SIP).

With the CS 1000E, customers can evolve from a traditional Time Division Multiplexing (TDM) network to a converged IP network. Deployment is seamless because the CS 1000E integrates with existing PBX systems from Avaya and third parties. This enables customers to expand the size and functionality of their networks while preserving their investment in legacy equipment, such as Meridian 1, Option 11C, and Communication Server 1000 systems.

Being IP-based, the CS 1000E supports distributed architecture. This enables customers to locate systems and components where they fit best. For example, using the Branch Office feature, customers can establish Branch Office Media Gateways (MG 1000B) in remote sites to extend complete feature sets across multiple locations and time zones. Customers can also configure the CS 1000E to support Campus Redundancy and Geographic Redundancy to increase system availability.

Like other Enterprise Solutions from Avaya, the CS 1000E delivers business-grade availability, security, reliability, and scalability. And as always, CS 1000E customers receive industry-leading support services from Avaya to ensure successful implementation.

Key Attributes

- Adaptable to meet current and future needs

  - Delivers investment protection and evolution path to next-generation multimedia communications

- Superior IP Telephony experience

  - More open platform to take advantage of innovative applications, and feature-rich next generation clients

- Improved reliability and security

  - Business continuity improvement from a reliable and secure environment

- Simplified convergence solution

  - Product portfolio simplified for easier deployment, configuration and management

Key features

Key features of the CS 1000E system are as follows:

The following sections describe these features in detail.

IP-based switching with TDM capability

The CS 1000E is an IP PBX that supports TDM PBX capabilities. Unlike traditional, circuit-switched PBX systems, the IP-based CS 1000E Core Call Server has no dedicated switching infrastructure. All voice communication between network elements uses a Telephony LAN (TLAN) subnet.

Evolving to the CS 1000E and a converged IP network provides several advantages. For example, it enables the customer to deliver a consistent set of services to all locations, whether large or small. It also eliminates separate voice wiring.

What's more, customers need not compromise voice quality or features by selecting a CS 1000E system. That's because the CS 1000E enables customers to route calls over their circuit-switched

networks or over their Quality of Service (QoS) managed IP network, according to their own rules and requirements.

Flexible architecture

The CS 1000E supports flexible, distributed architecture across a QoS-managed IP network. For example, a High Availability (HA) configuration with dual, redundant Common Processor Pentium Mobile (CP PM) processors can support up to 22,000 IP Phones. To support more IP Phones, multiple CS 1000E systems can be installed across the QoS-managed IP network.

In terms of physical size, the CS 1000E is smaller than legacy Large Systems, and CS 1000E components are rack-mountable in industry-standard 19-inch racks.

Standard Availability and High Availability

CS 1000E VxWorks-based architecture offers options for single and redundant processors. The CP PM card can be configured as a single call processor (Standard Availability CS 1000E) or in a redundant processor configuration (High Availability CS 1000E). The redundant CP PIV processor configuration is also available as a High Availability CS 1000E system.

The CS 1000E Standard Availability replaces CS 1000M Chassis, and CS 1000M Cabinet system types. You can upgrade a Standard Availability (SA) system to a High Availability (HA) system with the addition of a second CP PM card and by enabling the software package 410: HIGH_AVAIL HIGH AVAILABILITY. You can deploy existing or new systems in any supported Media Gateway. illustrates an example of a CS 1000E SA and HA system with CP PM cards.
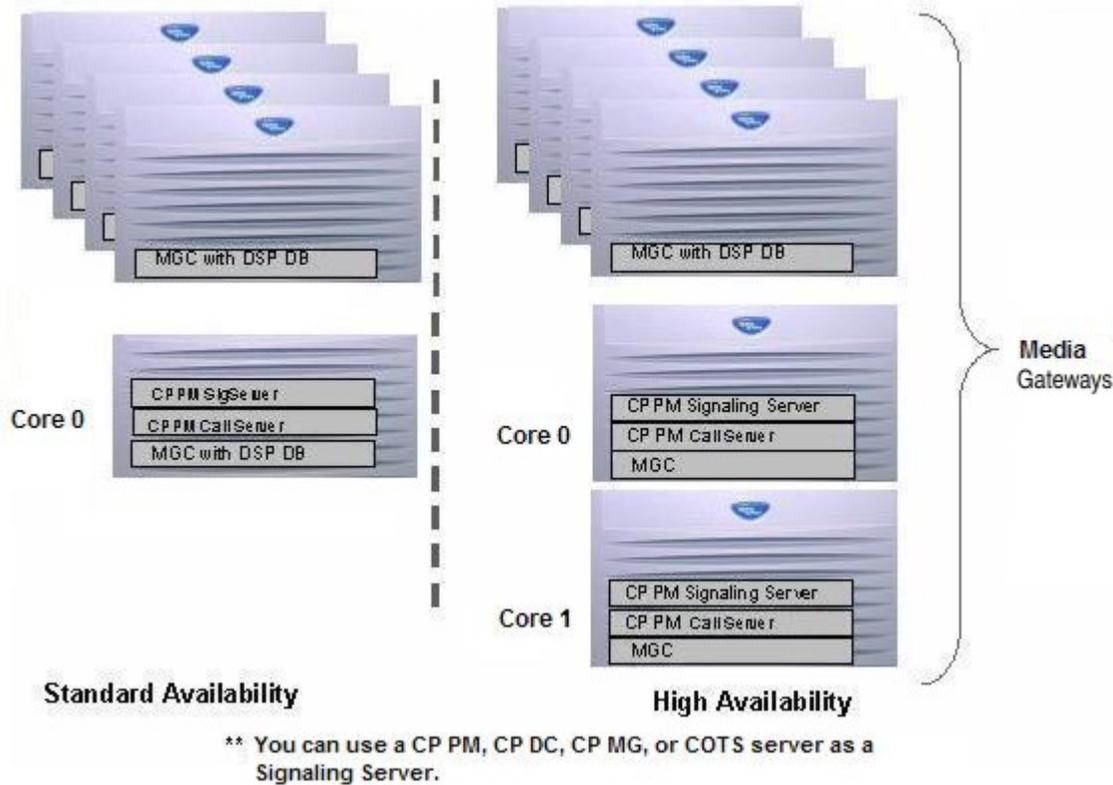
Figure 1: Standard Availability CS 1000E and High Availability CS 1000E

⊛ **Note:**

The Linux-based Co-resident Call Server and Signaling Server does not support a stand-alone SA, or a HA configuration (dual core with either Active or Inactive role). For systems that require a stand-alone SA, or a HA configuration, a VxWorks-based Server platform must be deployed.

Co-resident Call Server and Signaling Server

The Co-resident Call Server and Signaling Server (Co-res CS and SS) system can run the Call Server software, the Signaling Server software, and System Management software on the same hardware platform running the Linux base operating system. For CS 1000, the Co-res CS and SS system supports various hardware platforms, see Table 1: Hardware platform supported roles on page 13. For more information about Co-res CS and SS systems, see *Co-resident Call Server and Signaling Server Fundamentals, NN43001-509*.

High Scalability

The CS 1000E High Scalability (HS) solution provides a centralized deployment model to allow network consolidation with a solution that provides business continuity while minimizing management overhead. This solution offers increased scalability for supporting large Communication Server 1000 networks.

For more information about CS 1000E High Scalability, see *Avaya Communication Server 1000E Planning and Engineering - High Scalability Solutions, NN43041-221*.

Branch Office

The CS 1000E also supports the Branch Office Media Gateway (MG 1000B) configuration, which enables a user at a remote location to access the same features available at the main site. This allows customers to extend complete feature sets across multiple locations and time zones and reduce operating costs.

You can deploy any supported Media Gateway as a MG 1000B. For more information about Branch Office, see *Branch Office Installation and Commissioning, NN43001-314*

Redundant architecture

The CS 1000E (HA) comes configured with fully redundant Call Servers, similar to the dual CPUs used in CS 1000M, Meridian 1 Large Systems. The sections below describe key configuration options.

Campus Redundancy

With Campus Redundancy, a customer can separate the inactive Call Server from the active Call Server using a dedicated 100 Meg bit pipe between cores configured to meet specified network parameters. When this configuration is implemented, a major failure of the active Call Server (for example, due to fire or flood) does not disable the remote Call Server.

Geographic Redundancy

Geographic Redundancy increases the reliability of CS 1000E systems by providing a remote system to serve as a backup for a local system. Depending on the configuration, the remote backup

system ensures continued service for resources in case of a catastrophic failure (for example, as a result of floods or fire). Geographic Redundancy also offers automatic database replication between main and backup systems to promote a smooth transition. When this configuration is implemented, the customer enhances the disaster recovery capability of their network and further secures ultra-high reliability.

Industry-standard interworking and interoperability

The CS 1000E supports interworking and interoperability with other enterprise PBX systems from Avaya and third parties. This enables customers to smoothly migrate from traditional TDM-based telephony products to IP-based telephony products.

The CS 1000E supports interworking with many Avaya products, including Business Communication Manager (BCM) and CS 1000M, using standard SIP and H.323 protocols with Meridian Customer Defined Networking (MCDN) extensions to provide more complete feature transparency. The CS 1000E also uses industry-standard SIP and H.323 protocols to support interworking with third-party products.

For existing Meridian 1 and Succession 1000 customers, the CS 1000E supports reuse of equipment. Reuse means faster deployment, reduced cost, and lower training costs. For example, customers can reuse circuit cards and Media Gateways from Meridian 1 and Succession 1000 systems in a CS 1000E system.

System management capabilities

The CS 1000E provides system management capabilities through an integrated set of interfaces. These interfaces increase configuration capability and reduce operating cost, in part by centralizing services and service provisioning.

Management interfaces supported by the CS 1000E include traditional Command Line Interfaces (CLI) and Unified Communication Management (UCM), which includes the following services and applications:

- Deployment Manager
- Base Manager
- Patching Manager
- SNMP Profile Manager
- Network Routing Service Manager
- Element Manager
- Subscriber Manager

Unified Communication Management framework

The Avaya UCM framework provides:

- Private Certificate Authority.

- Secure Shell (SSH) access to the Command Line Interface.

- Centralized point of access for the management of users, passwords, system access, and security.

- UCM navigator provides an overview of network components from the host's perspective.

- Single point of access to manage the entire network. Element Manager and NRS Manager are components of UCM.

Deployment Manager

Use Deployment Manager on the Primary security server for an end-to-end installation and configuration of Linux base and applications on a Server. Deployment Manager provides a simplified and unified solution that enables network installation of Avaya Linux base on target servers.

UCM Deployment Manager provides two methods for software deployment:

- centralized software deployment (recommended)

- local software deployment

For more information about software deployment, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Base Manager

The Base Manager, a Web-based interface, is used for low level configuration of all Linux elements. From Base Manager, you can also configure forwarding of logs that are generated on the backup and member servers for consolidation on the primary security server.

For more information about Base Manager and how to access it through UCM, see *Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Patching Manager

The Patching Manager centrally deploys patches from the primary security server to other Linux servers in the same security domain. For more information, see *Patching Fundamentals, NN43001-407*.

SNMP Profile Manager

The SNMP Profile Manager centrally configures SNMP parameters for all elements from the primary security server to other Linux servers in the same security domain. For more information, see *Avaya Communication Server 1000 Fault Management — SNMP, NN43001-719*.

Network Routing Service Manager

Network Routing Service Manager (NRSM) is a web-based configuration interface. You can perform the following NRS configuration functions using NRS Manager:

- configure a numbering plan
- add, modify, or delete preconfigured endpoint data
- add, modify, or delete numbering plan entries on a per-endpoint basis
- retrieve the current configuration database
- interwork with a preconfigured database
- revert to the standby database
- change system passwords

Element Manager

CS 1000E supports Element Manager (EM), a web-based GUI that offers an alternative to traditional overlays and CLIs. Element Manager simplifies overall management of items like Network Routing Service (NRS), IP services, IP Peer configuration, and software downloads.

Subscriber Manager

The Subscriber Manager centrally manages subscribers and subscriber accounts from the primary security server. For more information, see *Subscriber Manager Fundamentals, NN43001-120*.

Traditional Command Line Interfaces

CS 1000E fully supports traditional CLIs, including overlays.

Software applications and features

The CS 1000E system provides access to the full suite of Meridian software applications and features. It also provides access to an emerging suite of IP-based applications and features that increase operational efficiency while lowering costs through convergence and user mobility.

In brief, the CS 1000E supports the following features and applications:

- Traditional telephony applications. Traditional telephony features (Call Waiting, ACD, CDR, and so on) are fully supported.
- Networking applications. ISDN PRI, ISDN BRI, ESN, and other Meridian 1 networking applications are fully supported.
- Voicemail applications. CallPilot is fully suppported.
- Multimedia Communication Server 5100 (MCS 5100) applications. The MCS 5100 portfolio of multimedia applications for the enterprise and other standards-based SIP applications are supported.
- Contact Center applications. Contact Center applications are fully supported.
- Wireless applications. CS 1000E supports WLAN IP Telephony Manager 2245 and WLAN Application Gateway 2246. Support is also provided for Avaya Integrated DECT (DECT).
- Integrated applications. The complete suite of Integrated applications is supported, including:

  - Avaya Integrated Conference Bridge
  - Avaya Integrated Call Assistant
  - Avaya Integrated Call Director
  - Avaya Integrated Recorded Announcer
  - Avaya Hospitality Integrated Voice Services

UNIStim signaling encryption with DTLS

Secured UNIStim signaling encryption is provided by Datagram Transport Layer Security (DTLS). DTLS encrypts the data exchanges between the Signaling Server and the IP Phones. Previously, Secure Multimedia Controllers (SMC 2450) were required for UNIStim encryption, but DTLS requires no new additional hardware and can coexist with currently installed SMCs. DTLS and non-DTLS systems can be configured on the same network.

UCM Security Domain Manager

This section describes concepts associated with the Security Domain Manager (SDM). The SDM for VxWorks controls the joining of devices to security domain of the UCM Primary Security Server.

The UCM Primary Security Server acts as the RADIUS server from which Communication Server 1000 devices obtain authentication and access control parameters for CLI access. The RADIUS

related parameters are sent from the UCM Primary Security Server to Communication Server 1000 devices using SSH protocol.

When a device joins the UCM security domain, a mutually-trusted SSH channel is created with the following properties:

- the SSH server public key of the device is added to the known host key list of the UCM Primary Security Server
- the RSA public key of the UCM Primary Security Server is added to the authorized key list of the CS 1000 device

Before the UCM primary server RSA public key is added to the authorized key file, the fingerprint of the public key must be confirmed manually. This verification prevents third-party intercepts. Once a mutually trusted SSH tunnel has been established for the first time, the UCM Primary Security Server can send SSH remote commands to the device using RSA public key-based authentication.

The normal authentication process is as follows:

- the UCM Primary Security Server verifies the device SSH server public key against its known host list. Devices with a spoofed IP address are detected as they cannot possess both the public and private key pair of the original device.
- the device authenticates the UCM Primary Security Server using the authorized key list under the system account name.

The remote command is executed on the device only if it is received from a mutually authenticated SSH tunnel and the system account in question has the permissions to execute the command.

VxWorks based systems and devices can join the UCM security domain using the following modes:

- Manual mode—the joining and leaving of the UCM security domain operation is performed on each individual Call Server, MGC and MC(MC32S/SA) using the following commands:

  - LD 117 command: UCM [JOIN / LEAVE] DEVICE
  - OAM/PDT/IPL commands: joinSecDomain or leaveSecDomain

- User mode—the joining and leaving of the UCM security domain operation is performed centrally from the Call Server, where the administrator confirms the list of devices to be added or removed:

  - LD 117 command: UCM [JOIN / LEAVE] SYSTEM

SSH File Transfer Protocol (SFTP)

FTP is an inherently insecure method of transferring files due to the lack of encryption and authentication. In an FTP session, the user name, password, FTP commands, and transferred files are all transmitted in clear text without any security protection, and can be intercepted by anyone with the access to the FTP communication path. FTP has been widely viewed as a significant security weakness by almost all customers, and must be replaced by a secure file transfer protocol in CS 1000 systems.

SFTP is a network protocol that provides confidentiality and integrity to data (such as files or commands) transmitted between an SFTP client and a server. In addition, SFTP allows an SFTP client and an SFTP server to authenticate each other by using a password. SFTP allows data (such as file and/or command) transferred between an SFTP client and server over an encrypted and authenticated secure channel that cannot be intercepted or tampered with. SFTP is used to replace many usages of FTP (and other insecure data transfer protocols in some cases) in the system.

To provide backward compatibility, conventional FTP is still used for file transfer sessions between CS 1000 Release 7.0 or later and any prior release such as CS 1000 Release 5.0.

Feature operation during upgrade

After upgrading to CS 1000, both SFTP and FTP servers are supported. While both SFTP and FTP clients are supported on the devices associated with the Call Server, the SFTP client is used by default. Therefore, the Call Server should always be upgraded first. To use an FTP client, users must enable it by running commands (see .

There is no impact to CallPilot during an upgrade if it is part of the system. CallPilot usually functions as a client and can continue to use the FTP client to communicate with a CS 1000 Call Server supporting an SFTP and FTP server.

SFTP application support

A number of applications that support FTP can support SFTP.

From Server to all devices:

- account
- banner
- DBSYSCFG.db

Server redundancy:

- PSDL file update (only applicable to Call Server redundancy)

Other devices:

- Gateway Controller database files transfer from CS
- Personal Directory
- PDT disk/file command transfer
- UMS transfer
- Boot file, configuration, F/W, SNMP
- Gateway Controller, MC32S bootfile, configuration, loadware, installation file transfer

- IP phone F/W file transfer (EM -EM patching handler)
- Manufacturing delivery patch distribution

Table 2: SFTP application support

Applications supporting SFTP transfer	Type of SFTP data transfer
CS to all connecting devices	Sync of account DB, SYSCFG.db, Banner
CS to CS (inactive)	Sync of PSDL
CS to Gateway Controller	F/W and DB upgrade
CS to SS or Gateway Controller	Node info distribution
CS to SS	Manufacturing deliver patch distribution
CS to MC32S	Config/bootp file update
CS (active) to CS (redundant)	GR DB Replication ✳ **Note:** Starting with Communication Server 1000 Release 6.0, database replication occurs by SFTP. In Survivable Media Gateway configurations where some of the Call Servers have not yet been migrated to Release 6.0 or later software, database replication occurs using regular FTP until all Call Servers in the configuration have been migrated to Release 6.0 or later software.
EM to SS/CS/SA/	Uploading of F/W, Patch, BootP file and PD. SNMP update

Applications listed in the table below continue to support FTP only. The mitigation mechanism for those applications is to use IPSec.

Table 3: Applications supporting FTP only

Devices supporting FTP transfer	Type of FTP data transfer
CS to IPMG	SIPE S/W upgrade (obsolete)
SS to SS	SS patch distribution
NRS (Primary/secondary) to NRS (failsafe)	Database Replication
SS to external FTP server	PD backup
ITG to external FTP server	swDownload (parameters, e.g., file, username, pswd) initiated from ITG.

Secure transport commands

Different platforms, such as Signaling Server, MGC and ITG-SA, have local shell commands to enable/disable the secure/insecure transfers as well as STAT commands to display whether the secure/insecure transfer is allowed or not. There is no limitation for STAT command execution in different shells.

Enable/disable commands are only provided on the OAM and PDT2 shells. Only users with PWD2 rights can execute them. See Table 4: Secure transport commands on page 27.

Table 4: Secure transport commands

Command	Description
disInsecureTransfers	Disables all insecure FTP transfers in the system
enlInsecureTransfer	Enables all insecure FTP transfers in the system
disSecureTransfers	Disables all insecure SFTP transfers in the system
enlSecureTransfers	Enables all insecure SFTP transfers in the system
statInsecureTransfers	Displays enabled or disabled status of insecure transfer access
statSecureTransfers	Shows whether secure transfer access is enabled or disabled

SSH Library upgrade

The embedded security suite provides the following security features:

- SSH server supports both RSA and DSA key generation and authentication negotiation with an SSH client. For example, a CS 1000 SSH server uses RSA key authentication to communicate with a UCM Primary Server SSH client, since UCM only supports RSA key authentication.

- an SFTP server

- standard DTLS solution

SIP support

The Avaya Communication Server 1000 software supports the H.323 protocol as well as the Session Initiation Protocol (SIP) on the same Signaling Server hardware.

SIP is used to establish, modify, and terminate telephony sessions in IP networks. A session can be a simple two-way telephone call or a multimedia session that integrates voice, data, and video. SIP's text-based architecture speeds access to new services with greater flexibility and more scalability.

SIP Gateway offers an industry-standard, SIP-based, IP Peer solution that delivers a SIP interface for interoperability with standard SIP-based products, including Avaya SIP products. SIP Services, through a Converged Desktop, provides the CS 1000 telephony features as well as Multimedia Communication Server (MCS) 5100 applications.

The Converged Desktop capabilities of CS 1000E requires an MCS 5100 to be in the network. This interfaces to the CS 1000E by means of SIP trunks.

CS 1000 capacity enhancements and SIP-related interoperability enhance the positioning of large-sized networks and enable users to access multimedia when MCS 5100 servers and services are added.

Survivable SIP Media Gateway

The Survivable SIP Media Gateway (SSMG) is an architectural model for managing resources at individual locations in a Call Sever Geographic Redundancy (GR) model. An SSMG consists of a SIP Media Gateway Controller (SIP MG Controller) and a Survivable Server. This architecture separates the IP resources from the traditional digital resources by having two separate call servers.

- One call server (and the associated signaling proxies), known as the Survivable Server, handles the survival aspect of GR which includes receiving the database from the Primary Call Server, providing registration and access services to IP endpoints, for example, IP Phones.

- The second call server (and the associated signaling proxies), known as the SIP MG Controller, handles all the digital resources at the site, such as traditional TDM and analog phones, fax machines, and PRI/BRI trunk connectivity.

The MGC card and the associated DSPs register to the SIP MG Controller. The SIP Media Gateway (SIP MG Controller) connects the system to the digital resources through the SIP signaling interface.

For more information, see *Avaya Communication Server 1000E Planning and Engineering — High Scalability Solutions, NN43021-221*.

Desktop clients

The CS 1000E supports many new IP telephony devices, including IP Phones, SIP phones, and soft clients for desktop, tablet, and PDA devices. The CS 1000E also supports a wide range of traditional desktop clients, including analog (500/2500-type) telephones, digital telephones, and attendant consoles.

For more information on IP Phones, see *IP Phones Fundamentals, NN43001-368*. For more information on analog and digital telephones, see *Telephones and Consoles Fundamentals, NN43001-567*.

IP Phones with UNIStim software

The CS 1000E supports the following IP Phones with UNIStim software: 2001 IP Phone, 2002 IP Phone, 2004 IP Phone, Avaya 2007 IP Deskphones, Avaya 2033 IP Conference Phone, Avaya 2050 IP Softphone, Mobile Voice Client 2050, Avaya 1110 IP Deskphone, Avaya 1120E IP Deskphone,Avaya 1140E IP Deskphone, Avaya 1150E IP Deskphone, Avaya 1165E IP Deskphone, Avaya 1210 IP Deskphone, Avaya 1220 IP Deskphone, and Avaya 1230 IP Deskphone. The CS 1000E system also supports the Meridian IP Phone adapter package for the M26xx and M39xx telephones. The IP Phone adapter package is intended for local deployment and does not support analog PSTN fallback.

IP Deskphones with SIP software

The Avaya CS 1000E supports the following IP Deskphones with Session Initiation Protocol (SIP) software: Avaya 1120E IP Deskphone, Avaya 1140E IP Deskphone, Avaya 1220 IP Deskphone, Avaya 1230 IP Deskphone, IP Phone1535, IP Phone 3456, Teledex LD4200, and Teledex ND2200.

Traditional telephones

Traditional telephones are the following:

- Digital telephones:

  The CS 1000E system supports the M3900 series Meridian Digital Telephones. This includes the M3901 Entry Level Telephone, the M3902 Basic Telephone, the M3903 Enhanced Telephone, the M3904 Professional Telephone, and the M3905 Call Center Telephone.

  The CS 1000E also supports other digital telephones, including the M2006, the M2008, the M2008HF, the M2616, the M2016S, the M2216ACD, and the M2317 Telephone.

- Analog (500/2500-type) telephones and fax:

  The CS 1000E supports analog line cards that support analog (500/2500-type) telephones and T.38 fax interfaces.

Attendant consoles

The CS 1000E supports the Attendant PC software console and the M2250 attendant console.

The Attendant PC software enables users to perform attendant console and call processing functions on a Windows® PC using a mouse or keyboard. The Attendant PC combines the call-

processing power of the M2250 attendant console with the processing power and storage capacity of a PC to enhance attendant services.

IP Attendant console

The IP Attendant Console 3260 is an IP-enabled Attendant Console that replaces the need for a Personal Computer Console Interface Unit (PCCIU) or M2250 Digital Attendant Console for supported third party Attendant Console clients. The IP Attendant Console is included with the IP Media Services applications that are installed with the Signaling Server software.

The IP Attendant Gateway uses Session Initialization Protocol (SIP) to manage signaling between the IP Attendant Console and the Avaya Media Server. Communication with the Call Server is managed using the existing Transmission Control Protocol (TCP).

For more information about the IP Attendant console, see *Features and Services Fundamentals, NN43001-106*.

Chapter 5: System architecture

Contents

Avaya Communication Server 1000E Standard Availability and High Availability Server

The Avaya CS 1000E Standard Availability (SA) Call Server consists of one Common Processor Pentium Mobile (CP PM) card and one Media Gateway Controller (MGC) card in a Media Gateway. You can upgrade to a High Availability (HA) system with the addition of a second CS 1000E SA Call Server and by enabling the software package 410: HIGH_AVAIL HIGH AVAILABILITY. The CP PM card supports the stand-alone SA and the HA configurations. The Call Processor Pentium IV (CP PIV) supports the HA system configuration only.

Physical description

Figure 2: CS 1000E Call Server on page 32 shows a CP PM card and MGC card installed in an NTDU14 MG 1000E Chassis without the cover.

Figure 2: CS 1000E Call Server

Hardware components

Each CS 1000E SA Call Server contains the following:

- Media Gateway
- Server (CP PM card)
- Gateway Controller (MGC card)

Media Gateway

You can use any supported Media Gateway to house the Server and the Gateway Controller cards. Media Gateway Expanders are not supported. For more information about Media Gateways, see Media Gateway 1000E on page 35 and Media Gateway 1010 on page 39.

You can convert a CS 1000M Large System Universal Equipment Modules (UEM) into two Media Gateways for use in a CS 1000E system with a Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card. For more information, see Media Gateway Extended Peripheral Equipment Controller (MG XPEC) on page 42.

The Media Gateway provides the following functionality:

- provides digital trunks to the PSTN and trunking to other PBX systems using E1, T1, ISDN PRI, and ISDN BRI circuit cards
- supports Voice Gateway Media Cards for transcoding between IP and TDM
- provides tones, conference, and digital media services (for example, Music and Recorded Announcement) to all phones

- provides support for CallPilot and Avaya Integrated Applications
- provides direct physical connections for analog (500/2500-type) phones, digital phones, and fax machines
- provides direct physical connections for analog trunks
- supports the DECT application

The Media Gateway operates under the direct control of the Call Server. Up to 50 Media Gateways can be configured on the Call Server.

The Media Gateway supports the following circuit cards and applications:

- Server cards: provide Call Server or Signaling Server functions
- Gateway Controller card: provide Gateway controller functions and can provide DSP resources
- Voice Gateway Media Cards: transcode between IP and TDM
- Service cards: provide services such as Music or Recorded Announcements (RAN)
- DECT Mobility cards
- Digital PSTN Interface Cards, including E1, T1, ISDN PRI,and ISDN BRI: provide access to PSTN
- Analog interfaces to lines and trunks: support analog (500/2500-type) phones and fax, PSTN trunks, and external Music or RAN sources
- Digital line cards: support digital terminals, such as attendant consoles, M2000/M3900 series digital phones, and external systems that use digital line emulation, such as CallPilot Mini
- CLASS Modem card (XCMC)
- Avaya Integrated Applications, including:
  - Integrated Conference Bridge
  - Integrated Call Assistant
  - Integrated Call Director
  - Integrated Recorded Announcer
  - Hospitality Integrated Voice Services
- MGate cards for CallPilot
- CallPilot IPE

Common Processor Pentium Mobile (CP PM) card

The CP PM card (NTDW61 or NTDW99) is the main processor for the CS 1000E SA system, controlling all call processing and telephony services. It also provides the system memory required to store operating software and customer data. The CP PM card is the only Server card that can support the stand-alone SA and the HA configuration. For more information about the CP PM card, see *Circuit Card Reference, NN43001-311*.

Media Gateway Controller (MGC) card

The MGC card (NTDW60 or NTDW98) occupies slot 0 in the Media Gateway. The MGC card provides Gateway Controller functions and can provide Digital Signal Processor (DSP) resources for each Media Gateway in a CS 1000E system. The MGC only functions as a Gateway Controller under the control of a Server. For more information about the MGC card, see *Circuit Card Reference, NN43001-311*. Converted Large Systems use the MG XPEC card as the Gateway Controller.

Functional description

The Call Server provides the following functionality:

- provide main source of call processing
- process all voice and data connections
- control telephony services
- control circuit cards installed in Media Gateway 1000s
- provide resources for system administration and user database maintenance

Operating parameters

The CS 1000E (SA) has a single call processor (core 0). The CS 1000E (HA) has dual call processors (core 0 and core 1) to provide a fully redundant system.

Call processors (core 0 and core 1) operate in redundant mode: one runs the system while the other runs in a "warm standby" mode, ready to take over system control if the active Call Server fails.

The system configuration and user database are synchronized between the active and inactive Call Servers. This allows the inactive Call Server to assume call processing in the event of failure of the active Call Server.

The Call Server uses a proprietary protocol to control the Media Gateways. This proprietary protocol is similar to industry-standard Media Gateway Control Protocol (MGCP) or H.248 Gateways.

The Call Server can control up to 50 Media Gateways.

❋ **Note:**

The Call Server provides connectivity to telephony devices using IP signaling through Media Gateways rather than by direct physical connections.

Avaya CS 1000E High Scalability Solution

The High Scalability solution offers increased scalability of the Communication Server 1000 networks. A High Scalability (HS) system is a collection of CS 1000E High Availability (HA) Call Servers and Signaling Servers.

You can implement the High Scalability solution using any of the following deployment models:

- Campus Redundancy Multiple HA systems dispersed geographically

- Geographic Redundancy

- Multiple HA systems dispersed geographically

For more information about the High Scalability solution, see *Avaya Communication Server 1000E Planning and Engineering — High Scalability Solutions, NN43021-221*.

Media Gateway 1000E

The Media Gateway 1000E (MG 1000E) houses circuit cards and connectors to support the functionality of a Media Gateway and provides basic telephony media services, including tone detection and generation and conference, to CS 1000E telephones. The Media Gateway also supports Avaya Integrated Applications, including Integrated Recorded Announcer. It can also provide connectivity for digital and analog (500/2500-type) telephones as well as analog trunks for telephone and fax.

✳ Note:

The Branch Office Media Gateway can use any supported Media Gateway. For more information, see *Branch Office Installation and Commissioning, NN43001-314*

Physical description

shows the NTDU14 Media Gateway 1000E.

Comments? infodev@avaya.com
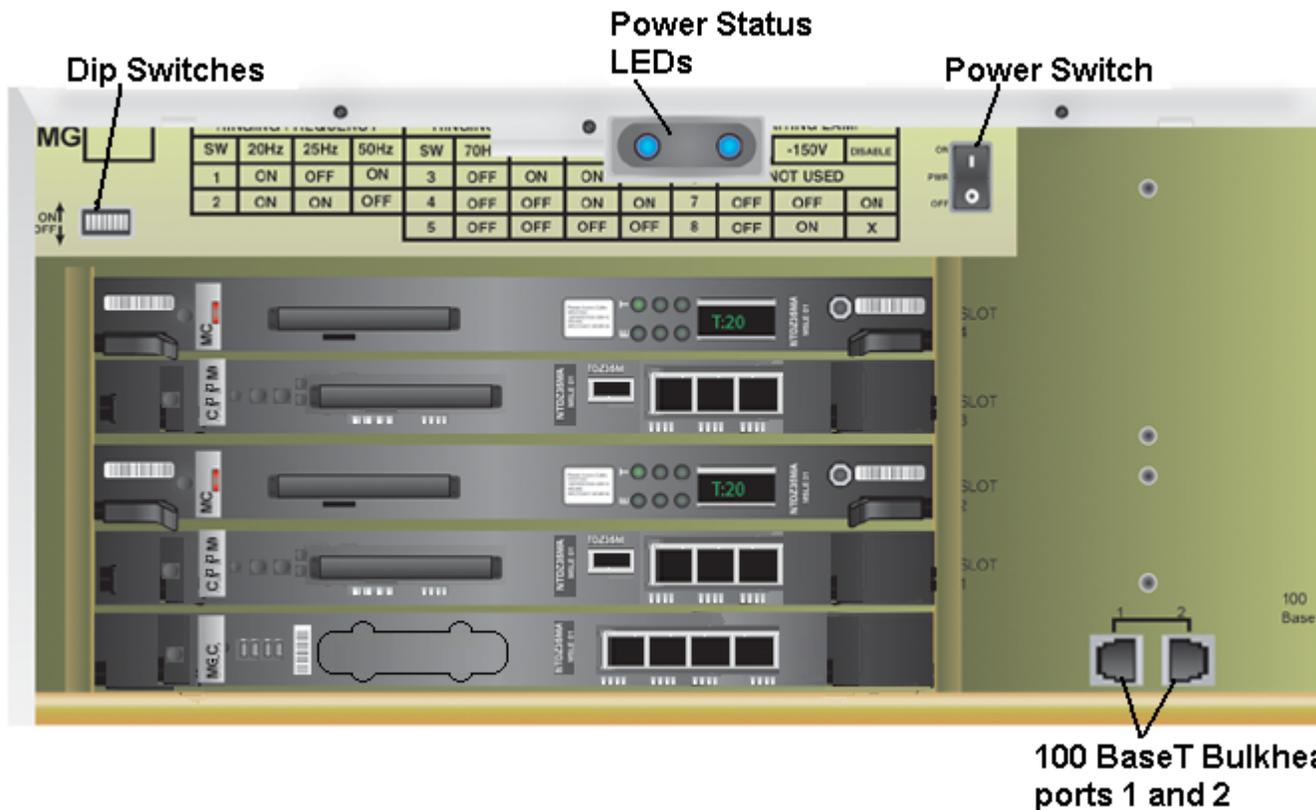
Figure 3: NTDU14 Media Gateway 1000E (front)

Hardware components

The following sections describe front and rear components of the MG 1000E.

Front components

Figure 3: NTDU14 Media Gateway 1000E (front) on page 36 shows the MG 1000E with the front cover removed. Note the following:

- The DIP switches set ringing voltages, ringing frequencies, and message waiting voltages.
- The 100BaseT bulkhead ports 1 and 2 provide direct connections to the rear bulkhead ports.

Rear components

Figure 4: Rear components in the Media Gateway 1000E on page 37 shows the rear components on the MG 1000E. Note the following:

- The AC power cord connector provides AC connection to the MG 1000E.
- AUX extends Power Failure Transfer Unit (PFTU) signals to the Main Distribution Frame (MDF).
- GND is used for ground cable termination.
- 100BaseT bulkhead ports 1 and 2 provide direct connections from the front bulkhead.
  - On MG 1000E, these ports provide connections to the Call Server through an ELAN switch.
- The serial port connects to maintenance terminals.
- DS-30X and CE-MUX interconnect the Media Gateway 1000 to the Media Gateway Expander.
- 25-pair connectors extend the IPE card ports to the MDF.
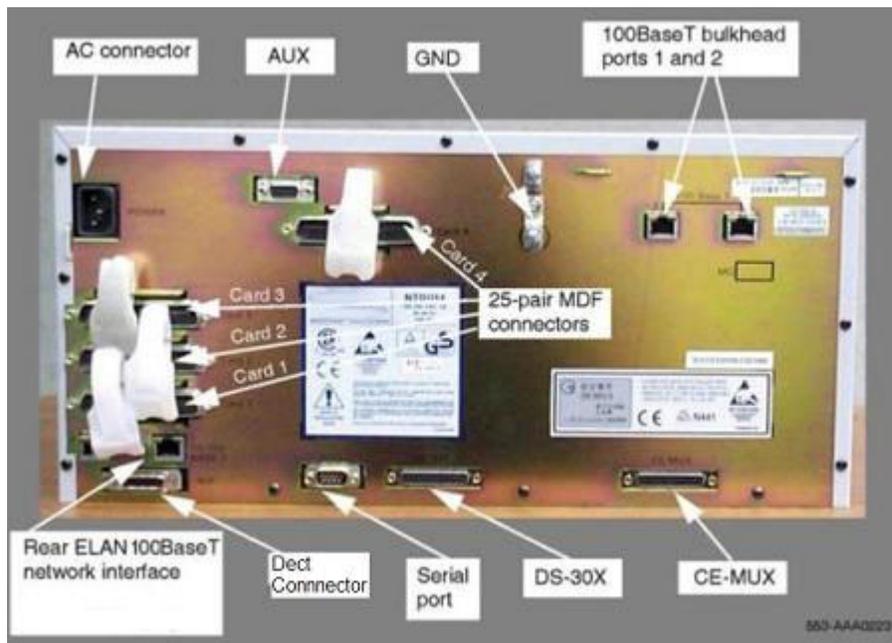
Figure 4: Rear components in the Media Gateway 1000E

Media Gateway Expander

Main Role

The Media Gateway Expander supports up to four circuit cards. The MG 1000E is required to support a Media Gateway Expander.

Physical description

[Figure 5: Media Gateway Expander (NTDU15)](#) on page 38 shows the Media Gateway Expander (NTDU15).

Figure 5: Media Gateway Expander (NTDU15)

Rear components

[Figure 6: Rear components in the Media Gateway Expander](#) on page 39 shows the rear components in the Expander. Note the following:

- The AC power cord connector provides an AC connection to the Expander.
- GND is used for ground cable termination.
- DS-30X and CE-MUX are used to interconnect the Media Gateway 1000 and the Expander.
- 25-pair connectors are used to extend IPE card ports to the MDF.
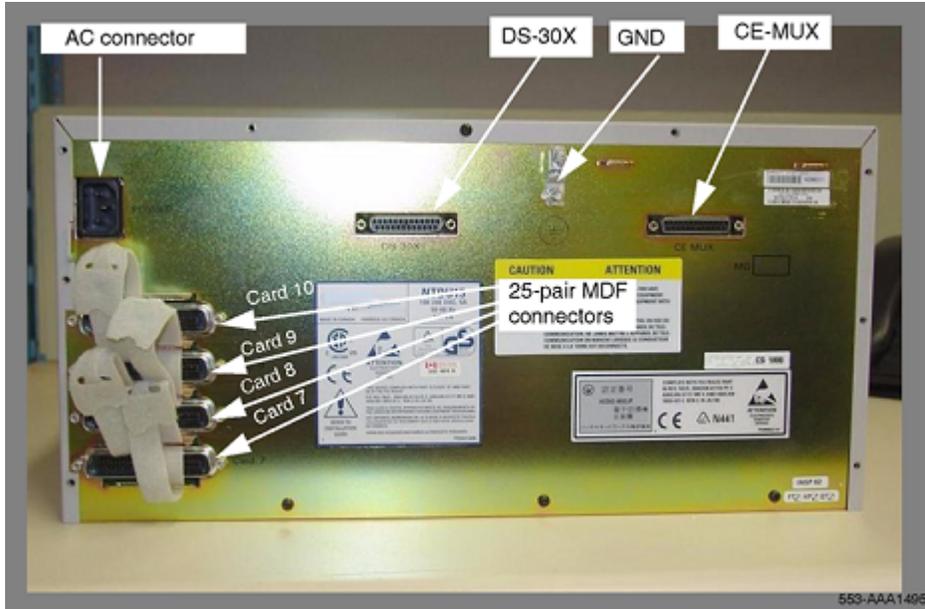
Figure 6: Rear components in the Media Gateway Expander

Operating parameters

Each MG 1000E supports one optional Expander.

Media Gateway 1010

The Media Gateway 1010 (MG 1010) is a rack mount Media Gateway chassis that provides a larger amount of card slots than a MG 1000E with Media Gateway Expander. The CS 1000E Call Server can connect to and control a maximum of 50 MG 1010s. Each MG 1010 provides a dedicated Gateway Cotnroller slot, two dedicated Server card slots, and ten slots for IPE cards. The MG 1010 is a single chassis that can provide more processing power and card capacity than a MG 1000E with Media Gateway Expander.

Physical description

The following sections describe the front and rear components of the MG 1010 (NTC310).

Front components

[Figure 7: MG 1010 front components](#) on page 40 shows the Media Gateway 1010 without the front cover. Note the following features:

- Ten IPE card slots
- Two Server card slots
- One Gateway Controller card slot
- One Media Gateway Utility (MGU) card provides LED status, ringing, message waiting voltage, dual homing Ethernet cable ports, and serial cable ports.
- One metal divider in chassis to separate MGU, Servers, and Gateway Controller from the IPE cards.
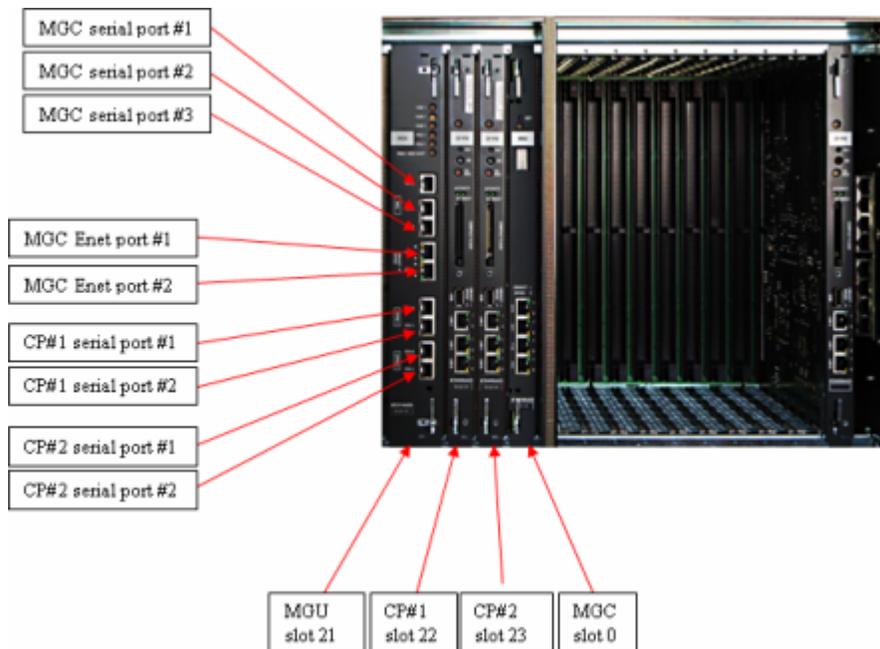
Figure 7: MG 1010 front components

[Figure 8: MG 1010 front cover](#) on page 41 shows the MG 1010 with the front cover. Note the following features:

- Window to view LED status of all cards
- Decorative cover provides additional EMC
- Two locking latches in top corners of front cover.

Figure 8: MG 1010 front cover

Rear components

[Figure 9: MG 1010 rear components](#) on page 42 shows the rear components of the MG 1010. Note the following features:

- Hot swappable redundant power supplies
- Hot swappable fans in a redundant N + 1 configuration for chassis cooling
- One DECT connector
- One AUX connector
- Ten MDF connectors
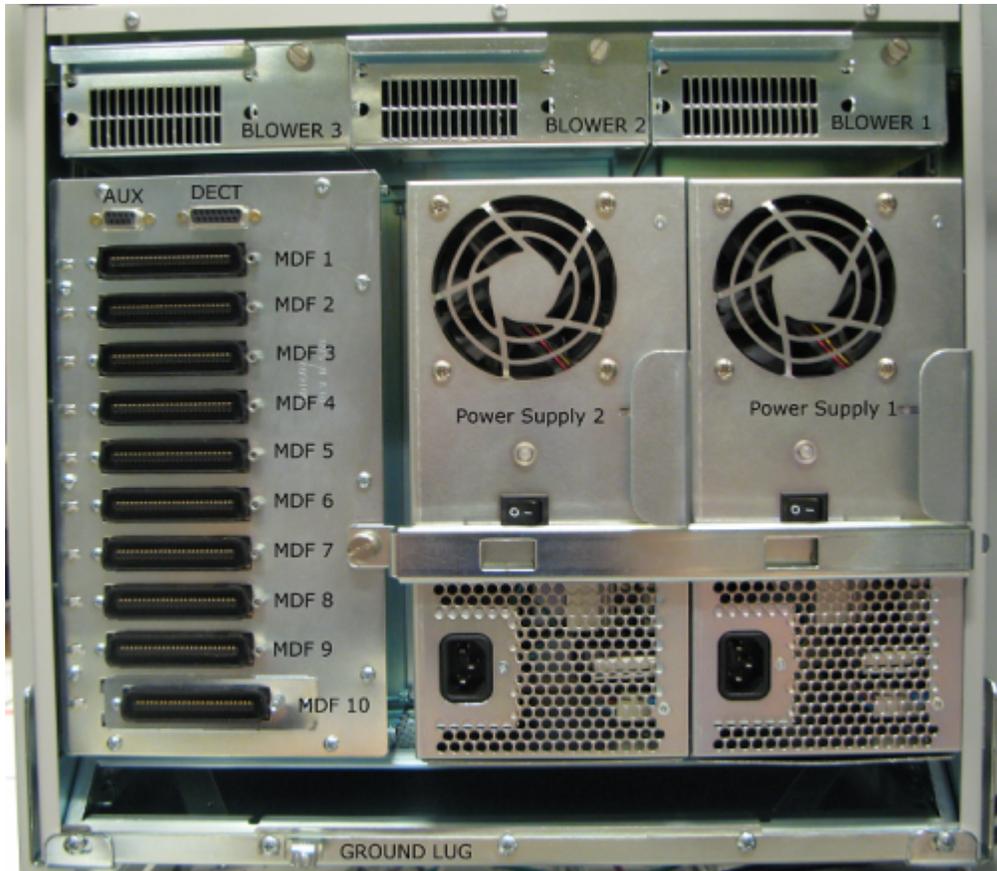
Figure 9: MG 1010 rear components

Media Gateway Extended Peripheral Equipment Controller (MG XPEC)

The Media Gateway Extended Peripheral Equipment Controller (MG XPEC) card provides a cost effective solution to migrate from a Meridian 1 or CS 1000M to a CS 1000E system while allowing customers to re-use most of their existing peripheral equipment. The NTDW20 MG XPEC card converts a NT8D37 Large System Universal Equipment Module (UEM) into two Media Gateway shelves (IPMG type MGX) for use in a CS 1000E system.

Routes can be added to the ELAN of the MGC and MG XPEC using Element Manager.

Functional description

The MG XPEC is a double wide, dual card assembly using ported MGC hardware. It is used to control PE line cards in an IPE shelf. The MG XPEC features a motherboard and daughterboard

architecture which act independently and provide the same hardware functionality as that of an MGC.

Each board of the dual assembly is populated with 192 DSP resources which are recognized by the software as the equivalent of two MGC DSP daughterboards.

The MG XPEC card can be thought of as two separate MGCs bolted together with the left board (motherboard) controlling the left half of the of the IPE shelf and the right (daughterboard) controlling the right half of the IPE shelf.

Figure 10: MG XPEC faceplate on page 43 provides a view of the MG XPEC faceplate.
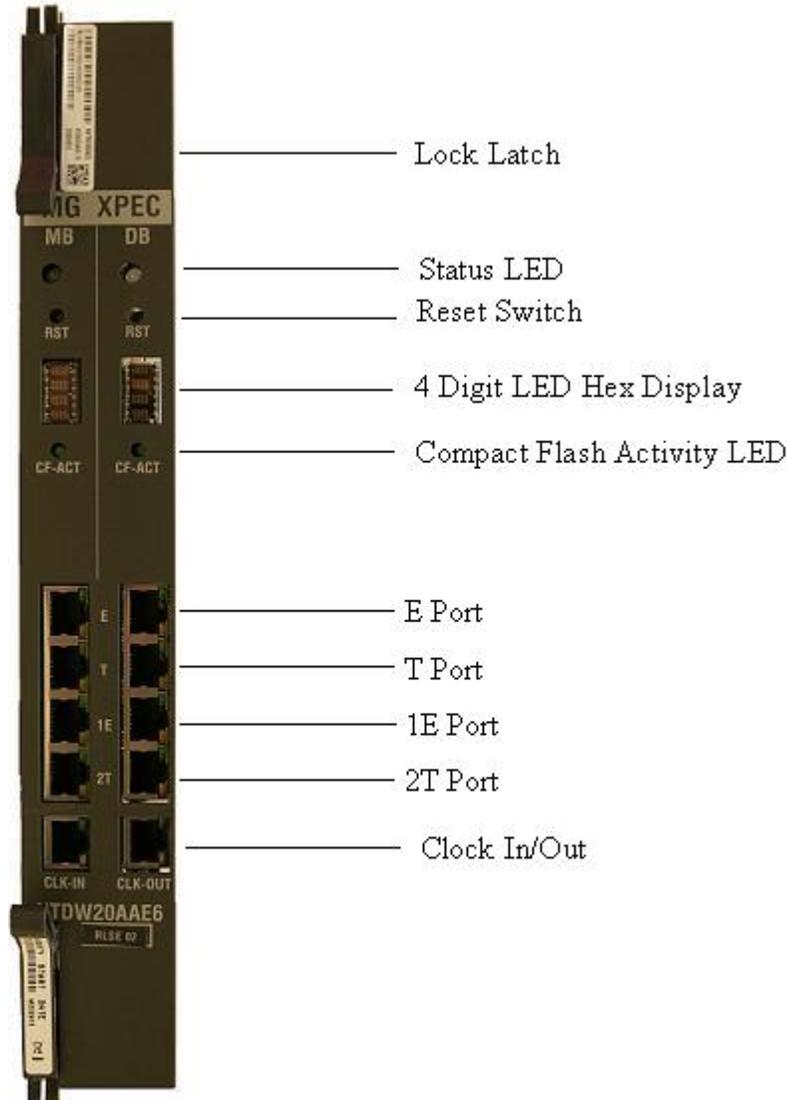
Figure 10: MG XPEC faceplate

For more information about converting IPE modules into Media Gateways with the MG XPEC card, see *Avaya Communication Server 1000M and Meridian 1 Planning and Engineering, NN43021-220*.

Media Gateway network connections

The following figure shows a schematic representation of the typical network connections for one MG 1000E.
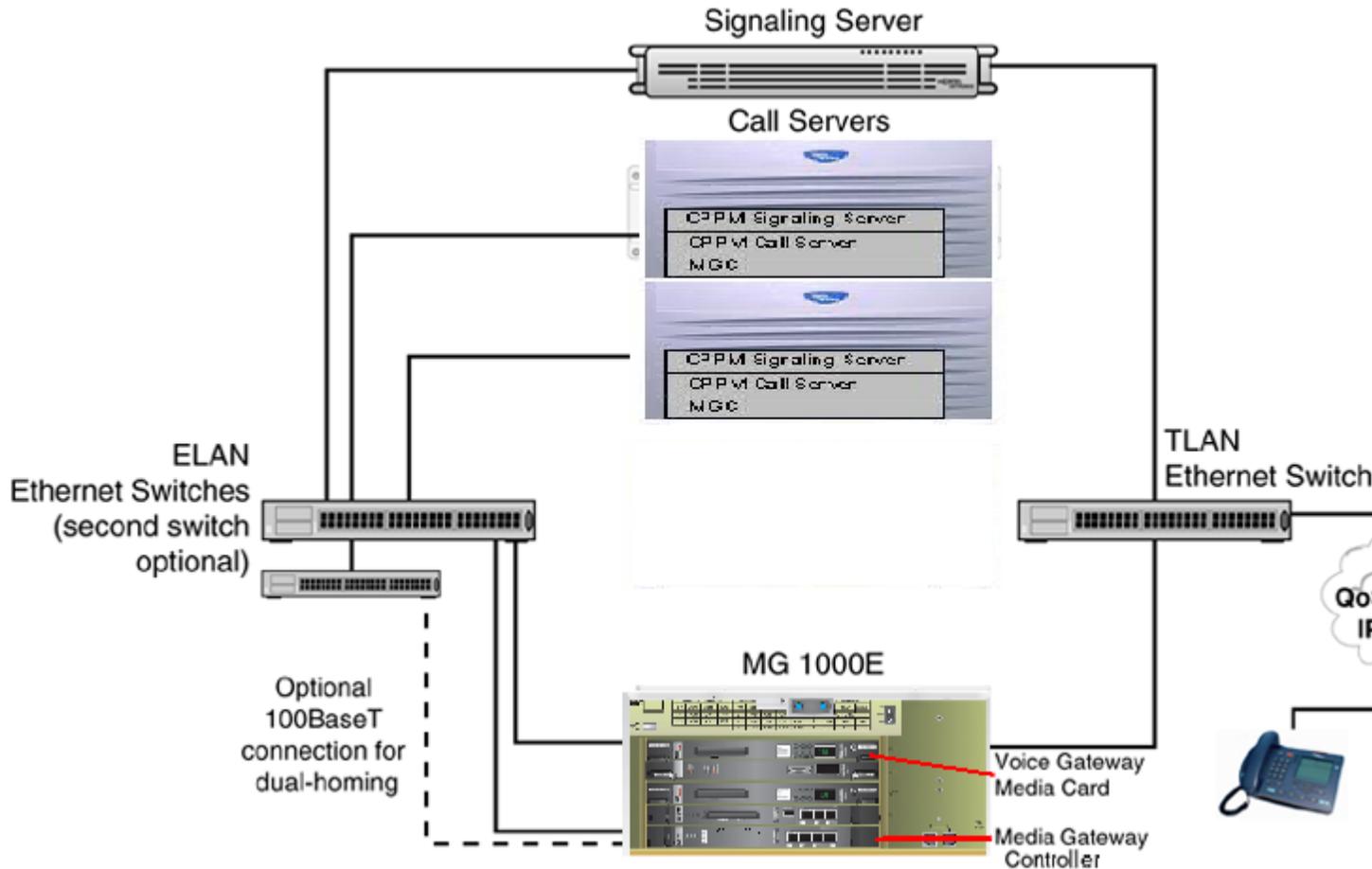
Figure 11: Network connections on MG 1000E

The separate Local Area Network (LAN) subnets that connect the Media Gateways and the Servers to the customer IP network are as follows:

- ELAN subnet. The ELAN subnet (100BaseT, full-duplex) is used to manage signaling traffic between the Call Server, Signaling Server, and Media Gateway 1000s. The ELAN subnet isolates critical telephony signaling between the Call Servers and the other components.

- TLAN subnet. The TLAN subnet (100BaseT, full-duplex) is used to manage voice and signaling traffic. It connects the Signaling Server and Voice Gateway Media Cards to the enterprise IP network. It also isolates the IP Telephony node interface from broadcast traffic.

System types

CS 1000 software uses a unique system type number for each Server configuration. The following table lists CS 1000E system types.

Table 5: CS 1000E system types

Hardware platform configuration	System type
CP PIV	3621
CP PM	4021
CP PM Co-res CS and SS	4121
CP DC Co-res CS and SS	4221
CP MG 32 Co-res CS and SS	4321
CP MG 128 Co-res CS and SS	4421
COTS2 Co-res CS and SS	4521

Signaling Server

The Signaling Server provides a central processor to drive Session Initiation Protocol (SIP), and H. 323 signaling, IP Phone signaling, and IP Peer Networking in the CS 1000E system. The Signaling Server has both an ELAN and a TLAN network interface, and communicates with the Call Server through the ELAN subnet.

Communication Server 1000 supports the following Signaling Server hardware platforms:

- Server cards
  - Common Processor Pentium Mobile (CP PM) card
  - Common Processor Dual Core (CP DC) card
- Commercial off-the-shelf (COTS) servers
  - Industrial Business Machines (IBM) X306m server (COTS1)
  - Hewlett Packard (HP) DL320-G4 server (COTS1)
  - IBM x3350 server (COTS2)
  - Dell R300 server (COTS2)

✳ **Note:**

All Signaling Server hardware platforms can support the stand-alone Linux-based Signaling Server configuration. The first-generation COTS servers do not support the Co-resident Call Server and Signaling Server configuration.

The Signaling Server provides signaling interfaces to the IP network using the following software components:

- SIP/H.323 Signaling Gateways

- IP Phone Terminal Proxy Server (TPS)
- Network Routing Service (NRS)
- Element Manager
- Application Server for Personal Directory, Redial List, and Callers List for IP Phones

Common Processor Pentium Mobile (CP PM) server

The Common Processor Pentium Mobile (CP PM) card is a Server card for use in a CS 1000 system. The NTDW61 and NTDW99 single slot CP PM card models support the CS 1000E system.

The CP PM card can reside in any IPE slot in a supported Media Gateway except for slot 0. Slot 0 is dedicated to the Gateway Controller.

The CP PM card configured as a Signaling Server has the following components:

- Intel Pentium M processor (1.4 Ghz)
- 40 GB Internal hard drive
- hot-pluggable Compact Flash (CF) card slot in the faceplate
- 2 Gb of SDRAM
- One 1 Gb/s Ethernet port
- Two 100BaseT Ethernet ports
- Two serial ports
- One USB port

The CP PM card requires a minimum 40 GB hard drive, 2 GB RAM, and BIOS version 18 to support the Linux-based Signaling Server configuration.

The CP PM card supports the Standard Availability Call Server, High Availability Call Server, stand-alone Signaling Server, and the Co-resident Call Server and Signaling Server configurations.

For more information about the CP PM card hardware components, see *Circuit Card Reference, NN43001-311*.

Common Processor Dual Core (CP DC) server

The Common Processor Dual Core (CP DC) card is a Server card for use in a CS 1000 system. The CP DC card replaces the existing Common Processor Pentium Mobile (CP PM) card. The NTDW53 single slot CP DC card supports the CS 1000E system.

The CP DC card can reside in any IPE slot in a supported Media Gateway except for slot 0. Slot 0 is dedicated to the Gateway Controller.

The CP DC card contains a dual core AMD processor and upgraded components which can provide improvements in processing power and speed over existing Server cards. The CP DC card provides performance improvements in MIPS, maximum memory capacity, and network transfer rates.

The CP DC card includes the following main components:

- AMD Athlon 64 X2 1.8 Ghz dual core processor

- 2 GB DDR2 RAM (expandable to 4 GB)

- 160 GB SATA hard drive (Server file system)

- Three faceplate USB 2.0 ports (for installations, upgrades, patches, and USB keyboard and mouse support)

- One faceplate VGA port (monitor support)

- Two faceplate Gigabit Ethernet ports

- Faceplate status LED and card reset buttons

The NTDW53 CP DC card is designed for the CS 1000E Media Gateway. The NTDW54 CP DC card is designed for the CS 1000M IPE Universal Equipment Module (UEM). A different faceplate and separate product code (NTDW54AAE6) are required to install a CP DC in a large system IPE UEM. You also require a bulkhead cable adapter (NTDW69AAE5) for the Ethernet ports.

The CP DC card is required for some CS 1000 Signaling Server applications, such as Avaya Media Server.

The CP DC card requires the Linux base Operating System, and supports the Co-resident Call Server and Signaling Server, or stand-alone Signaling Server configurations. The CP DC card does not support the standard or high availability Call Server configuration.

✳ **Note:**

The CP DC card only stores a single BIOS image. During an upgrade, there is a risk that a sudden loss of power or other corruption could render the card unserviceable.

For more information about the CP DC card hardware components, see *Circuit Card Reference, NN43001-311*.

Common Processor Media Gateway (CP MG) server

The Common Processor Media Gateway (CP MG) card is a Server card for use in a CS 1000E system. The CP MG card functions as a Server, a Gateway Controller, and provides Digital Signal Processor (DSP) resources.

The CP MG card is available in two versions:

- NTDW56BAE6 - CP MG card with 32 DSP ports (CP MG 32)

- NTDW59BAE6 - CP MG card with 128 DSP ports (CP MG 128)

The CP MG card provides improvements in port density and cost reductions by functioning as a Call Server or Application Server and a Gateway Controller with DSP resources while only occupying slot 0 in a Media Gateway. The CP MG card supports all CS 1000 IPE cards, and supports the full suite of CS 1000 telephones.

The CP MG card includes the following main components:

- Intel EP80579 integrated processor, 1200 Mhz (Common Processor)
- 2 GB DDR2 RAM (expandable to 3 GB)
- 160 GB SATA hard drive (Server file system)
- Mindspeed Chagall-2 processor M82515 (Gateway Controller)
- Compact Flash card (ATA) (Gateway Controller file system)
- Mindspeed Picasso M82710 (32 port) or Matisse M82910 (128 port) DSP resources
- Embedded Ethernet switch (links the Server to the Gateway Controller)

The CP MG card faceplate provides a USB 2.0 port, two Server serial ports, two Ethernet ports, status LEDs, a four character display, and reset buttons. The CP MG card backplane provides two Ethernet ports, and three serial ports.

The Common Processor component of the CP MG card provides the Server functions. The Gateway Controller component of the CP MG card is based on the same architecture as the Media Gateway Controller (MGC) card and uses the common MGC loadware. The Gateway Controller component of the CP MG card registers to the Server with an IPMG type of MGS.

The CP MG card requires the Linux base Operating System, and supports the Co-resident Call Server and Signaling Server, and CS 1000E TDM configurations. The CP MG card does not support the stand-alone Signaling Server, CS 1000E standard availability, or CS 1000E high availability Call Server configurations.

For more information about the CP MG card hardware components, see *Circuit Card Reference, NN43001-311*.

IBM X306m server

The International Business Machines (IBM) X306m 1U server is a rack-mounted, Pentium 4, PC-based, industry-standard, commercial off-the-shelf (COTS) server.

The IBM X306m 1U server has the following components:

- Intel Pentium 4 processor (3.6 GHz)
- Two 80 GB simple swap Serial ATA hard drives (1 drive configured)
- 8 GB of RAM PC4200 DDR II by means of 4 DIMM slots (2 GB configured)
- Two 1 Gb/s Ethernet ports
- One DVD-COMBO (DVD/CD-RW) drive
- One serial port
- Four USB ports

HP DL320-G4 server

The Hewlett Packard (HP) DL320-G4 1U server is a rack-mounted, Pentium 4, PC-based, industry-standard, commercial off-the-shelf (COTS) server.

The HP DL320-G4 1U server has the following components:

- Intel Pentium 4 processor (3.6 GHz)
- Two 80 GB SATA Hard drives (1 configured)
- 4 GB PC2-4200 ECC DDR2 SDRAM (2 GB configured)
- Two 10/100/1000BaseT Ethernet ports
- One CD-R/DVD ROM drive
- One serial port
- Three USB ports

IBM x3350 server

The IBM x3350 server is a rack-mounted, Intel Core 2 Quad CPU, commercial off-the-shelf (COTS) server.

The IBM x3350 server has the following components:

- Intel Core 2 Quad CPU –2.66GHz
- 250Gb RAID 1 Array (2x 250Gb Hard Drives, Hot-Swappable)
- 4Gb Memory
- CD-RW/DVD Drive
- Redundant Power Supply (Hot-Swappable)
- Dual GigaBit Ethernet Ports
- BIOS and RAID settings preconfigured for Avaya applications

Dell R300

The Dell R300 server is a rack-mounted, Intel Quad Core Xenon CPU, commercial off-the-shelf (COTS) server.

The Dell R300 server has the following components:

- Intel Quad Core Xenon CPU –2.5GHz
- 250Gb RAID 1 Array (2x 250Gb Hard Drives, Hot-Swappable)
- 4Gb Memory

- CD-RW/DVD Drive
- Redundant Power Supply (Hot-Swappable)
- Dual 1Gbit Ethernet Ports
- BIOS and RAID settings preconfigured for Avaya applications

Signaling Server software applications

The Signaling Server runs the following software applications:

- Terminal Proxy Server (TPS) on page 50
- SIP/H.323 Signaling Gateways on page 50
- Network Routing Service (NRS) on page 51
- SIP Proxy on page 52
- SIP Line on page 52
- #unique_107
- Element Manager on page 53
- NRS Manager on page 53
- Application Server for Personal Directories on page 53
- IP Media Services on page 53

Terminal Proxy Server (TPS)

The Terminal Proxy Server (TPS) acts as a signaling gateway between the IP Phones and the Call Servers using the UNIStim protocol. It performs the following functions:

- Converts the IP Phone UNIStim messages into messages the Call Server can interpret.
- Allows IP Phones to access telephony features provided by the Call Server.

   * **Note:**

   UNIStim stands for the Unified Networks Internet protocol Stimulus.

The TPS also controls the IP Phone registration.

SIP/H.323 Signaling Gateways

SIP/H.323 Signaling Gateways are software components configured on virtual loops, similar to IP Phones. SIP/H.323 Signaling Gateways bridge existing call processing features and the IP network. They also enable access to the routing and features in the MCDN feature set.

   * **Note:**

   The SIP/H.323 Signaling Gateway must register with the Network Routing Service (NRS).

> **⊛ Note:**
>
> Virtual TNs enable you to configure service data without hardwiring IP Phones to the CS 1000E system. Virtual TNs are configured in LD 97.

To support IP Peer Networking in a CS 1000E system, the Call Server must be associated with Signaling Servers that run SIP/H.323 Signaling Gateway software (see *IP Peer Networking Installation and Commissioning, NN43001-313* for details). The number of Signaling Servers required depends on the capacity and level of redundancy required.

Network Routing Service (NRS)

NRS is offered in two versions: a SIP Redirect Server NRS and a SIP Proxy NRS.

The SIP Redirect Server NRS is hosted either co-resident with Signaling Server applications, or in a stand-alone mode on a dedicated Common Processor Pentium Mobile (CP PM) server running the VxWorks™ real-time operating system.

The SIP Proxy NRS is hosted in a stand-alone mode on a dedicated commercial off the shelf server running the Linux™ real-time operating system. The SIP Proxy NRS is referred to as the Linux-based NRS.

The NRS application provides network-based routing, combining the following into a single application:

- H.323 Gatekeeper: The H.323 Gatekeeper provides central dialing plan management and routing for H.323-based endpoints and gateways.
- SIP Redirect Server: The SIP Redirect Server provides central dialing plan management and routing for SIP-based endpoints and gateways.
- NRS Database: The NRS database stores the central dialing plan in XML format for both the SIP Redirect Server and the H.323 Gatekeeper. The SIP Redirect Server and H.323 Gatekeeper both access this common endpoint and gateway database.
- Network Connection Service (NCS): The NCS is used only for Virtual Office, Branch Office, and Geographic Redundancy solutions.
- NRS Manager web interface: The NRS provides its own web interface to configure the SIP Redirect Server, the H.323 Gatekeeper, and the NCS.

The NRS application provides routing services to both H.323 and SIP-compliant devices. The H.323 Gatekeeper can be configured to support H.323 routing services, while the SIP Redirect Server can be configured to support SIP routing services.

The H.323 Gatekeeper and the SIP Redirect Server can reside on the same Signaling Server. Examples of H.323 and SIP-compatible endpoints needing the services of the NRS are CS 1000E. The NRS also supports endpoints that do not support H.323 Registration, Admission, and Status (RAS) or SIP registration with the NRS.

> **⊛ Note:**
>
> Systems that do not support H.323 RAS procedures and H.323 Gatekeeper procedures are referred to as non-RAS or static endpoints.

Each CS 1000E in an IP Peer network must register to the NRS. The NRS software identifies the IP addresses of PBXs based on the network-wide numbering plan. NRS registration eliminates the need for manual configuration of IP addresses and numbering plan information at every site.

SIP Proxy

CS 1000 software has a transaction stateful SIP Proxy to the IP Peer Network.

A SIP Proxy acts as both a server and a client. A SIP Proxy receives requests, determines where to send the requests, and acting as a client on behalf of SIP endpoints, passes requests to another server.

A SIP Proxy makes the following features and functionality possible:

1. Transport Layer Security (TLS).

   TLS provides the NRS with private, secure signaling, message authentication, confidentiality, and integrity through end-to-end encryption of media exchanged between two SIP endpoints.

2. Mixed transport layer protocol.

   A mixed transport layer protocol enables gateways using TCP, TLS over TCP, or UDP to interoperate.

3. Network features.

   By default the SIP Proxy and Redirect Server functions as a SIP Proxy. However, an endpoint can request transaction by transaction that the SIP Proxy act as a SIP Redirect Server.

   A SIP Redirect Server receives requests, but does not pass the requests to another server. Instead, a SIP Redirect Server sends a response back to the SIP endpoint, indicating the IP address of the called user.

4. Post-routing SIP URI modification.

5. Transaction forking.

SIP Line

The SIP Line Service fully integrates Session Initiation Protocol (SIP) endpoints in the CS 1000 system and extends the CS 1000 telephony features to the SIP IP Phones. The SIP Line Service comprises three components:

- The SIP Line Universal Extension (UEXT) called SIPL on the Call Server.
- The SIP Line Gateway (SLG) application.
- The system management interface (Element Manager) used to configure and manage the SIP Line Service.

For more information about SIP Line, see *SIP Line Fundamentals, NN43001-508*.

Element Manager

Element Manager is a software application that provides a web interface to support administration of system components, including the Signaling Server. With Element Manager, single web pages provide access to information traditionally spread throughout multiple overlays.

Element Manager provides tools to configure and maintain the following components:

- Call Servers
- Media Gateway, Expander
- MG 1000B
- Signaling Servers
- Voice Gateway Media Cards

NRS Manager

NRS Manager is a web-based management application used to configure, provision, and maintain the NRS. Key usability improvements introduced in the Linux-based NRS Manager are:

- Enhanced searching and sorting capabilities including wild cards and selectable scope of the search
- Capability to copy and move routing entries
- Simplified configuration for geographic redundancy
- Routing tests are fully integrated with endpoint and routing entry configuration
- SIP phone context mapping tools are fully integrated with endpoint and routing entry configuration
- Security infrastructure provided by the Enterprise Common Manager framework

For more information, see *Network Routing Service Installation and Commissioning, NN43001-564*.

Application Server for Personal Directories

The Application Server maintains the database for the Personal Directory, Caller's List, and Redial List features for UNIstim IP Phones. These features provide the following functionality:

- Personal Directory: stores up to 100 entries per user of user names and DNs.
- Callers List: stores up to 100 entries per user of caller ID information and most recent call time.
- Redial List: stores up to 20 entries per user of dialed DNs and received Call Party Name Display with time and date.

IP Media Services

In traditional TDM-based systems, media services such as conference mixing and media playback are provided by TDM hardware cards (MIRAN, XCT, and MGC). Delivering these services to IP endpoints requires many digital signaling processors (DSPs) to translate between the TDM backplane and IP voice packets.

IP Media Services provides IP versions of these services to the Communication Server (CS) 1000E by using the Avaya Media Server as the IP media service delivery platform. The Avaya MS supplies media services by using both secure and non-secure Real-time Transport Protocol (sRTP and RTP) channels controlled by the Call Server and Signalling Server, which map the Avaya MS resources to existing virtual TNs. The Avaya MS is an IP-based media server and therefore does not require DSPs for delivering IP media services to IP endpoints.

IP Media Services is installed with the Signaling Server application and enabled using Element Manager.

For more information, see *Signaling Server IP Line Applications Fundamentals, NN43001-125*.

Functional description

The Signaling Server provides the following functionality:

- provides IP signaling between system components on the LAN

- enables the Call Server to communicate with IP Phones

- supports key software components (see Signaling Server software applications on page 50)

Operating parameters

The Signaling Server provides signaling interfaces to the IP network using software components that run on the VxWorks operating system.

The Signaling Server can be installed in a load-sharing, survivable configuration.

The total number of Signaling Servers that you require depends on the capacity and redundancy level that you require.

Terminal Server

The optional MRV IR-8020M IP-based Terminal Server provides the Call Server with standard serial ports for applications and maintenance.

Physical description

Figure 12: Terminal Server on page 55 shows the Terminal Server.

Figure 12: Terminal Server

Hardware components

The MRV Terminal Server provides 20 console ports for modular RJ-45 connectors. It is also equipped with one RJ-45 10BaseT connection for network interface to the ELAN subnet and an internal modem to provide remote access.

Operating parameters

Traditionally, serial ports are used to connect terminals and modems to a system for system maintenance. As well, many third-party applications require serial port interfaces to connect to a PBX. Because the Call Server provides only two local serial ports for maintenance purposes, an IP-based Terminal Server is required to provide the necessary serial ports.

The Terminal Server provides standard serial ports for applications. These applications include billing systems that analyze Call Detail Recording (CDR) records, Site Event Buffers (SEB) that track fault conditions, and various legacy applications such as Property Management System (PMS) Interface and Intercept Computer applications. In addition, serial ports are used to connect system terminals for maintenance, modems for support staff, and printers for system output.

The Terminal Server is configured to automatically log in to the active Call Server at start-up. For this reason, each Call Server pair requires only one Terminal Server. Customers can configure up to 16 TTY ports for each Call Server pair.

The Terminal Server can be located anywhere on the ELAN subnet. However, if the Terminal Server is used to provide local connections to a Com port on the Call Server, it must be collocated with the system.

The Terminal Server can also be used as a central point to access and manage several devices through their serial ports.

> 🛈 **Important:**
> Currently, the CS 1000E only supports the MRV IR-8020M commercial Terminal Server.

Layer 2 switch

The Layer 2 Ethernet switch transmits data packets to devices interconnected by Ethernet to the ELAN or TLAN subnets. The switch only directs data to the target device, rather than to all attached devices. Layer 2 Ethernet switches are customer supplied components. You must ensure your network can support the ELAN and TLAN subnets required for a CS 1000E system. For more information, see *Converging the Data Network with VoIP Fundamentals, NN43001-260*.

Chapter 6: Configuration options

Contents

Introduction

The IP-distributed architecture of the Avaya Communication Server 1000E enables flexibility when it comes to component location.

The Server card occupies one slot in a Media Gateway. You can deploy a single call processor CS 1000E Standard Availability (SA) configuration, a dual redundant processor, CS 1000E High Availability (HA) configuration, or a Co-resident Call Server and Signaling Server configuration.

Given this flexibility, the CS 1000E offers many configuration options to support increased system redundancy. The CS 1000E can be deployed in many ways in LAN and WAN environments. Although many different installations are possible, most fall into one of the following categories:

- Multiple buildings in a campus

    - Campus-distributed Media Gateways
    - Campus Redundancy
- Multiple sites

    - Central Call Server with Branch Office
    - Geographic Redundancy

The following sections describe each of these configuration options.

> **✱ Note:**
>
> The following configurations provide CS 1000E systems with many options for redundancy and reliability. Careful planning is required to determine which configuration is right for your needs.

> **✱ Note:**
>
> Earlier, CS 1000 could connect to an Avaya Aura® Session Manager for connectivity to an Aura environment and other CS 1000 systems, release 7.5 and later, and an NRS functioning only as an H.323 gatekeeper. CS 1000 can now be connected to both a Session Manager and an NRS for SIP Redirect Service or SIP Proxy Service. SIP Redirect Service or SIP Proxy Service provides connectivity to CS 1000 systems earlier than Release 7.5. The NRS may still act as an H.323 gatekeeper for CS 1000 systems in the Aura network.
>
> This model is called the Routing Service Gateway model. For more information about the Routing Service Gateway model, see *Configuring Routing Service Gateway*.

Standard Availability deployment

A CS 1000E system configured with one stand-alone call processor (Standard Availability). illustrates a typical CP PM based CS 1000E SA system.
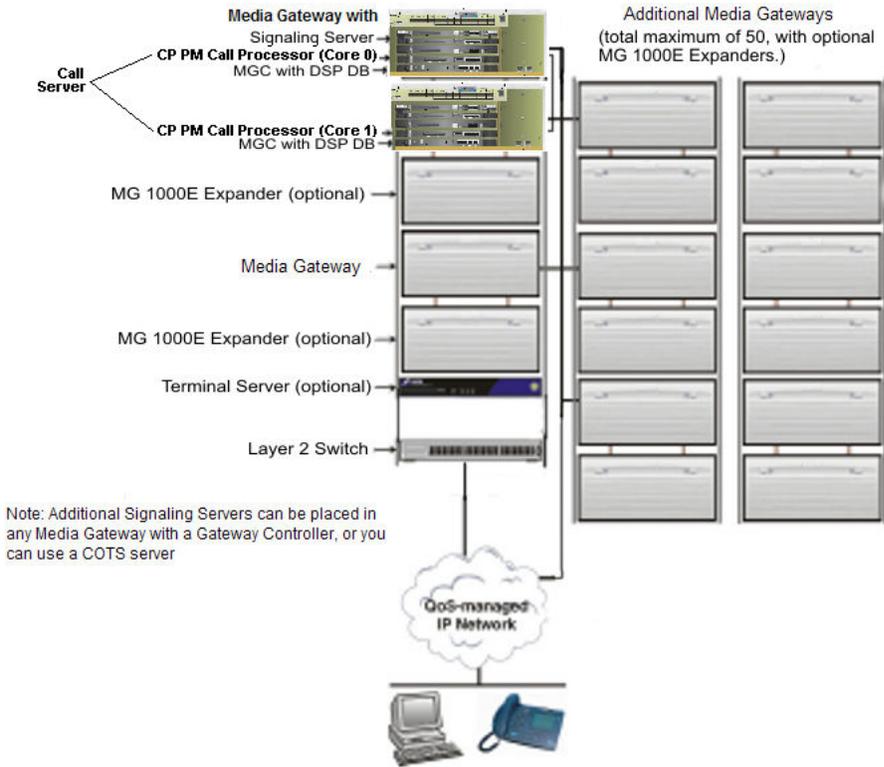
Figure 13: CS 1000E Standard Availability

High Availability deployment

The following figure shows the main components of a typical CS 1000E High Availability system.
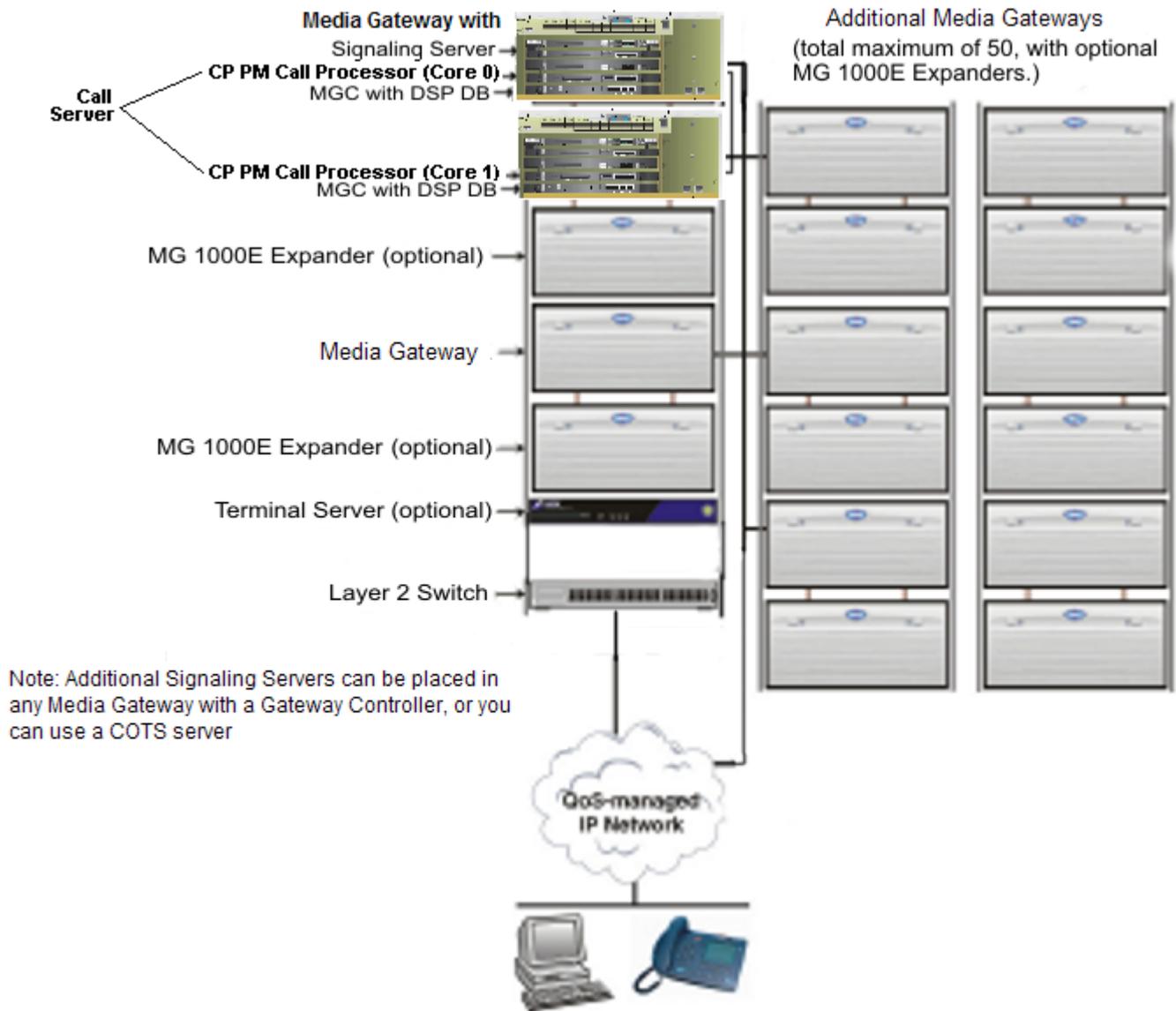
Figure 14: CS 1000E High Availability

The CS 1000E HA system provides core processing capability and IP functionality. It includes:

- Call Server containing dual CS 1000E Call Processors (Core 0 and Core 1)
- 1 to 50 Media Gateways and optional Media Gateway Expanders
- Signalling Servers (total number required depends on capacity and survivability levels)
- an MRV Terminal Server (optional)

- Layer 2 Ethernet Switches

Co-resident Call Server and Signaling Server deployment

The Co-resident Call Server and Signaling Server (Co-res CS and SS) can run the Call Server software, the Signaling Server software, and System Management software on one Server running the Linux base operating system. The hardware is deployed similar to an SA system, however only one Server is required. The single Server is functioning as the Call Server and the Signaling Server. The Co-res CS and SS configuration can be deployed in a Main Office or a Branch Office.

For CS 1000, the Co-res CS and SS supports various hardware platforms, see Table 1: Hardware platform supported roles on page 13. For more information about Co-res CS and SS systems, see *Co-resident Call Server and Signaling Server Fundamentals, NN43001-509*.

Campus-distributed Media Gateway deployment

With multiple buildings in a campus, you can distribute a Communication Server 1000E system across a campus IP network.Figure 15: Campus-distributed Media Gateways on page 62 shows Media Gateways distributed across multiple buildings in a campus setting.
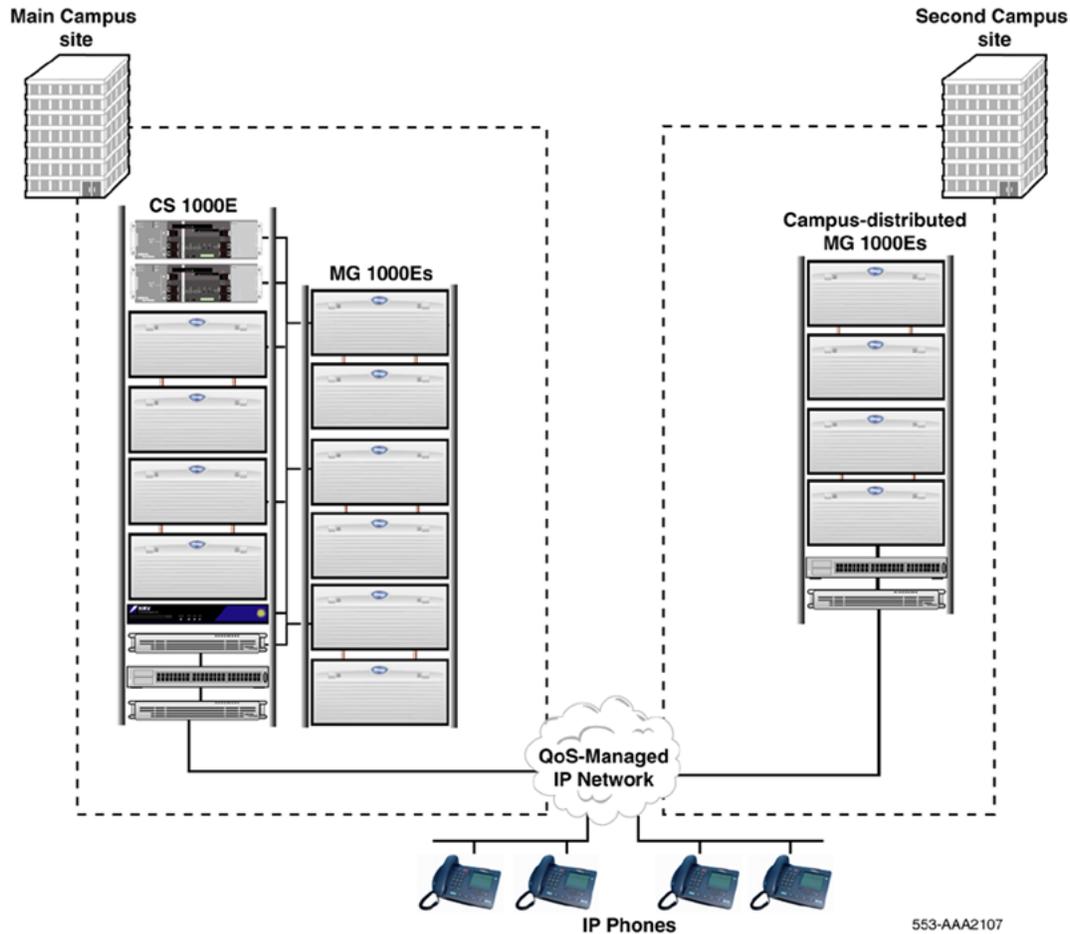
Figure 15: Campus-distributed Media Gateways

In this configuration, a CS 1000E system is installed at the main site, and additional Media Gateways and an optional Signaling Server are installed at a second campus site. All IP Phones are configured and managed centrally from the main site.

Campus Redundancy deployment

With Campus Redundancy, customers can separate Call Server core 0 and core 1 across a campus IP network. This provides additional system redundancy within a local configuration. The Call Server function normally and the inactive Call Processor assumes control of call processing if the active Call Processor fails.

To do this, the ELAN subnet and the subnet of the High Speed Pipe (HSP) are extended between the two Call Processor using a dedicated Layer 2 Virtual LAN configured to meet specified network parameters. shows a CS 1000E system in a Campus Redundancy configuration.
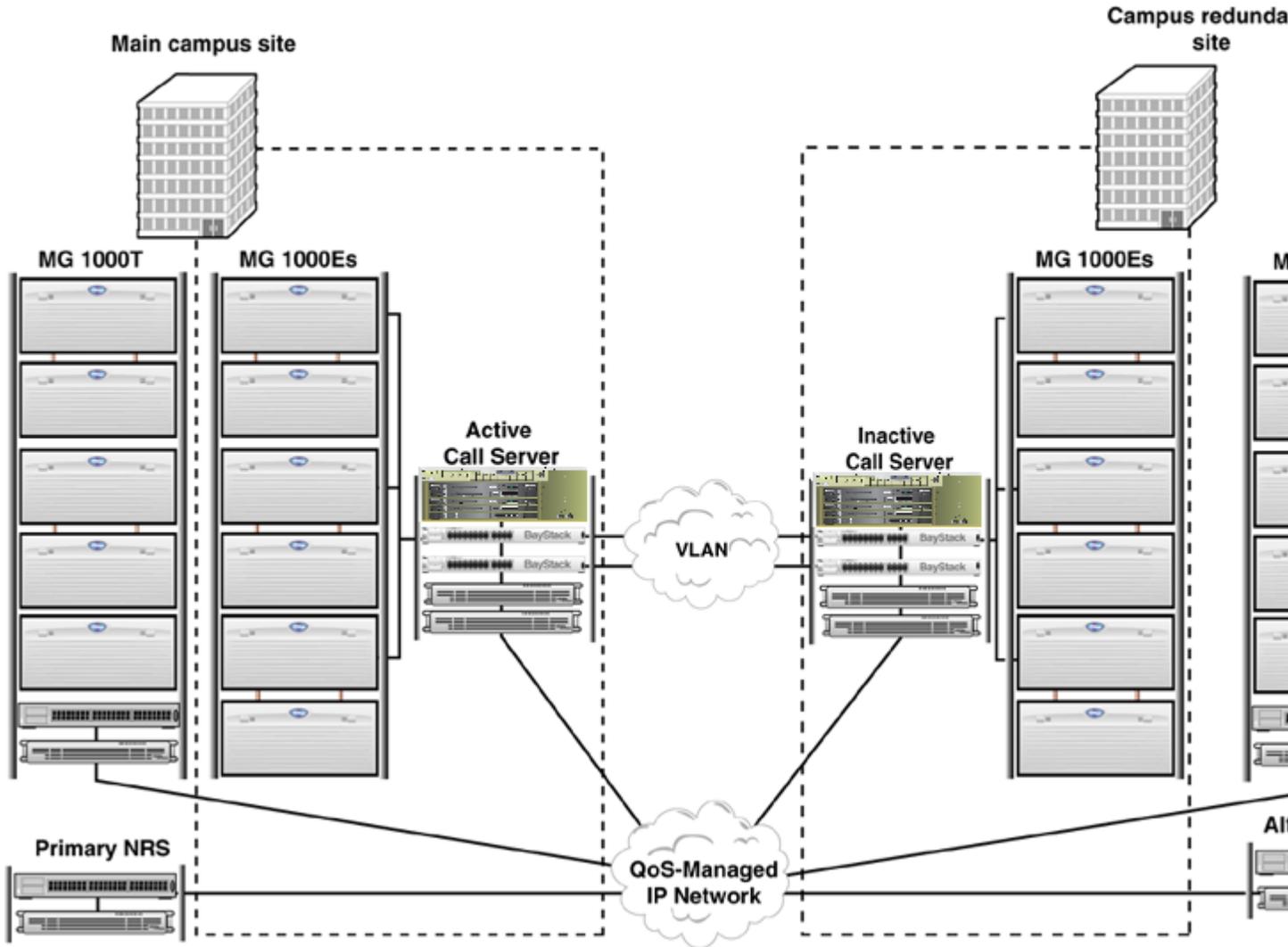
Figure 16: Campus Redundancy configuration

For more information on *Campus Redundancy, see System Redundancy Fundamentals, NN43001-507*.

Branch Office Media Gateway deployment

The CS 1000E system supports the Branch Office feature, which provides central administration of Media Gateway 1000B (MG 1000B) at remote sites. on page 64 shows a CS 1000E system with an MG 1000B installed at a remote branch office.
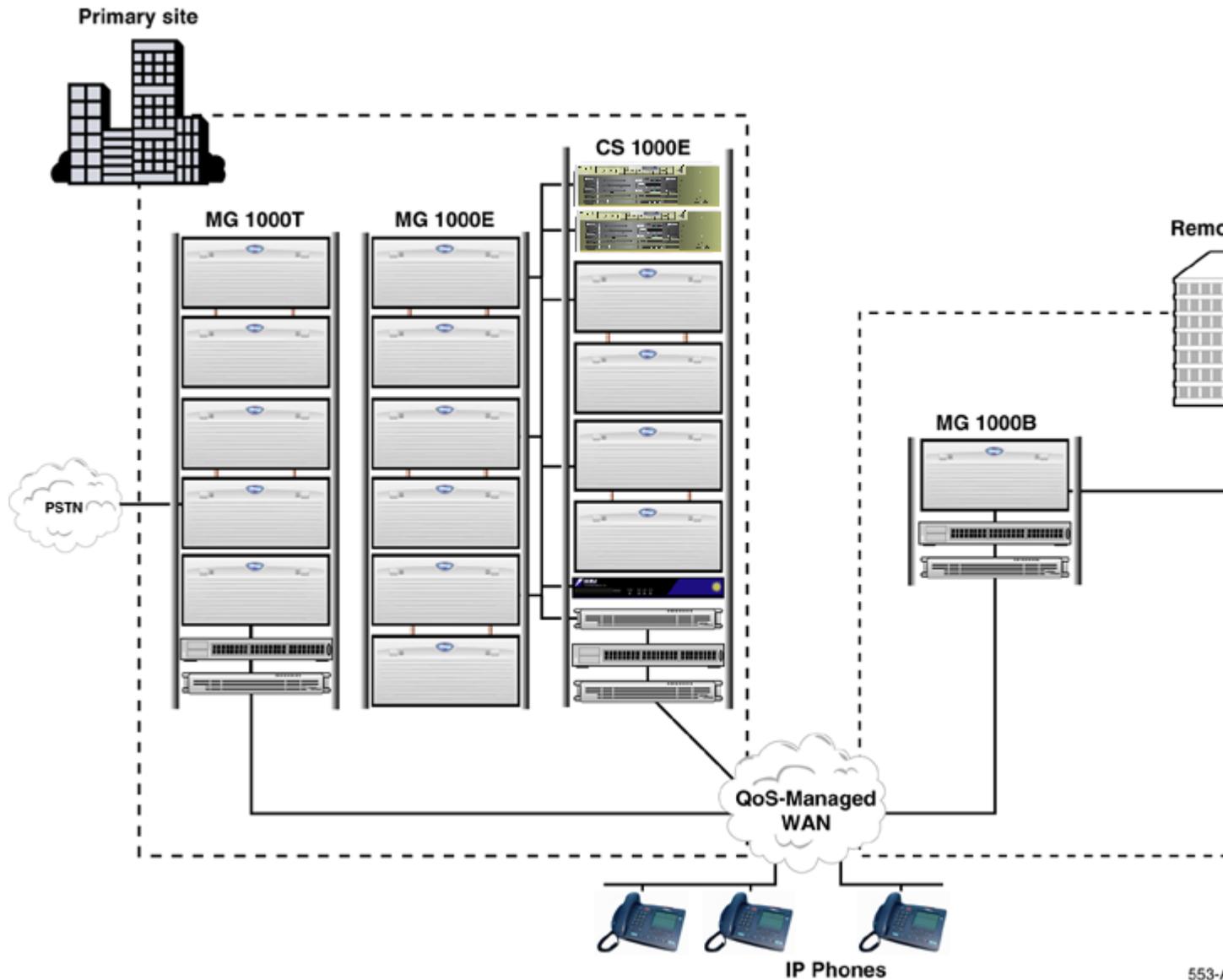
Figure 17: Branch Office configuration

In this configuration, the MG 1000B is survivable. This ensures that telephone service remains available if the main office fails. For more information, refer to *Branch Office Installation and Commissioning, NN43001-314*.

Geographic Redundancy deployment

Geographic Redundancy provides an additional layer of system redundancy. It allows a customer to locate a secondary backup system at a distance from a primary system. This ensures redundancy in the event of catastrophic failure of the primary site. With Geographic Redundancy, the configuration and user database of the primary system can be replicated across the WAN.

Figure 18: Geographic Redundancy on page 65 shows an inactive CS 1000E system backing up an active system using Geographic Redundancy.

* **Note:**

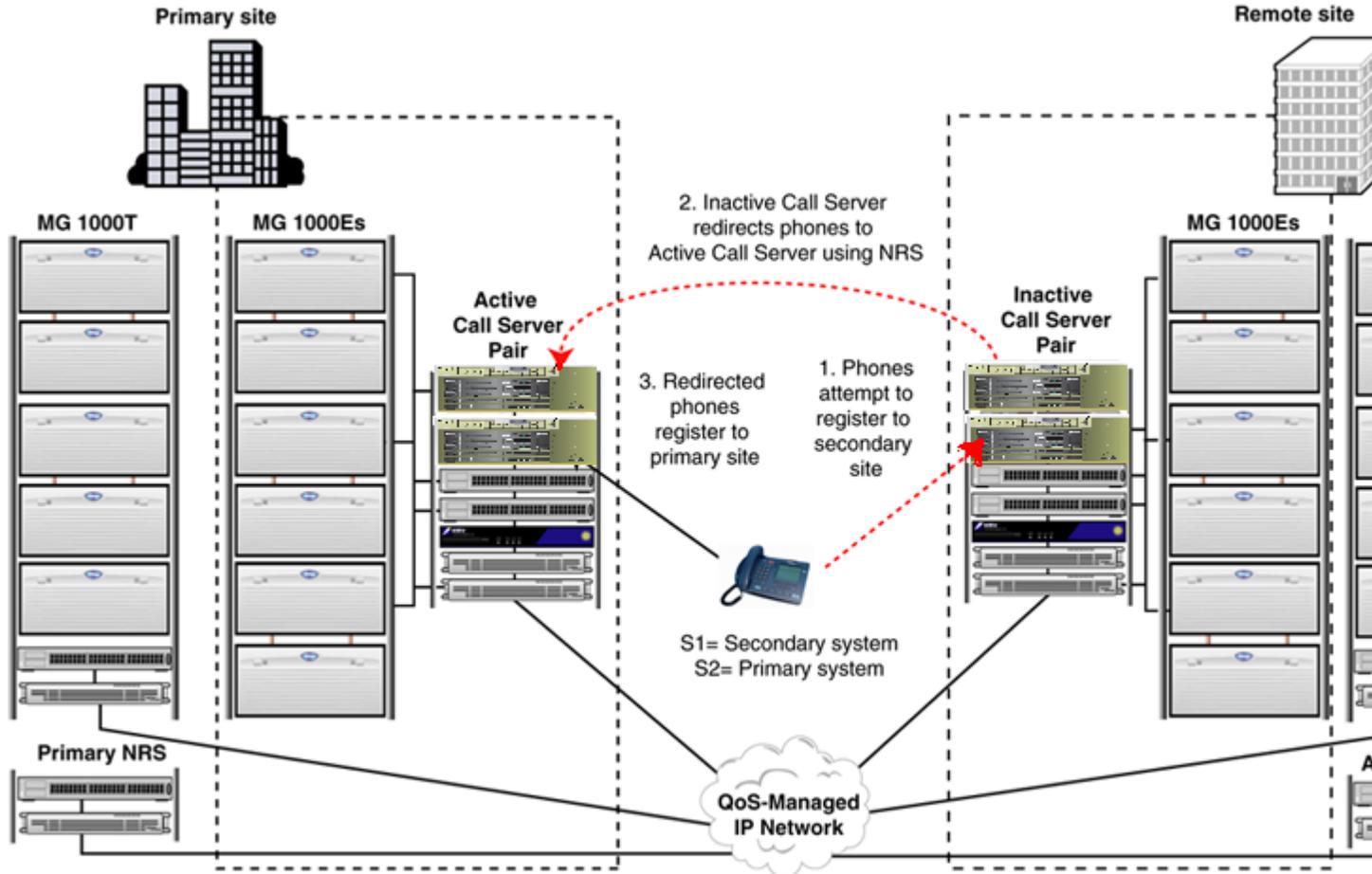Geographic Redundancy provides redundancy for IP Phones only.

Figure 18: Geographic Redundancy

For more information on Geographic Redundancy, see *System Redundancy Fundamentals, NN43001-507*.

High Scalability configuration

The CS 1000E High Scalability (HS) solution provides a centralized deployment model to allow network consolidation with a solution that provides business continuity while minimizing management overhead. This solution offers increased scalability for supporting large Communication Server 1000 networks. Figure 19: CS 1000E High Scalability on page 66 illustrates the architecture of a high scalability solution at a single Data Center.

CS 1000E High Scalability (HS)
Architecture

Data Center

HA Group 1

CPU 0

CPU 1

HA Pair Call Server

Signaling Server
(such as client TPS or SIP GW)

Element
Manager HS

Routing to Network
NRS/SPS

NRS

NRS routes between
HA Groups and to other
NRS servers

HA Group *n* • • •

CPU 0

CPU 1

HA Pair Call Server

Signaling Server
(such as client TPS or SIP GW)

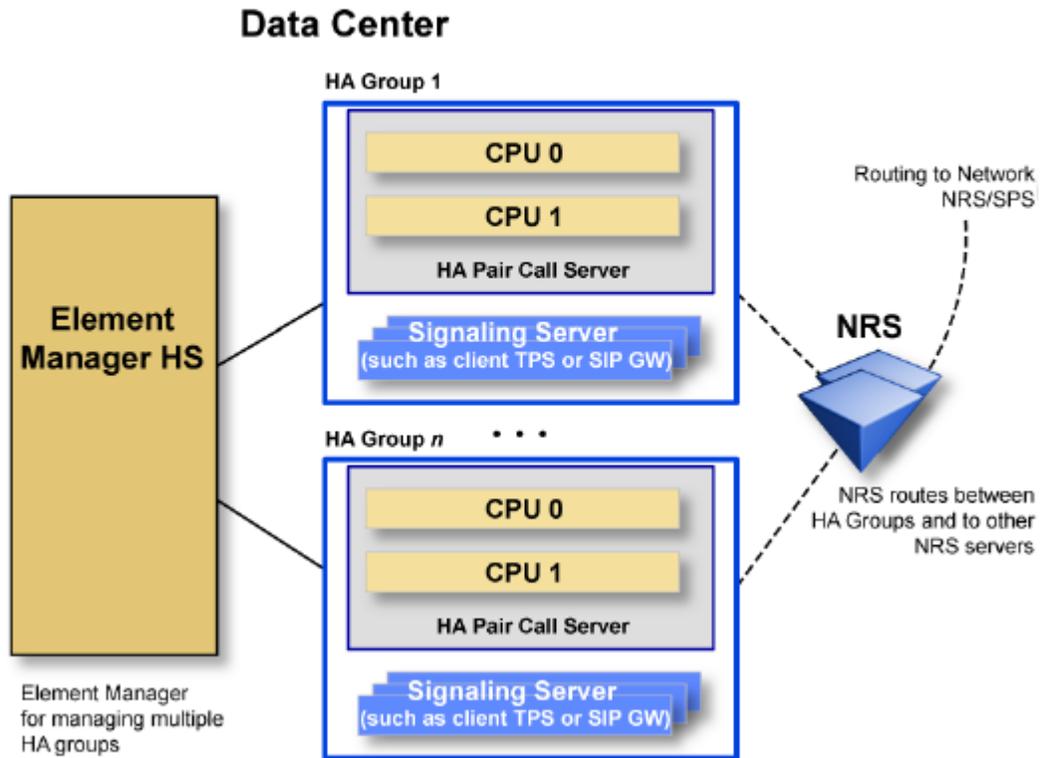Element Manager
for managing multiple
HA groups

Figure 19: CS 1000E High Scalability

You can deploy a CS 1000E HS with Campus Redundancy, Geographic Redundancy, or with multiple HA systems dispersed geographically.

For more information about CS 1000E High Scalability, see *Avaya Communication Server 1000E Planning and Engineering - High Scalability Solutions, NN43041-221* and *Avaya Communication Server 1000E High Scalability Installation and Commissioning, NN43041-312*.