

# HiPath 8000 V2.2

## Overview Guide

**SIEMENS**

Global network of innovation



1P A31003-H8022-T102-1-7618

**The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. The trademarks used are owned by Siemens AG or their respective owners.**

**The customer is responsible for ensuring that the system is installed/maintained in accordance with all the existing local country regulations and laws.**

## History of Changes

Document Version	Date	Summary
1	September 2006	First Release of V2.2

# History of Changes

# Content

<b>History of Changes</b> .....	<b>0-1</b>
<b>List of Figures</b> .....	<b>0-9</b>
<b>List of Tables</b> .....	<b>0-11</b>
<b>1 Important Notices</b> .....	<b>1-1</b>
1.1 About This Book .....	1-1
1.1.1 Purpose of this Book .....	1-1
1.1.2 How to Use This Guide .....	1-1
1.2 Related Information .....	1-2
1.3 Documentation Feedback .....	1-3
1.3.1 For U.S. Market Only .....	1-3
1.3.2 Countries other than U.S. ....	1-3
<b>2 HiPath 8000 Overview</b> .....	<b>2-1</b>
2.1 HiPath 8000 Main Components .....	2-2
2.2 HiPath 8000 Features .....	2-8
2.2.1 Features Highlights .....	2-8
2.2.2 Features Summary .....	2-10
2.3 HiPath 8000 Interfaces .....	2-14
2.4 System Scalability .....	2-16
2.5 Security .....	2-16
2.6 Quality of Service (QoS) .....	2-17
2.7 Reliability and Availability .....	2-18
2.7.1 Hardware Redundancy .....	2-18
2.7.2 Software Redundancy .....	2-18
<b>3 HiPath 8000 Hardware</b> .....	<b>3-1</b>
3.1 System Configurations .....	3-1
3.1.1 HiPath 8000 Base System .....	3-2
3.1.1.1 Intel Xeon processors .....	3-2
3.1.1.2 Memory .....	3-2
3.1.1.3 LEDs and Switches .....	3-4
3.1.1.4 External Ports .....	3-4
3.1.1.5 Hot-swap Redundant Power .....	3-6
3.1.1.6 System Management .....	3-6
3.1.2 IBM 346 Technical Specifications .....	3-6
3.1.3 Certified Ethernet Switches .....	3-8
<b>4 HiPath 8000 Software Functional Overview</b> .....	<b>4-1</b>
4.1 HiPath 8000 Base Software and Call Processing Applications .....	4-1
4.1.1 Resilient Telco Platform (RTP) .....	4-2

## Content

4.1.1.1	Important RTP Components	4-3
4.1.2	Universal Call Engine (UCE)	4-5
4.1.2.1	UCE Role	4-5
4.1.3	Signaling Managers	4-7
4.1.3.1	CSTA Signaling Manager	4-8
4.1.3.2	MGCP Signaling Manager	4-9
4.1.3.3	SIP Signaling Manager	4-10
4.1.4	Connection Control Manager	4-10
4.1.5	Services Logic Execution Environment (SLEE) for Native Services	4-10
4.2	HiPath 8000 Software Components	4-10
4.2.1	HiPath 8000 Software Features	4-11
4.2.2	HiPath 8000 Software Architecture	4-15
4.2.2.1	HiPath 8000 Active/Active Applications	4-16
4.2.3	HiPath 8000 Call Control and Signal Processing	4-17
4.2.3.1	Call Control	4-17
4.2.3.2	Service Control and Execution	4-18
4.2.3.3	Real-time Data Management	4-19
4.2.3.4	Call Resource Auditing	4-19
4.2.4	Comprehensive Endpoint Support	4-19
4.2.4.1	POTS	4-20
4.2.4.2	MGCP	4-20
4.2.4.3	Session Initiation Protocol (SIP)	4-20
4.2.5	Signaling Control and Processing	4-26
4.2.5.1	SIP-Q: QSIG Tunneled over SIP	4-26
4.2.5.2	SIP	4-27
4.2.6	Address Translation and Routing	4-29
4.2.6.1	Alternate Routing	4-29
4.2.6.2	Element Mass Provisioning	4-29
4.2.6.3	E.164 Directory Number Translation	4-30
4.2.6.4	Interchangeable NPA and NXX	4-30
4.2.6.5	Most-Matched Digit Translation	4-31
4.2.6.6	Origin Dependent Routing	4-31
4.2.6.7	Prefix Digit Translation	4-31
4.2.6.8	Private dialing and Numbering Plan (PNP) Support	4-32
4.2.6.9	Simultaneous Support for 7-Digit,10-Digit and 14-Digit Dialing	4-32
4.2.6.10	Vertical Service Code Translation	4-32
4.2.6.11	Zone Management	4-32
4.2.7	QoS Control	4-33
4.2.8	Operation, Administration, Maintenance, and Provisioning (OAM&P) Features	4-34
4.2.8.1	iSMC	4-35
4.2.8.2	iSSC	4-35
4.2.8.3	Call Detail Records	4-35
4.2.8.4	Rolling Upgrade	4-35
4.2.8.5	User Authorization, Authentication and Accountability	4-36

4.2.8.6	Software Packaging	4-37
4.2.8.7	Backup & Restore	4-37
4.3	HiPath 8000 Assistant Software	4-39
4.3.1	Software Deployment Details	4-39
4.3.2	HiPath 8000 Assistant – Context Overview	4-39
<b>5</b>	<b>Cluster Redundancy</b>	<b>5-1</b>
5.1	Cluster Redundancy Concept	5-1
5.2	Cluster Redundancy System Components	5-3
5.2.1	IBM 345/346 Linux	5-3
5.2.2	Ethernet Switch	5-4
5.2.3	Remote Supervisor Adapter (RSA)	5-4
5.3	Cluster Redundancy with Node Separation	5-4
5.4	Cluster Redundancy Basic Functionality	5-6
5.5	Process Configuration	5-8
5.5.1	RTP Startup Groups and Dependencies	5-9
5.5.2	RTP Alias Groups and Members	5-10
5.5.2.1	Equal Load Distribution	5-11
5.5.2.2	Local Equal Load Distribution	5-11
5.5.2.3	Exclusive Local Equal Load Distribution	5-11
5.5.2.4	Local Best Queue	5-11
5.5.2.5	Broadcast	5-11
5.5.2.6	Remote Broadcast	5-11
5.5.2.7	Backup alias	5-11
5.5.3	Contexts	5-12
5.6	HiPath 8000 Failover Strategy	5-12
5.6.1	Process Failover	5-13
5.6.2	Node Failover	5-13
5.6.3	Ethernet Card Failover	5-13
5.6.4	Ethernet Switch Failover	5-14
<b>6</b>	<b>Element and Network Management</b>	<b>6-1</b>
6.1	Element and Network Management Overview	6-1
6.1.1	Comprehensive Management Tools	6-2
6.1.1.1	Network Element Management System (EMS)	6-3
6.1.1.2	Configuration Management	6-4
6.1.1.3	Fault Management	6-4
6.1.2	Managing the HiPath 8000	6-4
6.1.3	Software Upgrades	6-5
6.1.4	Local and Remote Administration	6-5
6.2	Billing and Back Office Integration	6-6
6.2.1	Call Detail Records	6-6
6.2.1.1	Billing File Format	6-6
6.3	Script Capabilities	6-7
6.4	Security Features	6-7

## Content

6.4.1	CLI	6-7
6.4.2	iNMC User Security and Management	6-8
6.4.2.1	Node Groups	6-8
6.4.2.2	Access Profiles	6-8
6.4.3	iSMC User Management	6-9
6.4.3.1	Users and Roles	6-9
6.4.4	iSSC Security	6-10
6.4.4.1	Management Security	6-10
6.4.5	Transport Layer Security (TLS) Services	6-11
6.4.6	HiPath 8000 Assistant Security	6-11
6.5	iNMC Overview	6-12
6.5.1	iNMC Main Screen	6-13
6.5.2	iNMC Clients Per iNMC Server	6-14
6.6	HiPath 8000 Assistant	6-14
6.6.1	HiPath 8000 Assistant Home Page	6-14
6.6.2	HiPath 8000 Assistant Navigation Area	6-15
6.6.3	Menu Structure of the HiPath 8000 Assistant	6-16
6.7	Provisioning	6-17
6.7.1	HiPath 8000	6-17
6.7.1.1	Mass Provisioning	6-17
6.7.1.2	Private Numbering Plan	6-17
6.7.1.3	Rolling Upgrades	6-17
<b>7</b>	<b>Main and Extended Interface Components</b>	<b>7-1</b>
7.1	VoIP Session Border Controller	7-2
7.2	Firewalls	7-3
7.3	Media Servers	7-4
7.3.1	Integrated Media Server	7-4
7.3.2	IP Unity Meroon 6000 Media Server	7-5
7.3.2.1	IP Unity Meroon 6000 Media Server Hardware	7-6
7.3.2.2	IP Unity Applications	7-8
7.3.3	Convedia CMS 1000	7-9
7.4	Applications	7-10
7.4.1	ComAssistant S (TM)	7-10
7.4.2	OpenScope	7-11
7.4.3	Xpressions VM	7-11
7.5	Endpoints	7-12
7.5.1	optiPoint 410 S/420 S and WL2 S Standard SIP	7-12
7.5.2	optiClient 130 S	7-12
7.6	Gateways	7-13
7.6.1	RG 8700 Survivable Media Gateways	7-13
7.6.1.1	Steps to Assign an RG 8700 on the HiPath 8000	7-14
7.6.2	HiPath HG 3540 Serves as a SIP Gateway	7-15
7.6.3	Cisco 2621XM Multiservice Router for SIP Gateways	7-15
7.6.4	Secure Infrastructure for Remote Access (SIRA)	7-16



7.6.5 Survivable Branch Office . . . . .	7-16
7.6.6 RG 2700 Survivable Branch Office . . . . .	7-18
<b>8 System Performance and Sizing . . . . .</b>	<b>8-1</b>
8.1 Assumptions . . . . .	8-1
8.1.1 Call Modeling Criteria . . . . .	8-1
8.1.2 Performance as a Function of Number of Messages . . . . .	8-4
8.2 Performance and Sizing Data . . . . .	8-4
8.2.1 Overall Performance . . . . .	8-4
8.2.2 MTBF of Hardware . . . . .	8-5
8.2.3 Number of Ethernet Interfaces . . . . .	8-5
8.2.4 Database Sizing . . . . .	8-5
8.2.5 Context Sizing . . . . .	8-9
<b>9 Statistics, Accounting, and Diagnostics . . . . .</b>	<b>9-1</b>
9.1 Statistics and Accounting . . . . .	9-1
9.1.1 HiPath 8000 Level . . . . .	9-1
9.2 Monitoring Support . . . . .	9-2
9.2.1 Operational Measurements . . . . .	9-2
9.2.1.1 Traffic Measurements . . . . .	9-2
9.2.2 Call Trace . . . . .	9-3
9.3 Diagnostics Support . . . . .	9-3
9.3.1 Network Diagnostics . . . . .	9-3
<b>Index . . . . .</b>	<b>10-1</b>

# Content

## List of Figures

Figure 2-1	HiPath 8000 Standard Landscape . . . . .	2-3
Figure 2-2	The HiPath 8000 Compact Landscape with Integrated Media Server . . .	2-4
Figure 2-3	The HiPath 8000 Compact Landscape with Integrated Administration . . .	2-4
Figure 2-4	The HiPath 8000 Compact Landscape with a fully Integrated Media Server and Administration	2-5
Figure 2-5	The HiPath 8000 Assistant Manages Integrated Media Server and Administration	2-6
Figure 2-6	HiPath 8000 Interfaces . . . . .	2-15
Figure 3-1	HiPath 8000 Duplex Hardware Configuration . . . . .	3-1
Figure 3-2	IBM 346 Front View . . . . .	3-4
Figure 3-3	IBM 346 Port Numbers . . . . .	3-5
Figure 4-1	Software Complex Overview . . . . .	4-2
Figure 4-2	Role of the RTP middleware . . . . .	4-3
Figure 4-3	Application Software . . . . .	4-5
Figure 4-4	HiPath 8000 Universal Call Engine (UCE) Interfaces . . . . .	4-7
Figure 4-5	CSTA Implementation in the HiPath 8000 . . . . .	4-9
Figure 4-6	HiPath 8000 Software Architecture and Components . . . . .	4-15
Figure 4-7	Normal Active/Active Mode with RTP Support . . . . .	4-16
Figure 4-8	HiPath 8000 Call Processing Software Architecture . . . . .	4-17
Figure 4-9	Service Control and Execution Environment . . . . .	4-19
Figure 4-10	Hop-by-hop Application of TLS HiPath 8000 Back to Back User Agents	4-21
Figure 4-11	SIP Redirect Server Call Setup . . . . .	4-23
Figure 4-12	SIP Proxy Server Call Setup . . . . .	4-25
Figure 4-13	SIP Interface Block Diagram . . . . .	4-28
Figure 4-14	HiPath 8000 OAM&P Architecture . . . . .	4-34
Figure 4-15	HiPath 8000 Assistant Software Deployment . . . . .	4-39
Figure 4-16	HiPath 8000 Assistant Software Context . . . . .	4-40
Figure 5-1	Example of a HiPath 8000 System Architecture Configuration . . . . .	5-3
Figure 5-2	Cluster Redundancy Node Separation . . . . .	5-5
Figure 5-3	HiPath 8000 Redundancy Configuration . . . . .	5-7
Figure 5-4	HiPath Redundancy Configuration . . . . .	5-8
Figure 6-1	Billing Files Format . . . . .	6-6
Figure 6-2	iNMC EMS Structure . . . . .	6-12
Figure 6-3	iNMC Main Screen Components . . . . .	6-13
Figure 6-4	HiPath 8000 Assistant Home Page . . . . .	6-14
Figure 6-5	HiPath 8000 Assistant Navigation Area . . . . .	6-15
Figure 6-6	HiPath 8000 Assistant Menu Structure . . . . .	6-16
Figure 7-1	Juniper VF1000 Front and Back View . . . . .	7-2
Figure 7-2	Cisco PIX 535 Firewall . . . . .	7-3
Figure 7-3	Compact HiPath 8000 Assistant Media Server . . . . .	7-4

## List of Figures

Figure 7-4	IP Unity Mereon 6000 Chassis . . . . .	7-7
Figure 7-5	ComAssistant . . . . .	7-10
Figure 7-6	RG 8700 Deployment in Head and Branch Office Environments . . . . .	7-14
Figure 7-7	Cisco 2621 Front and Rear . . . . .	7-16
Figure 7-8	Branch Office Configuration . . . . .	7-17
Figure 8-1	HiPath 8000 Enterprise Single Switch . . . . .	8-2
Figure 8-2	HiPath 8000 Enterprise Network . . . . .	8-3
Figure 8-3	Compact HiPath 8000 Enterprise compact Switch . . . . .	8-3

## List of Tables

Table 1-1	HiPath 8000 Overview Chapter Descriptions . . . . .	1-1
Table 2-1	HiPath 8000 Features . . . . .	2-10
Table 3-1	IBM 346 Technical Specifications . . . . .	3-6
Table 4-1	HiPath 8000 Software Features . . . . .	4-11
Table 4-2	SIP Services . . . . .	4-20
Table 4-3	HiPath 8000 QoS Attributes . . . . .	4-33
Table 5-1	Process Elements . . . . .	5-9
Table 5-2	Failing Processes . . . . .	5-13
Table 6-1	HiPath 8000 CLI User Profile Components . . . . .	6-7
Table 6-2	iSMC Users . . . . .	6-9
Table 6-3	iSMC User Roles . . . . .	6-10
Table 8-1	HiPath 8000 V2.1 Protocols . . . . .	8-1
Table 8-2	HiPath 8000 Protocols and Configurations . . . . .	8-2
Table 8-3	Overall Performance . . . . .	8-4
Table 8-4	Trunk and Subscriber Limitations . . . . .	8-5
Table 8-5	Server Availability for IBM . . . . .	8-5
Table 8-6	Number of Ethernet Interfaces . . . . .	8-5
Table 8-7	Database Sizing . . . . .	8-6
Table 8-8	IBM x345/x346 Context Sizing . . . . .	8-9

## List of Tables

# 1 Important Notices

## 1.1 About This Book

### 1.1.1 Purpose of this Book

This book provides an overview of the HiPath 8000 from software and hardware perspectives. It describes product features, management tools, standards support, statistics, service and support, and product specifications.

The HiPath 8000 Overview is intended for users who want a high level overview of the general operations and functions of the HiPath 8000 system.

Users should be familiar with basic telecommunications equipment functionality.

### 1.1.2 How to Use This Guide

The following table describes the contents of this guide.

<b>Chapter</b>	<b>Description</b>
<a href="#">Chapter 2</a>	Introduces the components of the HiPath 8000 switch.
<a href="#">Chapter 3</a>	Describes the IBM hardware configuration needed to support the HiPath 8000.
<a href="#">Chapter 4</a>	Provides a comprehensive description of the software components that make up the HiPath 8000.
<a href="#">Chapter 5</a>	Defines the elements of Cluster Redundancy and details how the elements fit into the HiPath 8000.
<a href="#">Chapter 6</a>	Identifies the Element and Network Management functional interfaces such as the iNMC, iSMC/iSSC and CLI used to manage the HiPath 8000.
<a href="#">Chapter 7</a>	Lists and describes the Main (IP Unity Mereon 6000 Media Server/ applications, HiPath 4000 HG 3540 SIP-Q Gateway, Cisco SIP Gateway, RG 8700 Gateway, Convedia CMS-1000/, VoIP Session Border Controller and Firewalls) and extended (HiPath ComAssistant optiPoint 410 S/420 S phone family, Mediatrix 1400, AP1120, optiClient 130 S and SIRA) interface components.
<a href="#">Chapter 8</a>	Shows all the Performance and Sizing criteria for the HiPath 8000.
<a href="#">Chapter 9</a>	Presents the statistics, accounting, and diagnostics used with the HiPath 8000.

Table 1-1 HiPath 8000 Overview Chapter Descriptions

## **1.2 Related Information**

Related publications are as follows:

- *HiPath 8000 Call Detail Recording (CDR) Reference Guide*
- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Configuration and Definition Provisioning Worksheets*
- *HiPath 8000 Data Sheet*
- *HiPath 8000 Delta Specifications for Version 2.1*
- *HiPath Deployment Service Administration Manual*
- *HiPath 8000 E-911 Support and Planning Guide*
- *HiPath 8000 Feature Description Guide*
- *HiPath 8000 Master Glossary*
- *HiPath 8000, Master Index*
- *HiPath 8000 NetManager iSMC Customization Guide*
- *HiPath 8000 NetManager iSSC Installation and Customization Guide*
- *HiPath 8000 NetManager iNMC Server Installation, Administration and Utilities Guide*
- *HiPath 8000 Network Planning Guide*
- *HiPath 8000 Overview Guide*
- *HiPath 8000 SOAP/XML Subscriber Provisioning Interface Description Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 System Planning Guide*
- *HiPath 8000, Third Party Products Reference*
- *HiPath 8000 Traffic Measurements Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*
- *optiClient 130 S, V2.0, HiPath 8000/Cisco Proxy, Administrator Documentation and Operating Instructions*
- *optiPoint 150 S Administration Manual*



- *optipoint 150 S Operating Manual*
- *optiPoint 410/420 Advance S, V6.0 Administrator Manual*
- *optiPoint 410/420 Advance S, V6.0 User Manual*
- *optiPoint WL 2 Professional S, Administration Manual*
- *optiPoint WL 2 Professional S, Operating Manual*
- *OpenStage 60/80 User Manual*
- *OpenStage 60/80 Administration Manual*

## **1.3 Documentation Feedback**

### **1.3.1 For U.S. Market Only**

To report a problem with this document, call your next level of support:

- Customers should call the Siemens Customer Support Center (SCSC).
- Siemens employees should call the Interactive Customer Engagement Team (i-CET) or complete a Documentation Feedback Form on the LiveLink Product Documentation page.

When you call, be sure to include the following information. This will help identify which document you are having problems with.

- **Title:** HiPath 8000 V2.2, Overview Guide
- **Order Number:** A31003-H8022-T102-1-7618

### **1.3.2 Countries other than U.S.**

Please provide feedback on this document as follows:

- Submit a trouble ticket to ICTS, or
- Use the Document Feedback form that you can access from the front page of the HTML version of this document.

## **Important Notices**

*Documentation Feedback*

## **2 HiPath 8000 Overview**

HiPath is Siemens solutions and services offering, designed to give your business a practical approach to convergence. HiPath is the only solution in the market that provides open-standards for both pure Internet Protocol (IP) and hybrid systems, preserving maximum choice. The HiPath 8000 is the result of a Breakthrough project that initially developed a common softswitch base offered as the hiQ 8000.

This common software can be, depending on the target market, compiled for a Sun platform running Solaris (HiQ8000 for the Carrier market) or an IBM platform running LINUX (HiPath8000 for the Enterprise market). The current release of the HiPath 8000 is V2.1 which is equivalent to the hiQ 8000 Release 10.1.

This software contains specific features required for the Carrier and Enterprise customers as well as common features shared by both.

In addition, HiPath 8000 is an important component of Siemens' Vision LifeWorks, significantly increasing the productivity and effectiveness of business processes through the integration of communications solutions for carriers and enterprises. The core of the LifeWorks concept is the integration of home, business and carrier networks as well as wired and wireless networks.

By integrating communications among home offices, small offices, branch offices, regional offices, and headquarters, including Centrex-type solutions, and using new innovative and integrating products such as OpenScape, the Siemens solution thus creates a unified domain across both carrier and enterprise market segments.

This Chapter introduces you to the HiPath 8000 Release 2.1.

## HiPath 8000 Overview

### *HiPath 8000 Main Components*

## 2.1 HiPath 8000 Main Components

The HiPath 8000 () is a SIP-based real-time IP communication solution that can be deployed as either an enterprise solution or as a hosted service. Its main function is to provide carrier-grade universal switching and service delivery. The HiPath 8000 supports a wide range of VoIP signaling and call control protocols.

The HiPath 8000 is offered in two main configurations. The standard configuration [Figure 2-1](#) provides external Administration and Media Server support and is scalable from a few hundred to 100,000 users per individual system, and a virtually unlimited number of users per network.

For the smaller scale users (300 to 5000), the HiPath 8000 offers a compact configuration with three options:

1. A HiPath 8000 with an integrated Media Server [Figure 2-2](#) using the iNMC/iSMC administration server.
2. A HiPath 8000 with an integrated Administration system [Figure 2-3](#) with the HiPath 8000 V2.0 Assistant using the existing external Media Servers (IP Unity or Convedia).
3. A HiPath 8000 with a fully integrated Media Server and Administration system [Figure 2-4](#) using the HiPath 8000 Assistant V2.0.

The HiPath 8000 Assistant V2.0 combines the maintenance and administration functions of iNMC and iSMC with a single GUI interface. The tool runs on the same server as the HiPath 8000 and supports Web access to its functions, as well as a single point of access for the management of phones, media server and licenses.

The integrated Media Server supports redundancy and can be managed by the integrated HiPath 8000 Assistant V2.0 or by an iNMC/iSMC administration server.

Through Linux SuSE operating software, HiPath 8000 conforms to industry standards, and offers, alongside Session Initiation Protocol (SIP), unrestricted compatibility with all other commonly-used protocols, as well as with IBM x-Series standard hardware and Linux SuSE operating system software. Clustering software protects against both hardware and software failures and controls failover of active/standby Ethernet links and failover of cluster nodes. There is no single point of failure for the host hardware and software operating system. This ensures that all functions and applications maintain constant, unrestricted availability.

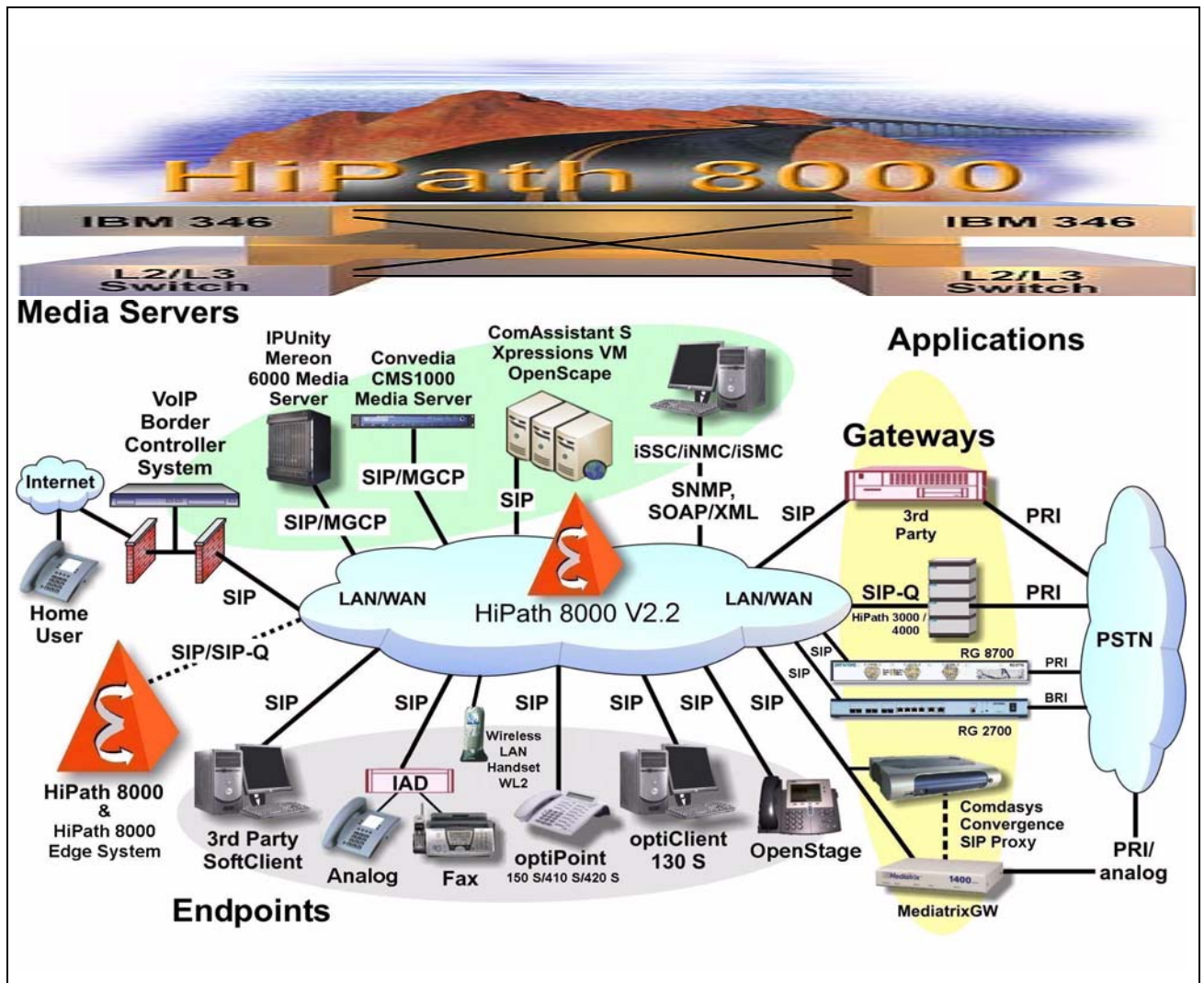


Figure 2-1 HiPath 8000 Standard Landscape

# HiPath 8000 Overview

## HiPath 8000 Main Components

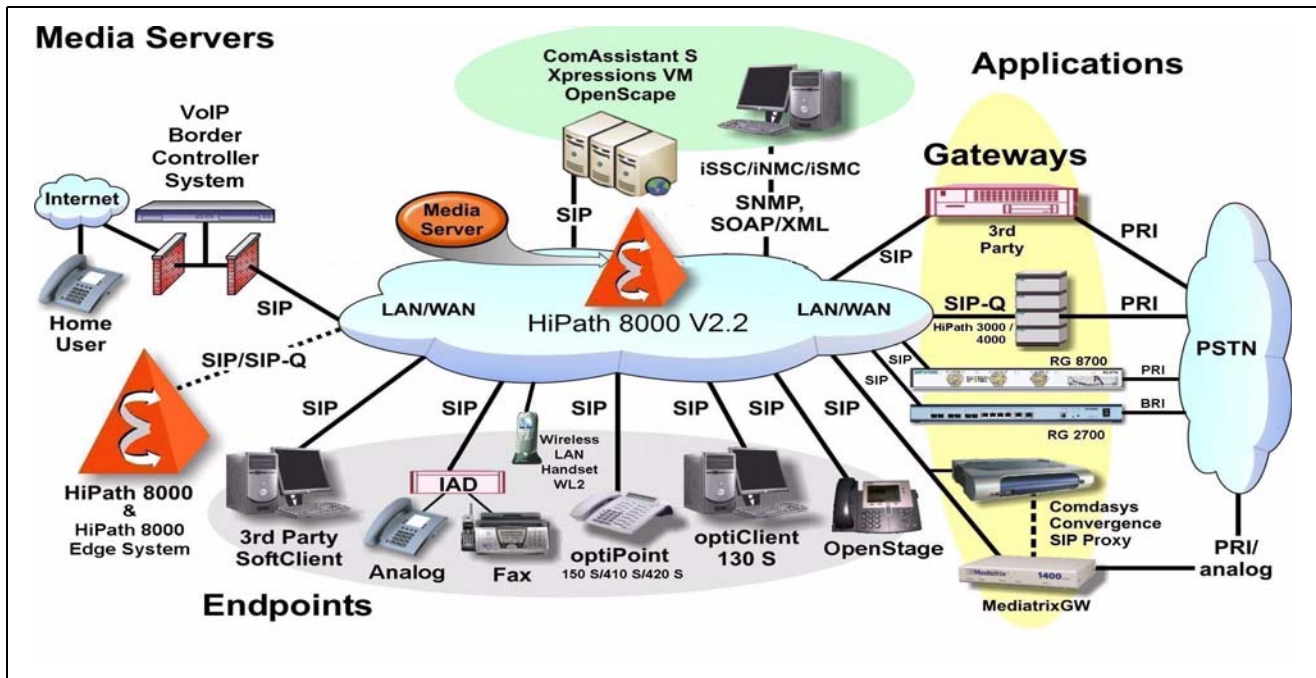


Figure 2-2 The HiPath 8000 Compact Landscape with Integrated Media Server

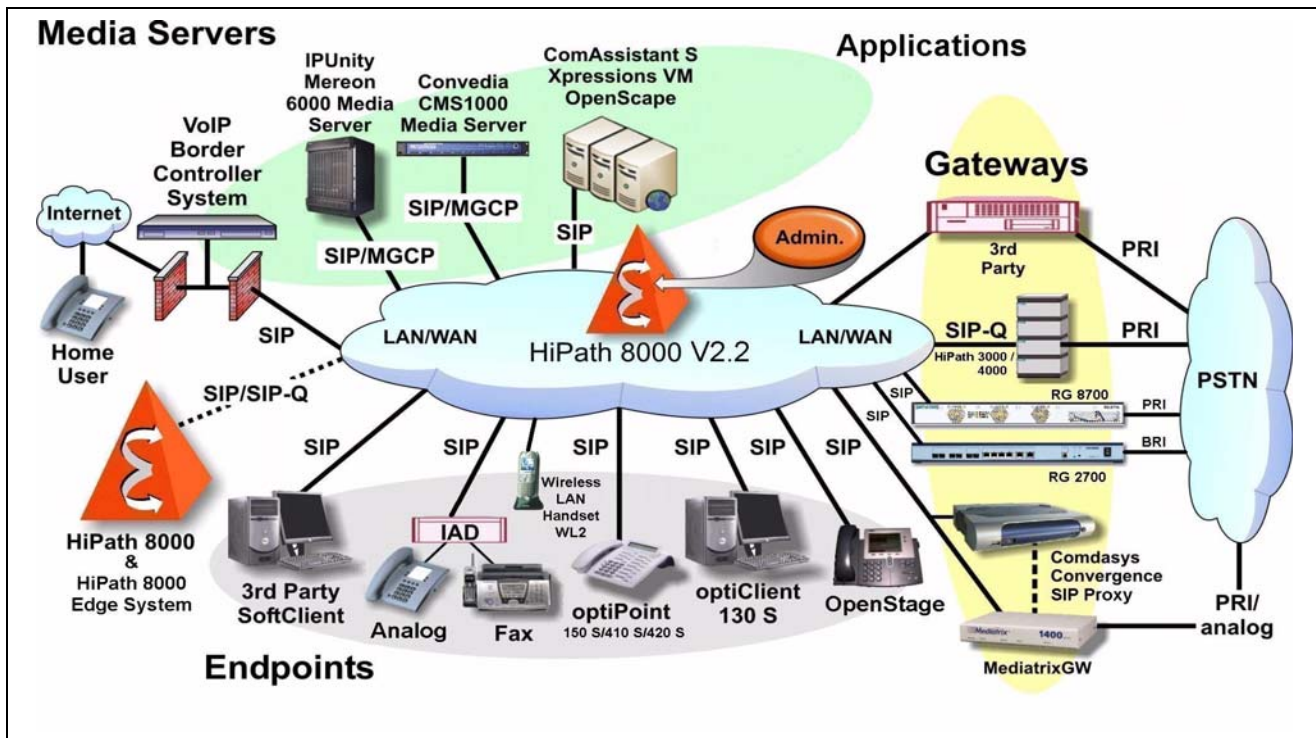


Figure 2-3 The HiPath 8000 Compact Landscape with Integrated Administration



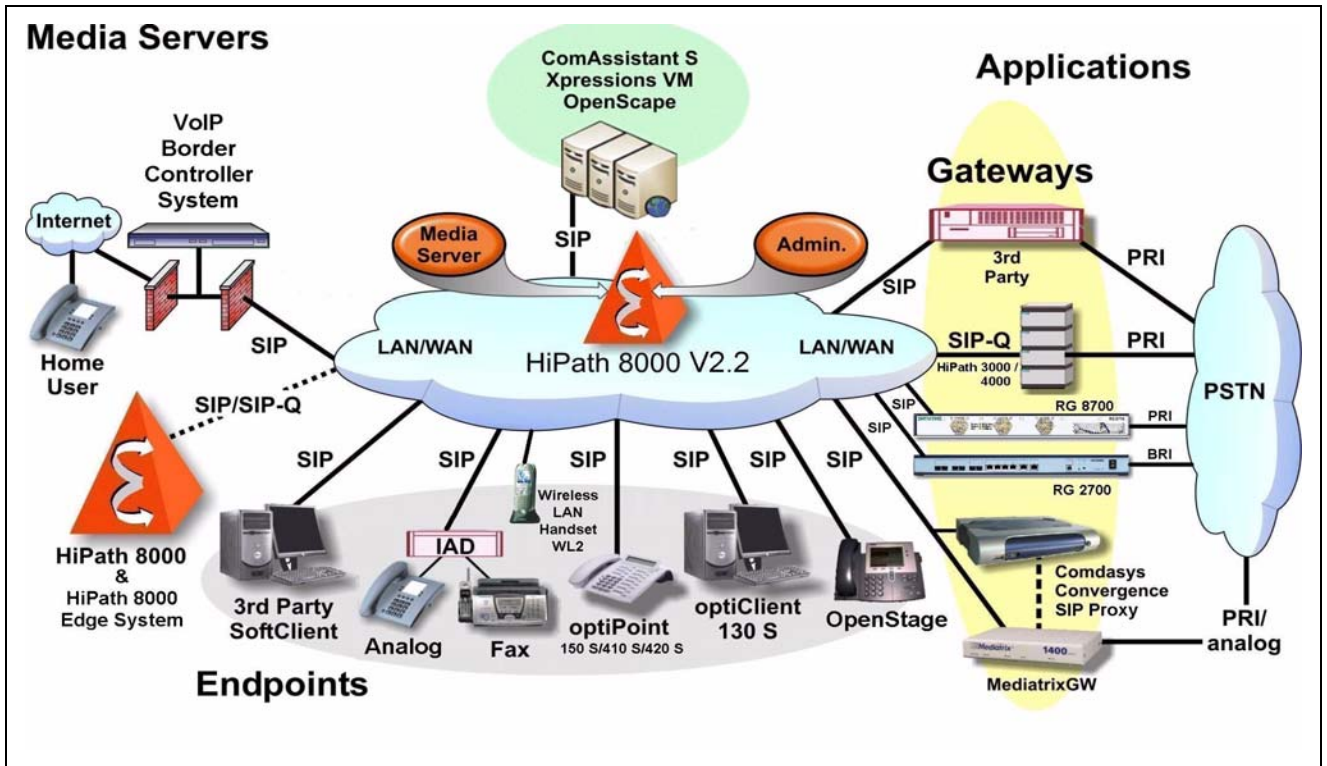


Figure 2-4 The HiPath 8000 Compact Landscape with a fully Integrated Media Server and Administration

## HiPath 8000 Overview

### HiPath 8000 Main Components

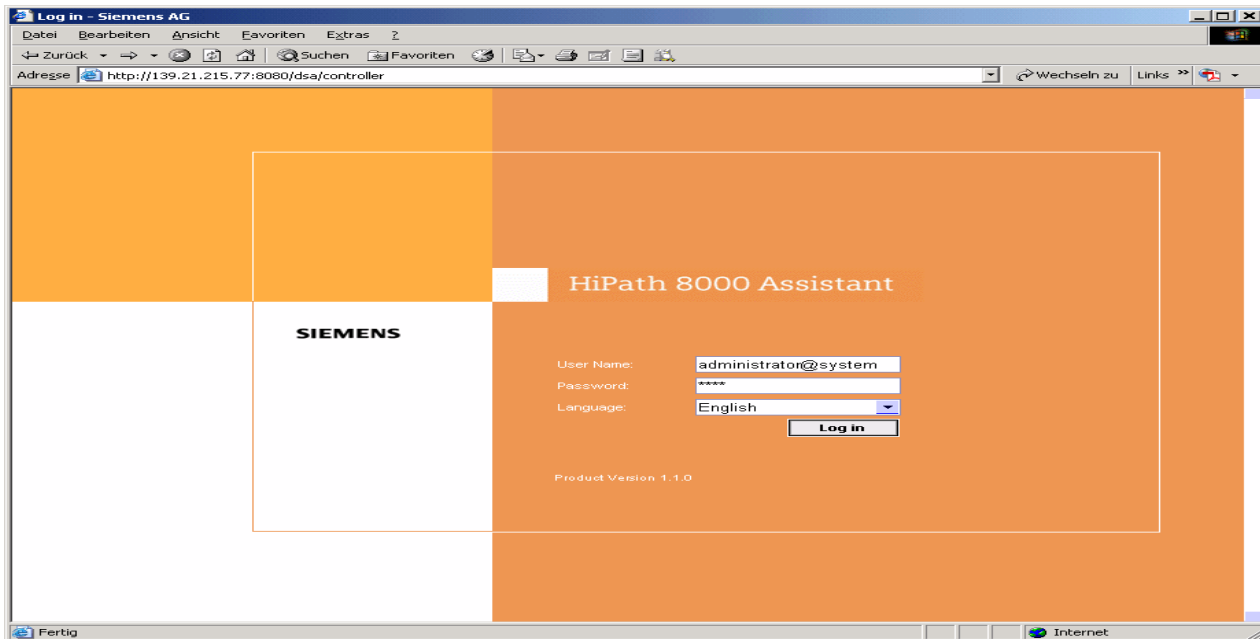


Figure 2-5 The HiPath 8000 Assistant Manages Integrated Media Server and Administration

The HiPath 8000 system landscape consist of:

- Two fully redundant IBM ® xSeries® 346 Cluster Servers with Novell's Linux SLES9 Operating Systems using a SolidTech Database offer flexibility, reliability and fast throughput. Note, redundancy is optional with the HiPath 8000 compact version using HiPath 8000 Assistant.
- L2/L3 Ethernet Switches efficiently handle Switched VLANS and IP routing functions.
- VoIP Session Border Controller (that is, Juniper VoiceFlow) offers security and control for calls originating from the Internet. The Siemens optiClient 130 S offers an optional internet interface solution for PC based voice and data communications.
- Media Servers (that is, IP Unity Mereon 6000 & 3000 V2.7 & V3.1 and Convedia CMS 1000 & 6000 or the functionality within the HiPath 8000 compact version provides numerous features (including tones and announcements), on a single platform, negating the need to deploy multiple systems.
- SIP Phones Endpoints support a comprehensive array of features and facilities, which provide the users with an easy to use and reliable communications environment, extending the capabilities made available by traditional TDM telephony. The optiPoint 410 S/420 S standard SIP phones with a wide range of features offer a continuity of features and support. In addition, the Siemens Deployment Service provides a HiPath Management application for administering workpoints.



- SIP Network Applications including Openscape, Xpressions VM and enhanced ComAssistant S.
- An Element Management System provides craft administration by means of the Service and Network Management Control Servers. The Network Management Center (NMC) application consists of an NMC server and NMC client which can serve as two separate administrator levels. The Service Management Center (iSMC) is closed application for the user administration of subscribers and other functions managed through system administrators. The NMC and SMC functionality is contained within the compact HiPath 8000 via the HiPath 8000 Assistant. Also, a Subscriber Self-Care (iSSC) is a toolkit that allows customers to create web-based services to support local switching requirements.
- A SIP-Q interface to the PSTN by means of the HiPath 4000/HG3540V2. The HiPath 4000 V3.0 Real Time IP System is the optimal solution for connecting traditional IP and TDM clients with SIP clients to HiPath 8000. HiPath 4000 functions as a media gateway and thus expands the operating possibilities of HiPath 8000.
- A SIP interface to the PSTN by means of the RG 8700 or RG 2700 Survivable Gateways or equivalent 3rd Party Gateways.
- A SIP or SIP-Q interface between HiPath 8000 networks.

## HiPath 8000 Overview

### *HiPath 8000 Features*

## 2.2 HiPath 8000 Features

### 2.2.1 Features Highlights

The HiPath 8000 offers numerous features including:

- **Complete Security System** which controls access and usage. For advanced options, the Siemens HiPath Security offers a comprehensive portfolio of products and services to create gap-less security plans.
- **Total Package of current Enterprise telephony features** that provides a software suite of features for the HiPath 8000 RealTime IP System. Alongside call processing features, it includes back-end connectivity for applications and management.
- **Comprehensive Management facilities** through Simple Network Management Protocol (SNMP) v2/3, command line interface (CLI), or Network Management Center (iNMC), Subscriber Management by the Service Management Center (iSMC) and Subscriber Self-Care (iSSC) web services performed by means of Simple Object Access Protocol (SOAP) over HyperText Transfer Protocol (HTTP). Also the HiPath MetaManagement is the comprehensive and wide-ranging management solution for unified administration of networks made up of HiPath Real Time IP Systems, applications and industry-standard third-party products. In addition, the compact HiPath 8000 incorporates the functionality of the iNMC and iSMC and media server into one communication platform using the HiPath 8000 Assistant and provides for upward migration of all administrative features.
- **Numerous Interfaces** for advanced services and applications, such as instant and multi-media messaging, presence services, billing services, collaboration services, call centers, hot desking, IBM Message Center, Xpressions, OpenScape and other enterprise applications.
- **HiPath 8000 Cold/Warm Standby** provides Stand-Alone-Service-Areas consisting of geographically co-located VoIP elements, which can be controlled by a mini-HiPath in case of loss of communication with the main HiPath 8000.
- **Offers total system redundancy with node separation** which reduces the risk of total loss of voice services when one of the nodes is out of service due to a fire, flood, hurricane, building damage, and so on.
- **Provides RG 8700 and HiPath 4000 gateways and supports gateways of other vendors** using standard interfaces such as SIP and SIP-Q and Interworking with third-party PBXs.
- **Resilient Telco Platform (RTP) middleware** provides continuous operation if one of the two nodes fails.
- **Advanced Routing and Rerouting** of SIP Calls based upon Quality and Costs and .provides the rerouting of SIP calls if a gateway cannot process a connection request

- **Automatic Configuration Control** provides a means to detect what kind of hardware is being installed, how many CPUs, how much memory, what type of Fast Ethernet cards, etc. thus avoiding the support different load builds for each of the server configurations.
- **Flexible Software Architecture** enables an easy integration into customer's data infrastructure.
- **Straightforward installation and operation** due to plug and play orientation and in-house self-maintenance, with automatic, progressive and complete backup and restore.
- **V2.1 DataBase Access Layer (DBAL) Optimization and Serviceability improvements** ensure better performance by reducing start-up time, provide more efficient error detection and recovery, improve connection handling and offer easier software maintainability and site serviceability.
- **V2.2 Enhancements for Executive-Assistant Workflow** provides enhancements to both HiPath 8000 and Siemens OptiPoint SIP endpoints, to support the different applications whereby a group of people, Executives and Assistants wish to work together in a specific arrangement for greater work efficiency.
- **V2.2 Improved MWI Delivery for Newly Registered Phones** provide the right MWI status to the phone after registration.
- **V2.2 Rapid Recovery of Failed Transport Layer Security (TLS) connections for SIP Endpoints** enhances the response to detect and recover the connection whenever the TLS connection is lost.
- **V2.2 Internal Static Call Admission Control (CAC)/ Bandwidth Management Solution for the HiPath 8000** serves the purpose of limiting the amount of bandwidth that is allowed to be used for media stream (i.e. RTP/voice and UDPLP/fax) traffic over bandwidth limited ("bottleneck") links in the network.
- **V2.2 Long Life Platform for the HiPath 8000** introduces new platforms, such as the IBM X.343, Fujitsu-Siemens or HP to replace the IBM X.345/IBM X.346 family as the platform for the HiPath 8000.
- **V2.2 HiPath 8000 Assistant Support for User Management** allows customers to integrate administrative tasks (MAC) across heterogeneous platforms.
- **V2.2 UA Registration During WAN Outage** provides SIP UA Registration Renewal during WAN Outage by improving connectivity for intermittent losses of connectivity by allowing SIP UA registrations to be "renewed" on a provisional basis.
- **V2.2 CDR Modifications for Enterprise Call Transfer Scenarios** shows the total time spent on extensions (when more than one is involved) contrasting the time spent on the trunk.
- **V2.2 OpenStage Phone support** offer the next generation of SIP phones replacing optiPoint 500, 410, 420 and 600.

## HiPath 8000 Overview

### HiPath 8000 Features

## 2.2.2 Features Summary

Table 2-1 summarizes the HiPath 8000 features.

<b>Signaling Protocol</b>	
<ul style="list-style-type: none"><li>● CSTA</li><li>● SIP-Q (SIP over QSIG)</li><li>● SIP</li></ul>	<ul style="list-style-type: none"><li>● QSIG allows legacy users to talk with SIP users. QSIG also supports notification when called party is idle and mixed platform single voicemail with MWI.</li></ul>
<ul style="list-style-type: none"><li>● Any-to-Any Signaling Mediation.</li></ul>	<ul style="list-style-type: none"><li>● Session Initiation Protocol (SIP) with transparent transport of SDP data</li></ul>
<ul style="list-style-type: none"><li>● Conventional H.245 and FastStart Signaling with Gateways and Endpoints.</li></ul>	<ul style="list-style-type: none"><li>● SIP for subscriber endpoint signaling. This includes VoIP phones, VoIP PC clients or Customer Premises Gateways.</li></ul>
<ul style="list-style-type: none"><li>● SIP/SIP-Q supports tandem traffic between HiPath 8000 networks</li></ul>	<ul style="list-style-type: none"><li>● SIP Over TCP (SIP servers and phones may connect by means of UDP or TCP; a combined UDP/TCP dispatcher is required.)</li></ul>
<b>Call Processing</b>	
<ul style="list-style-type: none"><li>● QoS Controls for Code C, Packetization Period, Service Type, Echo Cancellation, Resource Reservation, and Silence Suppression</li></ul>	
<b>Network</b>	
<ul style="list-style-type: none"><li>● Answer Timeout Timer for SIP</li><li>● T.38 FAX Support</li><li>● SIP/SIP-Q between HiPath 8000 networks</li></ul>	<ul style="list-style-type: none"><li>● Enhanced DTMF</li><li>● CSTA Optimization</li><li>● QSIG Call Back on Free</li></ul>
<b>Address Translation and Routing</b>	
<ul style="list-style-type: none"><li>● Most Matched Digit Translation</li></ul>	<ul style="list-style-type: none"><li>● Alternate Routing</li></ul>
<ul style="list-style-type: none"><li>● Dialing Plan Enhancements supporting multiple dialing plans per Business Group</li></ul>	<ul style="list-style-type: none"><li>● Origination Dependent Routing</li></ul>
<ul style="list-style-type: none"><li>● International, National, and Subscriber E164 Directory Number Translation</li></ul>	<ul style="list-style-type: none"><li>● Simultaneous Support for 7-Digit and 10-Digit Dialing</li></ul>
<ul style="list-style-type: none"><li>● Interchangeable NPA and NXX</li></ul>	<ul style="list-style-type: none"><li>● Station Dialing</li></ul>
<ul style="list-style-type: none"><li>● Keypad Operations</li></ul>	<ul style="list-style-type: none"><li>● Least Cost Routing</li></ul>
<ul style="list-style-type: none"><li>● Channel Selection</li></ul>	<ul style="list-style-type: none"><li>● Resource Allocation</li></ul>

Table 2-1 HiPath 8000 Features (Sheet 1 of 4)

<ul style="list-style-type: none"> <li>Private numbering plan which includes extension numbering up to 7-digits, L0, L1 and L2 region levels</li> </ul>	<ul style="list-style-type: none"> <li>Barrier Codes (for example, Off-Net, On-Net)</li> </ul>
<b>Emergency Calling Features</b>	
<ul style="list-style-type: none"> <li>Provides the ability to route emergency calls through the HiPath 4000 or Cisco gateways and to the Telident station translation system (STS) for emergency calling (E911) support.</li> </ul>	<ul style="list-style-type: none"> <li>Location Identifiers (LIN) provide location numbers for each line in a business group.</li> </ul>
<b>OAM&amp;P</b>	
<ul style="list-style-type: none"> <li>Automated Software Installation for Repeatability of Site Configurations with enhanced DVD Media Option</li> </ul>	<ul style="list-style-type: none"> <li>Mass Provisioning by means of Expert Mode CLI</li> <li>Real Time Trace (RTT) allows tracing of external and internal messages.</li> </ul>
<ul style="list-style-type: none"> <li>Complete Backup and Restore by means of iNMC Server or the HiPath 8000 Assistant.</li> </ul>	<ul style="list-style-type: none"> <li>Log File Retrieval tool</li> <li>Modular UNIX Packaging for Upgrades</li> <li>Query of Subscriber Transient Operational Status</li> </ul>
<ul style="list-style-type: none"> <li>Billing for Business Groups</li> </ul>	<ul style="list-style-type: none"> <li>Installation Audits</li> <li>Installation Wizard</li> </ul>
<ul style="list-style-type: none"> <li>Call Detail Records (CDRs) Retrieval</li> </ul>	<ul style="list-style-type: none"> <li>Removable Backup Media</li> <li>Rolling Software Upgrade</li> </ul>
<ul style="list-style-type: none"> <li>Element Management (Configuration/ Provisioning, Performance Monitoring, Fault Management, and so on) through SNMP and CLI</li> </ul>	<ul style="list-style-type: none"> <li>Subscriber Self Management by means of the web-enabled Subscriber Self-Care (iSSC) application.</li> <li>System Software and Patch Level Status</li> </ul>
<ul style="list-style-type: none"> <li>APS Upgrades</li> <li>Fault Isolation</li> <li>Recovery</li> </ul>	<ul style="list-style-type: none"> <li>Basic Traffic Tool is a Performance Monitoring tool for incoming SIP calls.</li> <li>Traffic Measurements for Hunt Groups</li> <li>Upgrade Rollback within Maintenance Window</li> </ul>
<b>Security</b>	
<ul style="list-style-type: none"> <li>Account and Password Management Security</li> </ul>	<ul style="list-style-type: none"> <li>Defending Denial-of-Service Attacks</li> </ul>
<ul style="list-style-type: none"> <li>Audit</li> </ul>	<ul style="list-style-type: none"> <li>IPSec Baseline for IP security</li> </ul>

Table 2-1 HiPath 8000 Features (Sheet 2 of 4)

## HiPath 8000 Overview

### HiPath 8000 Features

<ul style="list-style-type: none"> <li>Control of SIP Digest Authentication</li> </ul>	<ul style="list-style-type: none"> <li>NMC Enhanced Support for Alarming</li> <li>Payload Encryption</li> </ul>
<b>Subscriber</b>	
<ul style="list-style-type: none"> <li>Authentication, Audits, and so on</li> </ul>	<ul style="list-style-type: none"> <li>Enhanced Call Trace scheduled for Release 2.0</li> </ul>
<ul style="list-style-type: none"> <li>Basic Business Group <ul style="list-style-type: none"> <li>Intercom Dialing</li> <li>Main Number</li> <li>Hot Desking</li> <li>Department Names Sub-groupings</li> <li>Account Codes</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Feature Profiles</li> </ul>
<ul style="list-style-type: none"> <li>Call Diversion for Call Messaging Systems in Multiple Platforms</li> </ul>	<ul style="list-style-type: none"> <li>MLHG - Pilot Hunting</li> </ul>
<ul style="list-style-type: none"> <li>Call Forwarding with CDR for each call leg.</li> </ul>	<ul style="list-style-type: none"> <li>Multiple Originating Point Codes</li> </ul>
<ul style="list-style-type: none"> <li>Call Forwarding Busy Line</li> </ul>	<ul style="list-style-type: none"> <li>Operator Busy Line Verification (Barge-in)</li> </ul>
<ul style="list-style-type: none"> <li>Call Forwarding Extended (Web based control): CF All, Time of Day, Busy, Don't Answer, Selective</li> </ul>	<ul style="list-style-type: none"> <li>Operator Services Support</li> </ul>
<ul style="list-style-type: none"> <li>Call Forwarding No Answer</li> </ul>	<ul style="list-style-type: none"> <li>Remote Access to Call Forwarding</li> </ul>
<ul style="list-style-type: none"> <li>Call Pickup</li> </ul>	<ul style="list-style-type: none"> <li>Serial Ringing</li> <li>Simultaneous Ringing</li> </ul>
<ul style="list-style-type: none"> <li>Call Transfer/Call Transfer Security</li> </ul>	<ul style="list-style-type: none"> <li>SIP Enhancements</li> </ul>
<ul style="list-style-type: none"> <li>Caller ID</li> </ul>	<ul style="list-style-type: none"> <li>Speed Dialing</li> </ul>
<ul style="list-style-type: none"> <li>Caller ID Blocking</li> </ul>	<ul style="list-style-type: none"> <li>Three Way Call</li> </ul>
<ul style="list-style-type: none"> <li>Calling Name Delivery Blocking</li> </ul>	<ul style="list-style-type: none"> <li>Toll Free Dialing (for example, 800)</li> </ul>
<ul style="list-style-type: none"> <li>Display</li> </ul>	<ul style="list-style-type: none"> <li>Toll Restriction and Code Diversion</li> </ul>
<ul style="list-style-type: none"> <li>Directory Services Support.</li> </ul>	<ul style="list-style-type: none"> <li>Usage Sensitive Call Forwarding</li> </ul>
<ul style="list-style-type: none"> <li>Direct Station Selection</li> <li>Distinctive Ringing</li> </ul>	<ul style="list-style-type: none"> <li>Visual/Telephone Screen List Management</li> </ul>
<ul style="list-style-type: none"> <li></li> </ul>	<ul style="list-style-type: none"> <li>Voice Mail/Unified Messaging support</li> </ul>
<b>SIP Attendant Answering Position</b>	
Night Service	

Table 2-1 HiPath 8000 Features (Sheet 3 of 4)

<b>SIP Feature interworking with HiPath 4000 Legacy Users</b>	
Name and Number Presentation	Calling and connected party restrictions
Local feature support, such as Call Hold, Call Transfer and Conference.	
<b>SIP User Voice Features</b>	
Audible Ringing	Distinctive Ringing
Call Drop / Disconnect	Do Not Disturb
Call Forward All	DNS SRV (RFC 3263)
Call Forward Busy	DTMF in-band G.711
Call Forward No Answer	DTMF in RTP (RFC 2833)
Call Forwarding System	Forward Calls to VoiceMail
Call Forwarding Station - Fixed	Hold Ringback
Call Hold	Hotline and Warmline
Call log	Hunt groups - Pilot
Call Pickup Group	Internal/External Distinctive Ringing
Call Transfer Attended	Line Key Operating Modes Line Reservation
Call Transfer Unattended	Last number redial
Call Transfer Unscreened	Message Waiting Indication (by means of Notify)
Call Waiting for MGCP devices	Multiple Line Appearances/Key Set Multiple Line Preference
Calling Line ID /Caller ID	Music on Hold (local)
Calling Line ID Blocking	Music on Hold Line and Group Option
Conference (3-way calling)	Mute
Conference - Pick and Add To	Remote Access
Conference Large- Station Controlled	Repdial/DSS keys
Configurable Extension Dialing	Speed Dialing - System
Consultation/Consultation Hold	Toggle
Direct Outward Dialing	Volume Control for Speaker
Direct Inward Dialing	Volume Control for Ringer

Table 2-1 HiPath 8000 Features (Sheet 4 of 4)

## 2.3 HiPath 8000 Interfaces

The HiPath 8000 V2.1 uses fully redundant proxy registration servers (real-time media transaction controllers) (See [Figure 2-6](#)) that operate on industry standard Linux server over a QoS managed network. This application can reside and be managed from a data center like any other traditional data application. In addition, nodes can be geographically separated using redundant fiber optic links to reduce the risk of total loss of voice services.

The underlying middleware for the HiPath 8000 is a distributed computing and fault-tolerant platform called Resilient Telco Platform (RTP). This platform provides services that allow the applications to be implemented with two important architectural principles: 1) data resiliency and 2) location transparency. The use of a distributed architecture not only provides redundancy at the computing element level, but also at the process level. Computing-element clustering is supported by means of the hardware platform. Process-level redundancy is supported by means of the HiPath 8000 enabling software Resilient Telco Platform.

Location transparency is achieved by using a logical naming mechanism for the redundant process instances. This is referred to as aliasing. In general, the RTP Context services, such as the Context Manager, make the distributed HiPath 8000 architecture fault tolerant and scalable at the software level, with all of the essential application transparencies. Each process instance may have an alias that acts as a redundant instance. The configuration of aliases includes active-standby and active-active. Aliases may be in the same computing element, or node, or in different nodes, within a distributed architecture (also referred to as cluster).

The RTP Context Manager service supports data resiliency which provides seamless support of call processing when one of the cluster nodes goes down. This ensures that calls are not dropped when a node or process instance goes down. In particular, the Universal Call Engine and Signaling Managers invoke the Context Manager service to save and retrieve critical call-related information. Upon failure (for example at the process, CPU or node level), and possible loss of a given process instance, a redundant instance of the lost process is able to invoke the Context Manager, retrieve the latest call-related information, and resume the call signaling or processing seamlessly.

The RTP Node Manager provides mechanisms to monitor the application processes of the HiPath 8000. Network Elements Management I use the ObserveProcess mechanism to monitor the UCE, Signaling Managers, Connection Control Manager, PSTN Routing Manager, Routing Manager, AAA Manager and Usage Collection. NEM is then informed when any process becomes unavailable, and generates the appropriate critical alarms. It is also informed when a process becomes available, so that the corresponding alarms can be cleared.



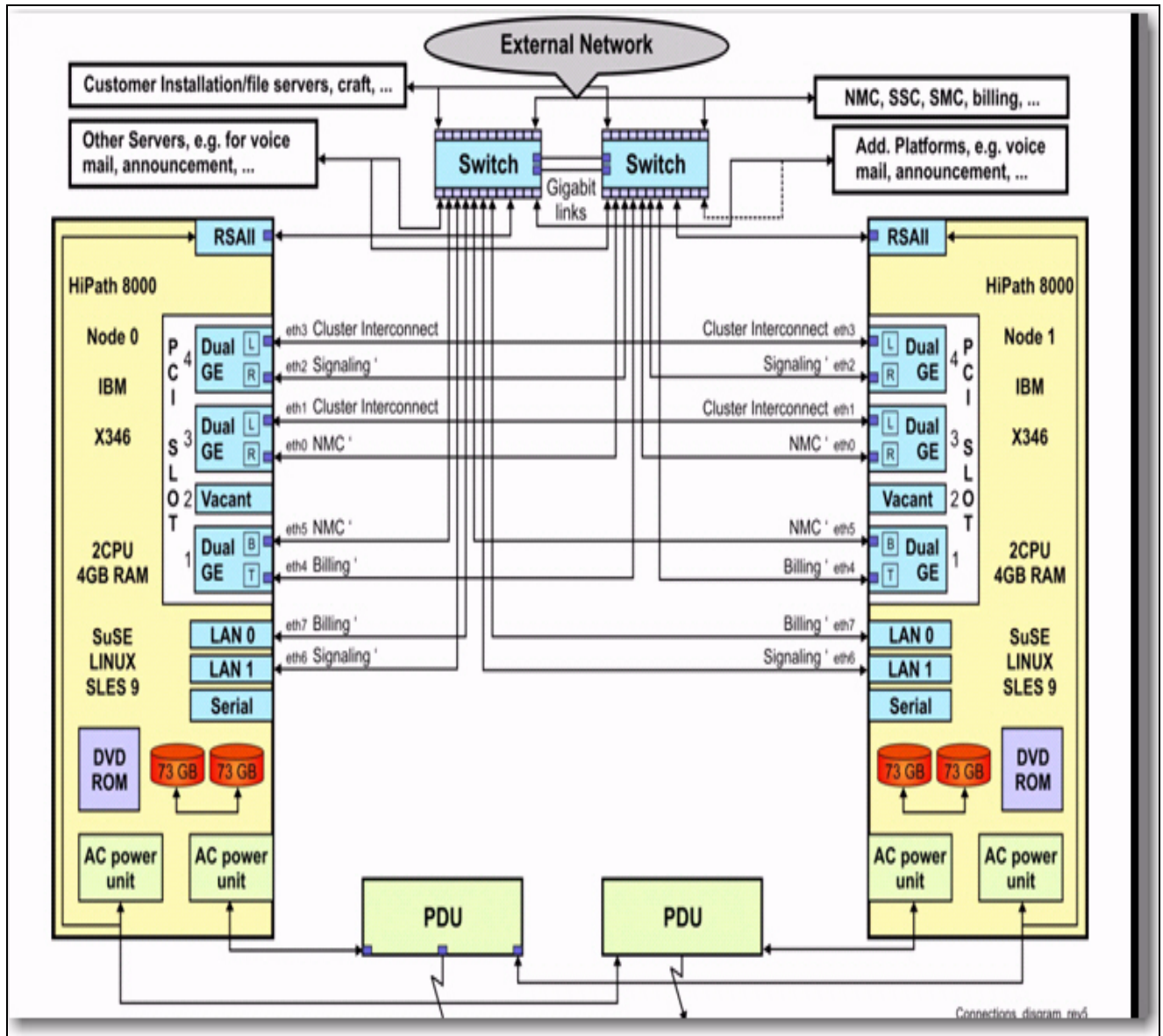


Figure 2-6 HiPath 8000 Interfaces

## HiPath 8000 Overview

### *System Scalability*

## 2.4 System Scalability

The HiPath 8000 is a highly scalable Enterprise softswitch switch that includes these scalability features:

- Busy Hour Call Attempt (BHCA) scalability – Supports up to 252,000 BHCA on IBM 346. (Actual performance of the system varies depending on call mix and protocols.)
- Maximum of 100,000 subscribers based on typical call model of 2.5 calls per subscriber in the busy hour
- Primary and secondary nodes run in active/active mode. Two systems provide 1+ system capacity and performance

## 2.5 Security

The HiPath 8000's two main security goals are to protect the customers and to protect the network and its equipment. Protecting customers includes the need to:

- Maintain Service Availability.
- Ensure confidentiality and integrity of customer information.

Protecting the network includes the need to:

- Ensure non-malicious interaction between customers and the system.
- Enforce customer access only to authorized features.
- Maintain the confidentiality and integrity of system information.
- Enforce operations span of control & scope of commands.
- Ensure non-malicious interactions among system elements.

The HiPath 8000 provides two main classes of security features:

- Preventive, for example, authentication
- Recording, for example, security logging

The preventive ones include:

- Authentication: The verification (proof) of the identity of a party.
- Access Control: The prevention of unauthorized use of a resource including the prevention of the use of a resource in an unauthorized manner.
- Data Integrity: The property that data has not been altered or destroyed in an unauthorized manner.

- **Data Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals or entities.

Security logging is a recording feature and it permits the detection and investigation of security breaches after they occurred. This requires the recording of security relevant information in a security log that can be analyzed by security experts.

Event logging provides sufficient information for an after-the-fact investigation of loss or impropriety and end-to-end accountability for all significant events.

There are other features related to security that need to be considered by network operators:

- **Accountability:** The property that ensures that the actions may be traced uniquely to a particular entity.
- **Data backup:** Files and programs are copied to facilitate recovery, if necessary.

The HiPath 8000 security strategy is based on a layered security approach. The first layer of security is the network design itself that separates bearer, signaling, and OAM&P traffic from each other and from other traffic on the network. The second layer of security is the support for integrated end-to-end secure interfaces within the HiPath 8000 equipment itself.

For additional information see the *HiPath 8000 Security Reference and Planning Guide*.

## **2.6 Quality of Service (QoS)**

The HiPath 8000 provides built-in capabilities to ensure a quality communications path every time. It supports network segmentation, giving the option of using VLANs to separate voice and data traffic on the LAN/WAN. The HiPath 8000 uses industry standard methods to ensure prioritization of Real Time Communications traffic to ensure user satisfaction. For enhanced QoS management, HiPath QoS 2000 and HiPath QoS Manager integrate all the monitoring, policy, implementation and reporting tools necessary to guarantee application performance, thus optimizing usage of the full bandwidth for the disparate requirements of voice and data communication, and ensuring that voice communication is always prioritized.

## **HiPath 8000 Overview**

### *Reliability and Availability*

## **2.7 Reliability and Availability**

### **2.7.1 Hardware Redundancy**

The HiPath 8000 hardware platform achieves carrier-grade reliability and availability based on the active/active clustered IBM Linux nodes. It supports hot swappable components, active/standby Fast Ethernet links, and crossover network connections through redundant, interconnected Ethernet switches.

The IBM cluster controls the failover of active/standby Ethernet links and failover of the clustered IBM nodes. For signaling, it supports active/active SIP links. For data storage, it supports two RAID1-controlled disks per node for 100% redundancy. If one of the hard drives fails, the integrated IBM ServeRAID controller switches read and write requests to the remaining drives.

### **2.7.2 Software Redundancy**

The HiPath 8000 software platform achieves carrier-grade reliability and availability based on the Fujitsu-Siemens PrimeCluster software, the Resilient Telco Platform (RTP) middleware, and the SolidTech FlowEngine database. The HiPath 8000 clustering software provides an administrator with a single system image and supports internode communications among the individual IBM nodes that form the cluster. It also provides an interface to the Remote Service Adapter which allows automatic server shut down.

The RTP middleware manages node and process failovers within and across the nodes.

### 3 HiPath 8000 Hardware

The HiPath 8000 is a protocol-independent, switching platform capable of bridging legacy and next generation networks. The HiPath 8000 call model enables new services that cross both existing voice and data networks. It extends services to next generation wireless networks, as well as IP and circuit switched networks. The foundation of the HiPath 8000 is the Resilient Telco Platform (RTP) and the Universal Call Engine (UCE).

The HiPath 8000 adheres to the softswitch concept, providing next-generation call switching on an open platform. This design lends itself to the use of third-party, open platform hardware products.

This chapter describes the hardware of the HiPath 8000.

#### 3.1 System Configurations

The HiPath 8000 is available in a duplex two-node configuration. The duplex configuration provides 1:1 failover when one node fails. [Figure 3-1](#) shows the HiPath 8000 duplex hardware configuration.

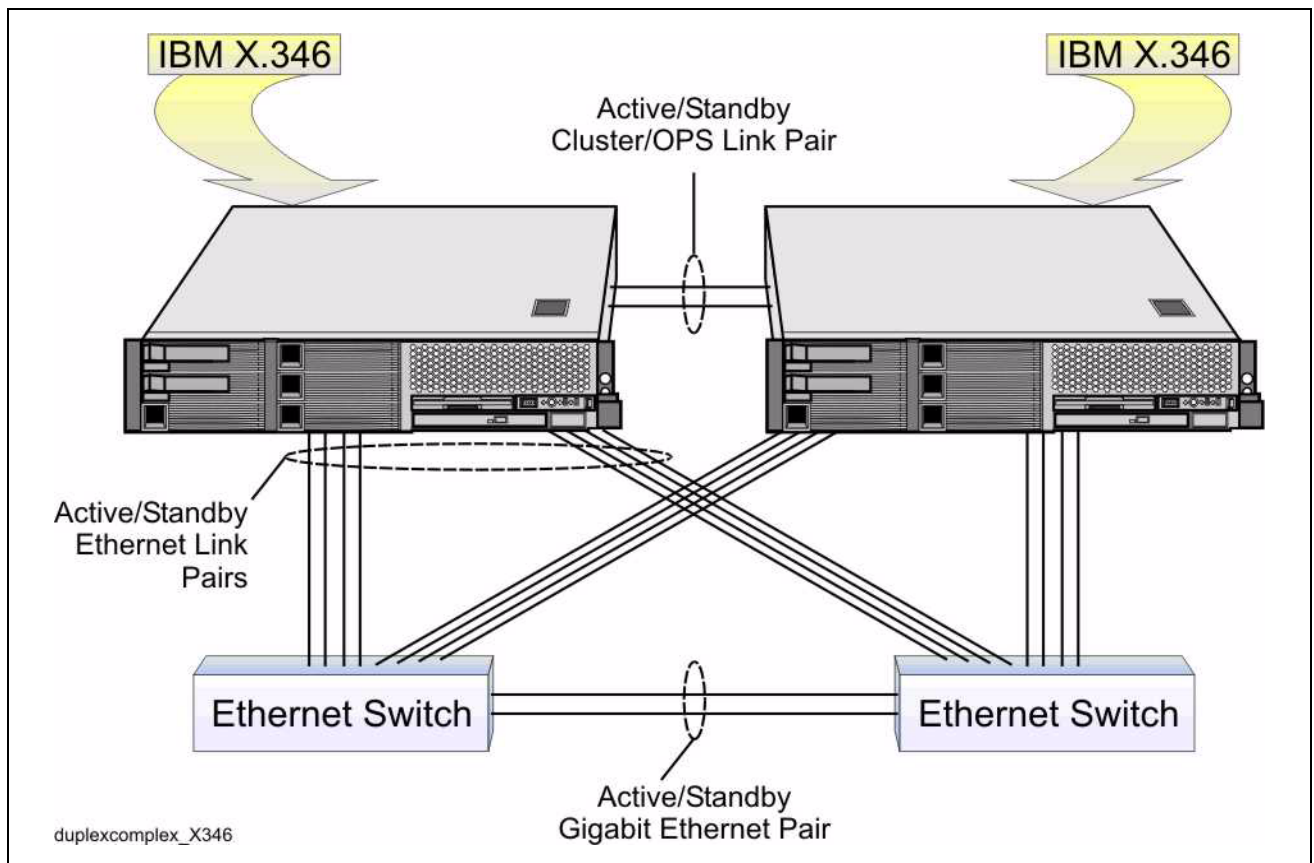


Figure 3-1 HiPath 8000 Duplex Hardware Configuration

## **HiPath 8000 Hardware**

### *System Configurations*

The HiPath 8000 connects to other servers for voice mail, announcements, and so on, and to the external IP network through a pair of Ethernet switches that provide redundant networking. The Ethernet switches also connect the HiPath 8000 to external billing mediation servers and the network and element management server.

#### **3.1.1 HiPath 8000 Base System**

The HiPath 8000 hardware package consists of dual IBM x-Series servers. Each server provides:

- Up to two Intel® Xeon™ processors up to 3.6GHz with 800MHz front-side bus speed supports Intel Extended Memory 64 Technology.
- Up to 16GB of DDR2 memory using 8 DIMM slots with enhanced memory availability features, 4 PCI (2 x PCI-X) slots and upgradable I/O to PCI-Express
- Up to 6 hot-swappable SCSI hard disk drive support and available internal tape backup option for storage flexibility, integrated RAID-0, -1 with optional upgrade to RAID-5 by means of the ServeRAIDTM-7k-no PCI slot required
- Up to eight Ethernet ports along with 10 other external ports
- Hot-swap redundant cooling, power and hard disk drives
- The integrated system management processor provides overall monitoring.

Because a RoHS compliant server for HiPath 8000 is needed, a RoHS compliant based on x346 architecture is tested as the alternative to IBM x3650T platform 9 (to be released in V2.2). It is form fit and functionally equivalent to the existing x346 and requires less testing and validation. The same RoHS compliant server will be used for sales in the US and other countries.

##### **3.1.1.1 Intel Xeon processors**

The processors deliver processing speeds up to 3.6GHz 800MHz 1MB L2 Cache Xeon Processor with Intel EM64T. 800MHz front-side bus speed increases system throughput by up to 50%. They also incorporate new Hyper-Threading technology, allowing them to execute more than one thread per processor.

##### **3.1.1.2 Memory**

The x346 supports up to 16GB Double Data Rate (DDR-2) memory. DDR memory executes twice the number of operations per cycle than traditional SDRAM memory.

The x346 comes standard with Integrated RAID 1 for mirroring capability on the server. The x346 integrated mirroring provides simultaneous physical mirroring of two drives, allowing for fault tolerant, high-availability data. In the case of hard drive failure, the hot-swap capability allows you to easily restore the system by simply swapping out drives.

The ServeRAID 5i card offers hardware-based RAID for increased data protection and server availability. The ServeRAID 5i provides RAID 5 functionality by taking control of the Ultra 320 SCSI controller on the motherboard.

### 3.1.1.3 LEDs and Switches

Figure 3-2 shows the LEDs and switches.

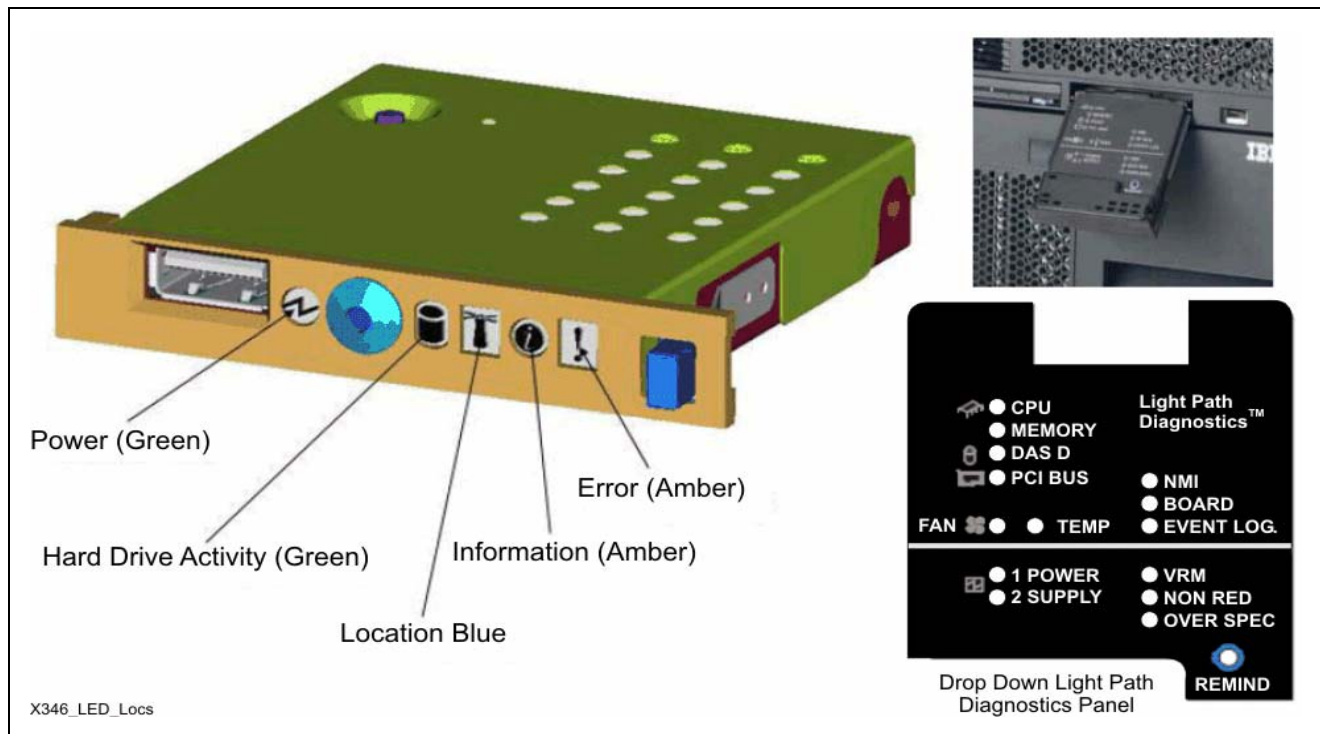


Figure 3-2 IBM 346 Front View

### 3.1.1.4 External Ports

The HiPath 8000 supports eight Ethernet ports (see Figure 3-3) (the additional six port Dual Gigabit Ethernet card plus the standard two Gigabit Ethernet ports) per server for internal and external communication. These include:

- two used for Signaling (SIP)
- two used for Billing
- two used for OSS (iNMC)
- two used for cluster cross-connect)

Other external ports include:

- One serial port
- Three USB ports
- Two systems management (RS485) ports



- One video port
- One keyboard port
- One mouse port
- One external SCSI port

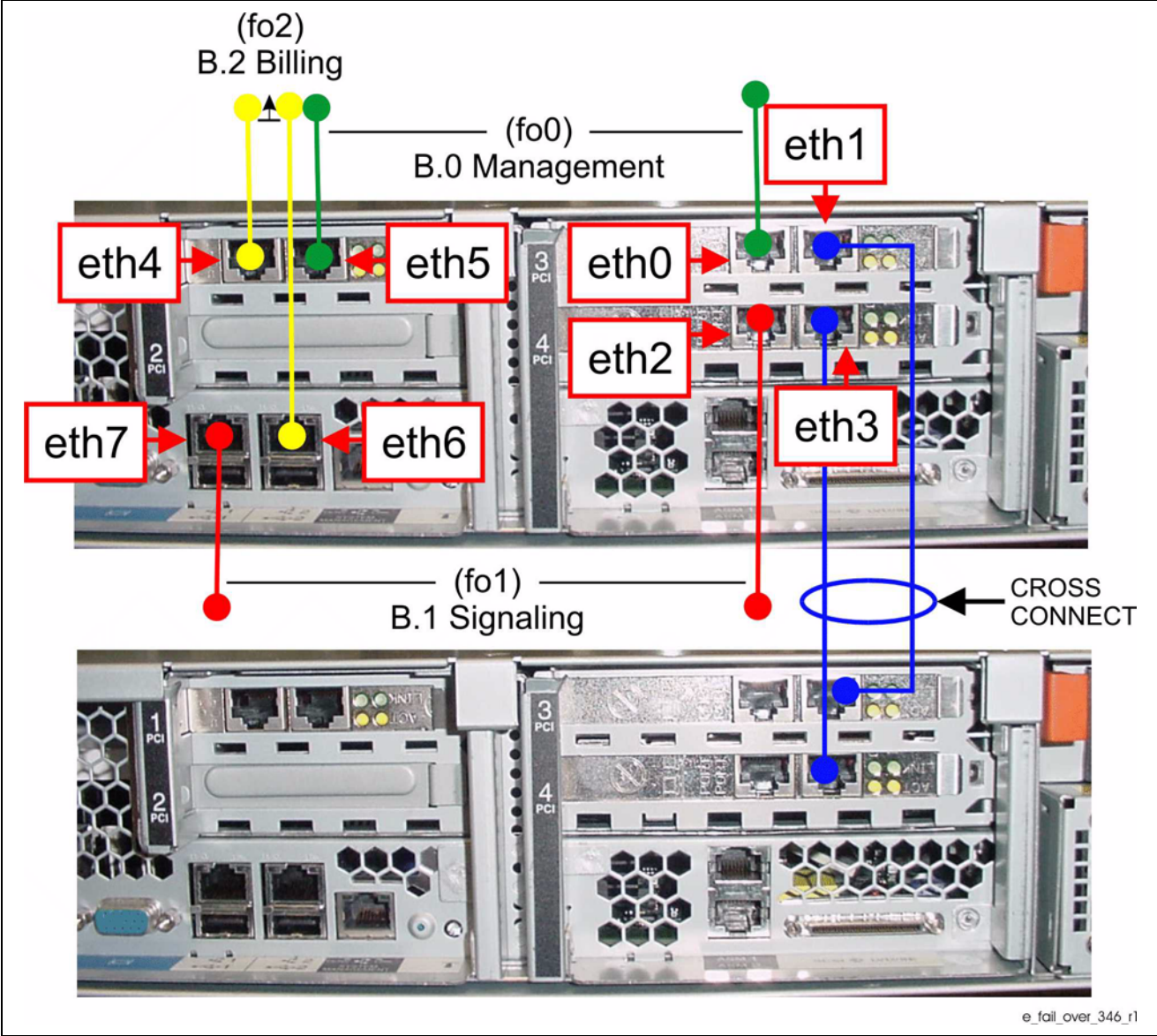


Figure 3-3 IBM 346 Port Numbers

## HiPath 8000 Hardware

### System Configurations

#### 3.1.1.5 Hot-swap Redundant Power

The x346 comes standard with one 350W power supply. Customers have the option to upgrade to two 350W power supplies for redundancy. The second power supply option comes with three additional cooling fans.

The x346 provides redundant cooling capability with five hot-swap redundant fans.

#### 3.1.1.6 System Management

The integrated system management processor monitors system environmentals and provides predictive failure analysis on processors, memory, voltage regulator modules, power supplies, fans and hard disk drives.

### 3.1.2 IBM 346 Technical Specifications

Features	Benefits
Up to 2 Intel® Xeon™ Processors (Nocona 800Mhz FSB)	Provides power, scalability for improved performance
Up to 16GB of DDR-II PC2100 ECC Memory	Allows for extreme scalability and improved performance with 8 dimm slots
Internal Tape Support	Support for DDS5 Tape.
Supports up to 6 Ultra320 HS HDDs	Up to 440GB of internal storage
5 PCI Slots (4 PCI-X)	Offers optional PCI-E riser card slots, replacing the two PCI-X 64/133Mhz slots with two PCI-E x8 slots for improved availability and performance. This allows customers to optimize for performance and migrate to PCI-E when the adapters they use are available.
Dual Ultra320 SCSI controller	Up to double the data transfer rate from Ultra160
Integrated Ultra320 RAID 0,1. Embedded RAID ServRAID-7k RAID 5 option	Provides standard RAID 1 mirroring of hard disk drives for data protection
CD / DVD	Provides 24x (CD), 8x (DVD) read speed
Dual Integrated Gigabit Ethernet	Affords high-speed network connectivity without using a valuable PCI slot

Table 3-1 IBM 346 Technical Specifications (Sheet 1 of 2)

<b>Features</b>	<b>Benefits</b>
Hot-swap/redundant power and cooling with 6 redundant fans	Reduces unplanned down time by maintaining system performance if a fan/power supply fails
	Reduces planned down time by allowing failed fans/power supplies to be replaced without taking the server down
Light Path Diagnostics self diagnosis panel	Provides a lighted path to failing components, thus expediting hardware repairs, which dramatically reduces service time
Remote Deployment with Wake on LAN and Preboot eXecution (PXE®)	WOL saves you time and money by providing the capability to remotely manage servers
	PXE provides remote control of server initialization process, saving IT staff travel and dollars; Designed to work with IBM's Remote Deployment Manager
Integrated System Management Processor	Provides extensive around-the-clock remote management capabilities
	Increases server availability by continuously monitoring system and notifying administrators of potential system failures before they happen
IBM Director and IBM Director Extensions	Provide comprehensive server management from a central console
	Helps increase uptime and reduce costs through advanced server management capabilities
Support for IBM Remote Supervisor Adapter	Decreases downtime by allowing IT staff to manage systems remotely, whether the server is operational or not
	Provides full graphical console redirection, allowing the use of a local desktop to access and control a server
	Round-the-clock multi-mode alerting includes e-mail with event log, SNMP, pager and LAN

Table 3-1 IBM 346 Technical Specifications (Sheet 2 of 2)

### **3.1.3 Certified Ethernet Switches**

The HiPath 8000 uses 3Com (or equivalent OEM) certified Ethernet Switches which conform to the full duplex implementation of the Gigabit Ethernet standard, IEEE 802.3z.

## **4 HiPath 8000 Software Functional Overview**

This chapter describes the software components of the HiPath 8000.

### **4.1 HiPath 8000 Base Software and Call Processing Applications**

The HiPath 8000 system software (see [Figure 4-1](#)) and application services support includes:

- SuSe LINUX Enterprise Server 9 (SLES-9) operating system
- Fujitsu-Siemens PrimeCluster
- Resilient Telco Platform (RTP) middleware package
- Element and resource management software that provides options for service and resource configuration, provisioning, maintenance, diagnostics, and accounting
- Routing of calls between any two endpoints from PSTN or IP
- IP connections
- Intelligent call control capabilities for digit translation and routing
- VoIP switching, call origination, and termination
- Signaling capabilities
  - SIP and SIP-Q
  - CSTA
  - MGCP
- Call and service usage collection for billing and traffic engineering
- Dynamically loaded calling services by means of Services Logic Execution Environment (SLEE) and its APIs for services such as Caller ID, Originating Call Blocking, and Customer Calling services
- QoS control for IP bearer traffic

# HiPath 8000 Software Functional Overview

## HiPath 8000 Base Software and Call Processing Applications

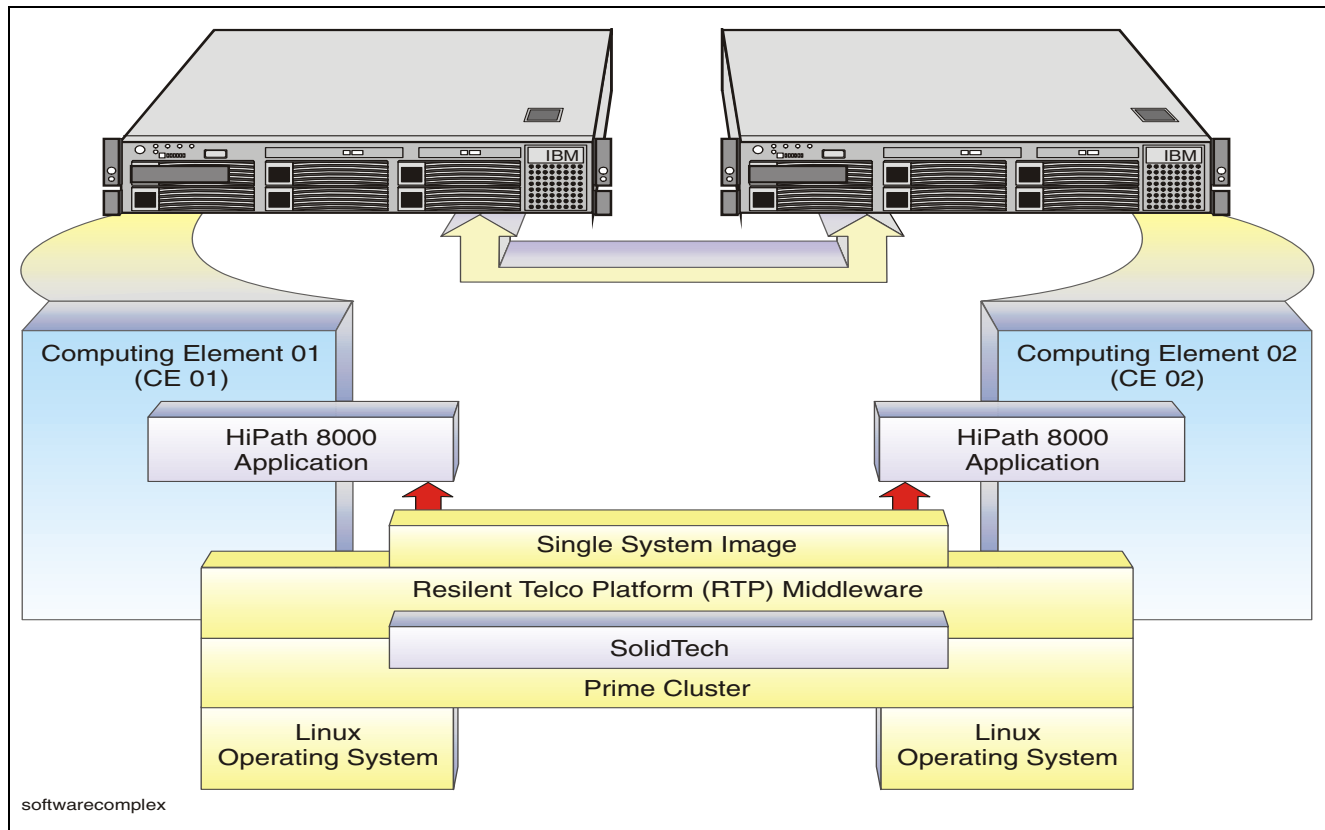


Figure 4-1 Software Complex Overview

### 4.1.1 Resilient Telco Platform (RTP)

The HiPath 8000 utilizes the Fujitsu-Siemens Computers GmbH Resilient Telco Platform (RTP). The RTP is a distributed computing and fault tolerant platform that is the underlying middleware for the HiPath 8000. The RTP provides services that implement applications with location transparency and data resiliency. The use of a distributed architecture provides redundancy at the computing element level and at the process level. Computing element clustering is supported by using the HiPath 8000 hardware platform. The HiPath 8000 RTP software supports process level redundancy.

Location transparency is achieved by using a logical naming mechanism for the redundant process instances, which is referred to as aliasing. In general, the RTP Context services, such as the Context Manager, make the distributed HiPath 8000 architecture fault tolerant and scalable at the software level, with all of the essential application transparencies. Each process instance may have an alias that acts as a redundant instance. The configuration of aliases includes active-standby and active-active. Aliases may be in the same computing element, or node, or in different nodes, within a distributed architecture (also referred to as cluster).

Data resiliency is achieved through the use of the RTP Context Manager service. In particular, the Universal Call Engine and Signaling Managers invoke the Context Manager service to save and retrieve critical call-related information. Upon failure (for example, at the process, CPU or node level), and possible loss of a given process instance, a redundant instance of the lost process is able to invoke the Context Manager, retrieve the latest call-related information, and resume the call signaling or processing seamlessly.

The RTP Node Manager provides mechanisms to monitor the application processes of the HiPath 8000. Network Elements Management (NEM) uses the ObserveProcess mechanism to monitor the UCE, Signaling Managers, Connection Control Manager, PSTN Routing Manager, Routing Manager, AAA Manager, and Usage Collection. NEM is then informed when any process becomes unavailable, and generates the appropriate critical alarms. It is also informed when a process becomes available, so that the corresponding alarms can be cleared.

Figure 4-2 shows the role of the RTP middleware.

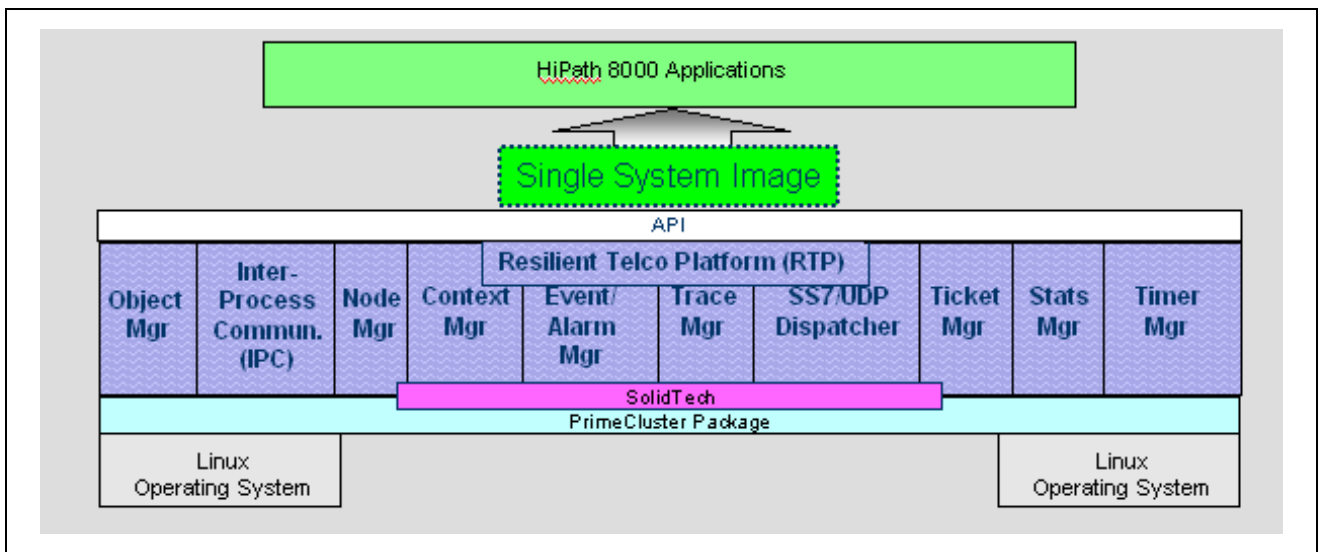


Figure 4-2 Role of the RTP middleware

#### 4.1.1.1 Important RTP Components

The major components of the RTP portion of the HiPath 8000 are:

- **Node and Communication Manager**

This component is responsible for the shutdown, restarting, and monitoring of RTP and HiPath 8000 application processes on each node in the cluster. There is a separate instance of the node manager on each member of the cluster. It is also responsible for maintaining the backup processes that are distributed across cluster members. Most processes started by the node manager are defined by a configuration file that is reference during startup.

## HiPath 8000 Software Functional Overview

### *HiPath 8000 Base Software and Call Processing Applications*

- **Inter-Process Communication (IPC)**

Communication between processes is done using well-defined messages. Processes can be combined into alias groups. For instance, there are four instances of the UCE across the cluster. Even distribution of the call load across all UCE's is accomplished largely by the IPC.

- **Context Manager**

A context is an object in memory that represents data and its state. The current state of a call, CDR-related information, timer information, active traces, and data from an external protocol packet are all candidates for context storage. The context manager is responsible for maintaining this information and maintaining a backup context on the other cluster node.

- **Event and Alarm Manager**

Events are special messages stored in replicated files. Events with a severity level attached to them (critical, minor) are called alarms. Events with severity cleared, warning, minor, major and critical are reported to the SNMP trap manager (the iNMC only accepts alarms and clearance, no warnings).

- **Trace Manager**

The trace manager is used for debugging purposes. It is used to create event files that track the execution behavior, at different severity levels, of selected RTP and HiPath 8000 processes.

- **TTUD Dispatcher**

Each node has multiple IP addresses for load distribution and resiliency reasons. The TTUD dispatcher provides these multiple communication channels to the external IP network.

- **Ticket Manager**

Handles the generic "ticket" object which is used in the Call Detail Records (CDRs) that are generated for billing purposes.

- **Statistics**

Provides the logging of operational statistics.

- **Timer Manager**

Provides the means for components to create timers and handles their expirations



## 4.1.2 Universal Call Engine (UCE)

The UCE (See [Figure 4-3](#)) is a high performance, call processing engine that contains the generic switching functions of the HiPath 8000. It provides a secure, generic interface to set up and release calls through the system. The UCE provides common logic to all signaling managers to route calls through the HiPath 8000.

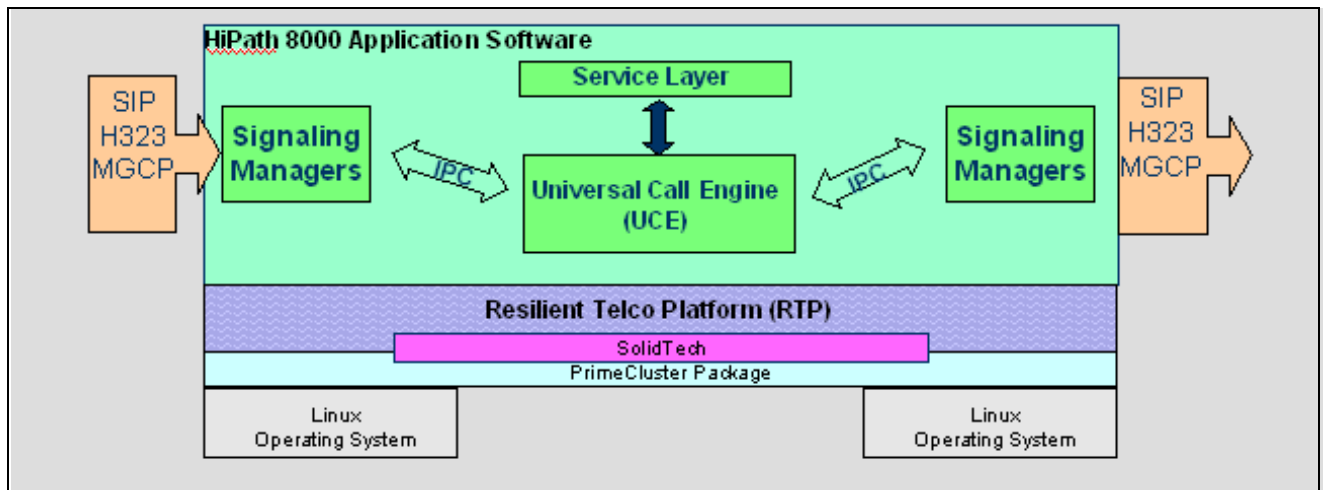


Figure 4-3 Application Software

The primary components for UCE call logic are:

- Incoming Transaction Segment (ITS) — Executes the originating (inbound) call logic (on A-side).
- Outgoing Transaction Segment (OTS) — Executes the terminating (outbound) call logic (on B-side).
- Associator Segment (AS) — Preserves the overall call topology and maintains the relationship between all ITS and OTS involved in a single call.
- Central Distributor Module - Brokers messages among the ITS, OTS and AS.

### 4.1.2.1 UCE Role

The UCE interacts with the service layer and the signaling managers. The service layer functions include:

- Manages access and user/subscriber related resources.
- Manages Call Admission Control by ensuring that enough bandwidth
- Authenticates calling subscribers prior to call setup using the Authentication, Authorization, and Accounting (AAA) Services.

## HiPath 8000 Software Functional Overview

### *HiPath 8000 Base Software and Call Processing Applications*

- Matches the subscribed capabilities of the users involved in each call with the resources allocated to that call.
- Enables mediation between call signaling through communication with various signaling managers.
- Provides access to digit translation and routing (XLA).
- Selectes the outgoing signaling manager based on the results from call routing.
- Generates Call Detail Records (CDRs) by means of the Usage Collection function.
- Coordinates the connection and release of physical and logical switching resources and the switching of connections by using the Connection Control Manager.
- Coordinates features and supplementary services that are dynamically loaded into the UCE.
- Interfaces with off-board services by using SIP.
- Acts on maintenance and administration requests that affect in-progress calls.

A large number of APIs provided to the UCE are crucial to HiPath 8000 programmability and the ability to interoperate with standards-based equipment.

Figure 4-4 shows the HiPath 8000 UCE interfaces.

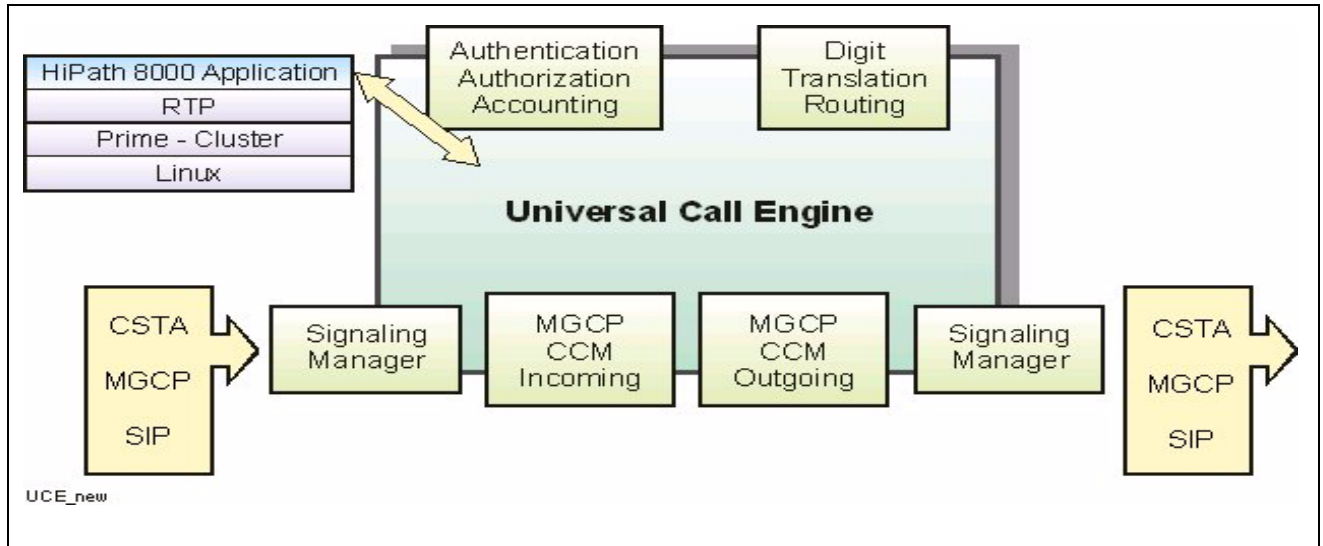


Figure 4-4 HiPath 8000 Universal Call Engine (UCE) Interfaces

### 4.1.3 Signaling Managers

There are various signaling managers that handle the different protocols terminated by the HiPath 8000. The signaling managers include:

- CSTA
- MGCP
- SIP
- SIP-Q

The main tasks of the signaling managers are:

- Handles all protocol functionality, such as;
  - Message encoding and decoding
  - Protocol state event processing
  - Protocol conformance checks
  - Protocol specific timers.
- Interfaces with the signaling stacks, where appropriate.

## HiPath 8000 Software Functional Overview

### *HiPath 8000 Base Software and Call Processing Applications*

- Adapts the external protocol messages to the common secure, normalized interface defined by the UCE.
- Receives/sends maintenance- and administration-related protocol messages and interacting with the HiPath 8000 maintenance functions.

#### **4.1.3.1 CSTA Signaling Manager**

The Computer Supported Telephony Application (CSTA) Signaling Manager (SM) transports and handles CSTA message traffic between CTI applications and the UCE. The CSTA SM is responsible for communicating with the application through TCP connections, converting call control messages between CSTA and UCE formats, and managing a CSTA session. It uses provisioning support, at startup, for notification of configuration changes and also for database access in validating messages. The CSTA SM maintains message interfaces to CSTA service and the services' database (SDAL/DBAL) and in turn, the CSTA SM authenticates user requests by means of SDAL/DBAL. Additionally, the CSTA SM acts as a signaling proxy for the user's telephone (currently, a SIP device).

To perform these functions, the CSTA SM makes use of the 3rd party call control (3PCC), MakeCall function, provided by UCE which can be used to originate a call between the SIP endpoint and the desired destination. Therefore, the features invoked by the CSTA SM are handled by the UCE. Additionally, there is a new service called CSTA Service that handles requests from the CSTA SM. CSTA Service is active for the entire life cycle of a call and it provides for the monitoring functionality required by all phone users. Currently, CSTA monitoring is limited to the prime line on the SIP device.

Figure 4-5 illustrates, at a high-level, how the CSTA Signaling Manager and CSTA Service fit within the HiPath 8000.

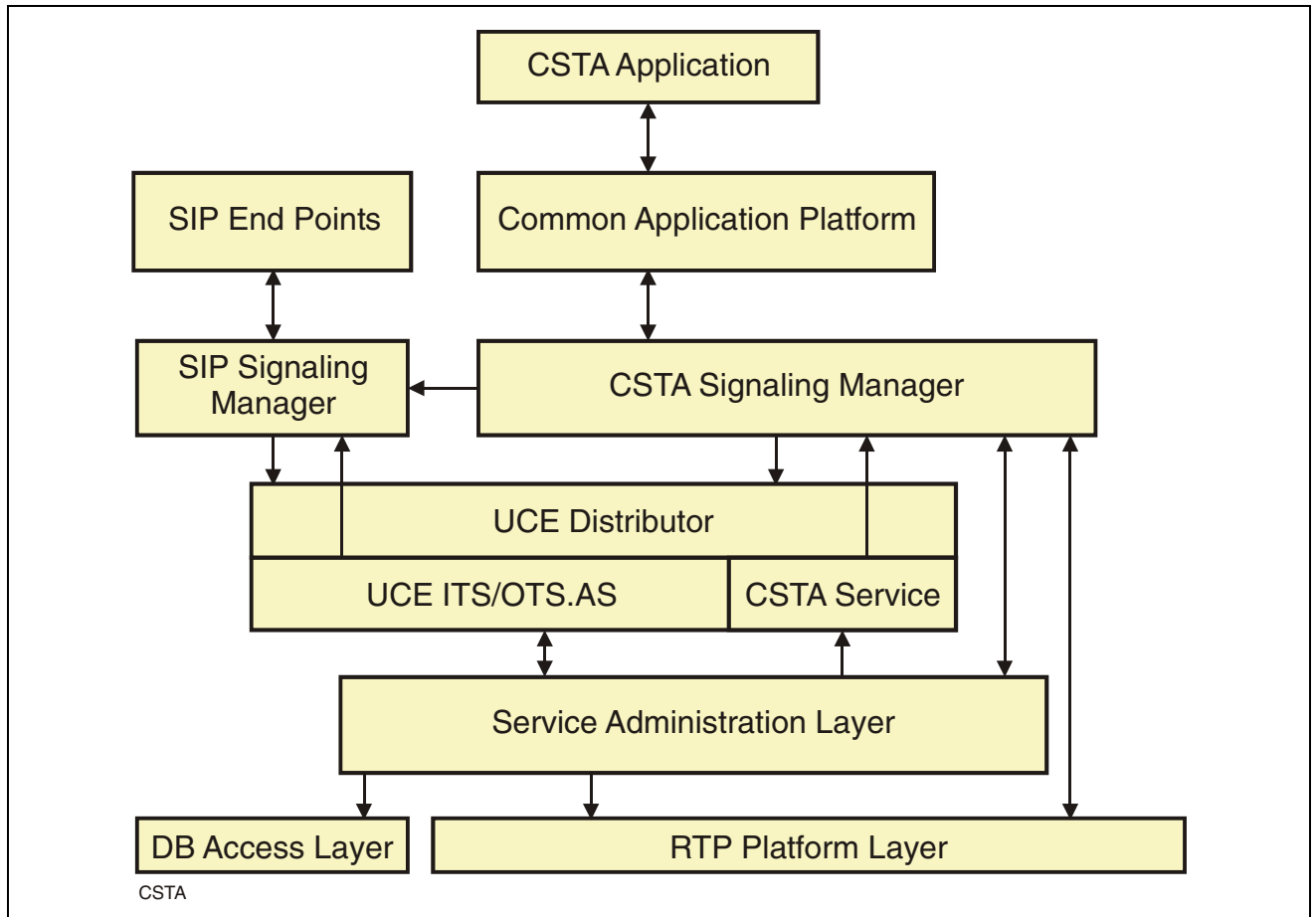


Figure 4-5 CSTA Implementation in the HiPath 8000

#### 4.1.3.2 MGCP Signaling Manager

The Media Gateway Control Protocol (MGCP) Manager provides the HiPath 8000 with call for MGCP endpoints. In the HiPath 8000 environment it is used exclusively to interface to the IP Unity Mereo 6000 Media Server and the Convedia CMS-1000 which provides mainly tones and announcements.

## HiPath 8000 Software Functional Overview

### *HiPath 8000 Software Components*

#### 4.1.3.3 SIP Signaling Manager

The SIP Signaling Manager transports message traffic between SIP and the HiPath 8000 call processing engine UCE. It is responsible for communicating with SIP endpoints through UDP connections, converting call control messages between SIP, SDP, and UCE formats and managing SIP sessions. The SDP transparency feature enables the SIP SM to forward the received SDP data to the second leg of the call without any modification in the parameters.

#### 4.1.4 Connection Control Manager

The Connection Control Manager (CCM) is responsible for the creation and deletion of the media connections associated with a call. Its main function is to support the IP Unity.

Since the HiPath 8000 and the media servers can be geographically separated, a control protocol is required between them that allows the HiPath 8000 to make and break a connection in the media gateways. The CCM implements these protocols and shields the UCE from the details.

#### 4.1.5 Services Logic Execution Environment (SLEE) for Native Services

The HiPath 8000 Services Logic Execution Environment (SLEE), also known as the HiPath 8000 Services Framework, is a collection of application programming interfaces (APIs) within the UCE. There are two ways to categorize SLEE services:

- **Network versus Nodal Based**
  - A service with execution logic that spans more than one network node is considered a network-based service (Toll Free and Internet Call Waiting).
  - A service with execution logic that is confined entirely within a single network node is considered a nodal-based service (call waiting and call transfer).
- **Call Processing vs. Non-call Processing Based**
  - A service with execution logic that is a part of a specific call is considered a call processing-based service (call forwarding).
  - A service with execution logic that is not confined to any specific call is considered a non-call processing-based service. The latter is less frequent than call processing based services (message waiting indicator and wireless messaging).

## 4.2 HiPath 8000 Software Components

This section describes the software components of the HiPath 8000. This includes software features, software architecture components, and an overview of call processing, traffic flow, signaling protocols, and routing mechanisms.

## 4.2.1 HiPath 8000 Software Features

Table 4-1 lists the HiPath 8000 software features. The next sections detail these features.

Category	Features
Platform	<ul style="list-style-type: none"><li>• Linux operating system</li><li>• Fujitsu-Siemens Prime-Cluster</li><li>• SolidTech shared-nothing database support for 1:1 cluster</li><li>• Resilient Telco Platform (RTP) middleware support for 1:1 cluster</li><li>• Duplex active/active applications for clustered softswitch</li><li>• Memory-based data management for realtime data access</li><li>• Dynamic data synchronization between nodes</li><li>• Overload handling</li><li>• Call resource auditing for channels and call data contexts</li></ul>
Signaling Protocols	<ul style="list-style-type: none"><li>• SIP signaling support between softswitch and application server</li><li>• Any to any signaling protocol mediation (SIP)</li></ul>

Table 4-1 HiPath 8000 Software Features (Sheet 1 of 4)

## HiPath 8000 Software Functional Overview

### HiPath 8000 Software Components

Category	Features
Call Processing	<ul style="list-style-type: none"> <li>● Universal Call Engine (UCE)</li> <li>● Service Logic Execution Environment (SLEE) supporting these extensible native services:               <ul style="list-style-type: none"> <li>● Anonymous Caller Rejection</li> <li>● Audible Ringing</li> <li>● Authentication, Audits, and so on</li> <li>● Automatic Callback</li> <li>● Automatic recall</li> <li>● Basic Business Group Intercom Dialing, Main Number, Hot Desking, Department Names Sub-groupings, Account Codes</li> <li>● Call Forwarding All</li> <li>● Call Forwarding Busy Line</li> <li>● Call Forwarding Extended (Web based control): CF All, Time of Day, Busy, Don't Answer, Selective</li> <li>● Call Log</li> <li>● Call Forwarding No Answer</li> <li>● Call Pickup</li> <li>● Call Transfer(Attended,Unattended,Unscreened)</li> <li>● Call Waiting</li> <li>● Caller ID</li> <li>● Caller ID Blocking</li> <li>● Calling Name Delivery</li> <li>● Calling Identity Delivery and Suppression</li> <li>● Calling Identity Delivery Call Waiting</li> <li>● Directory Services Support</li> <li>● Direct Station Select</li> <li>● Distinctive Ringing (Internal/External)</li> <li>● Enhanced Call Trace</li> <li>● Feature Profiles</li> <li>● MLHG - Pilot Hunting</li> <li>● Multiple Line Appearances/Key Set</li> <li>● Multiple Originating Point Codes</li> <li>● Music on Hold Line and Group Option</li> <li>● Operator Busy Line Verification</li> <li>● Operator Services Support</li> <li>● Remote Access to Call Forwarding</li> <li>● Selective Call Acceptance</li> <li>● Selective Call Rejection</li> <li>● Simultaneous Ringing</li> <li>● Speed Dialing</li> <li>● Three Way Call</li> <li>● Toll Free Dialing (for example, 800)</li> <li>● Toll Restriction and Code Diversion</li> <li>● Visual/Telephone Screen List Management</li> <li>● Voice Mail/SMDI support</li> <li>● Usage Sensitive Call Forwarding</li> </ul> </li> </ul>

Table 4-1 HiPath 8000 Software Features (Sheet 2 of 4)



Category	Features
Translation and Routing	<ul style="list-style-type: none"> <li>● 555-1212 line numbers</li> <li>● A-side signaling based routing</li> <li>● Alternate routing</li> <li>● Alternate routing with overflow among route types</li> <li>● Bearer capability routing</li> <li>● Destination codes</li> <li>● Digit modification for digit outpulsing</li> <li>● Directory Number announcements</li> <li>● E.164 compliance</li> <li>● Intercept treatment</li> <li>● Inter-changeable NPA and NXX</li> <li>● Leading digit and most-watched digit translation</li> <li>● N11 codes</li> <li>● NANP compliance</li> <li>● Origin-dependent routing</li> <li>● Prefix digit translation (1+, 101+, 011+, 01+, 0. 00. 0+)</li> <li>● Time-of-day routing</li> <li>● Vertical service codes</li> <li>● Virtual DN</li> <li>● International, national, and subscriber E164 directory number translation</li> <li>● Exchange access/feature group D</li> <li>● Resource allocation</li> <li>● Rotary, sequential and cyclic routing</li> <li>● Keyset Operations</li> </ul>
QoS Control	<ul style="list-style-type: none"> <li>● Originating HiPath 8000 and subscriber profile control                             <ul style="list-style-type: none"> <li>– Codec</li> <li>– Packetization period</li> <li>– Type of Service (TOS)</li> <li>– Resource reservation</li> <li>– Silence suppression</li> </ul> </li> </ul>

Table 4-1 HiPath 8000 Software Features (Sheet 3 of 4)

## HiPath 8000 Software Functional Overview

### HiPath 8000 Software Components

Category	Features
OAM&P	<ul style="list-style-type: none"><li>● Account and Password Management Security Enhancement</li><li>● Audit Enhancements</li><li>● Automated software installation for repeatability of site configurations with enhanced DVD Media Option</li><li>● Backup and restore through CLI and SNMP</li><li>● Billing for Business Groups</li><li>● Caller Authentication</li><li>● Call Detail Records (CDRs) generation</li><li>● Complete Backup and Restore by means of iNMC server</li><li>● CDR retrieval through push/pull mechanism</li><li>● Improved APS Upgrade</li><li>● Installation Wizard and Audits</li><li>● iSMC subscriber management through HTTP GUI interface</li><li>● Monitoring Tool for Incoming SIP calls</li><li>● Mass provisioning through expert mode CLI</li><li>● Network Management through iNMC GUI interface</li><li>● Rolling upgrade for system and application software installation</li><li>● Removable Backup Media</li><li>● Software productization through modular UNIX packaging for upgrades</li><li>● Basic Traffic Tool is a Performance Monitoring tool for incoming SIP calls</li></ul>
Element Management	<ul style="list-style-type: none"><li>● Element management interfaces<ul style="list-style-type: none"><li>– Menu-driven CLI</li><li>– Expert mode CLI (for Mass Provisioning)</li><li>– SNMP Network Management Center (iNMC)</li></ul></li><li>● Network management for softswitch system and all supported features<ul style="list-style-type: none"><li>– Configuration/provisioning management</li><li>– Fault management (traps)</li><li>– Maintenance management</li><li>– Statistics Reporting</li></ul></li></ul>

Table 4-1 HiPath 8000 Software Features (Sheet 4 of 4)

## 4.2.2 HiPath 8000 Software Architecture

The HiPath 8000 platform uses third-party, open platform software including the operating system, signaling stacks, and database products. Figure 4-6 shows the software components of the HiPath 8000 system.

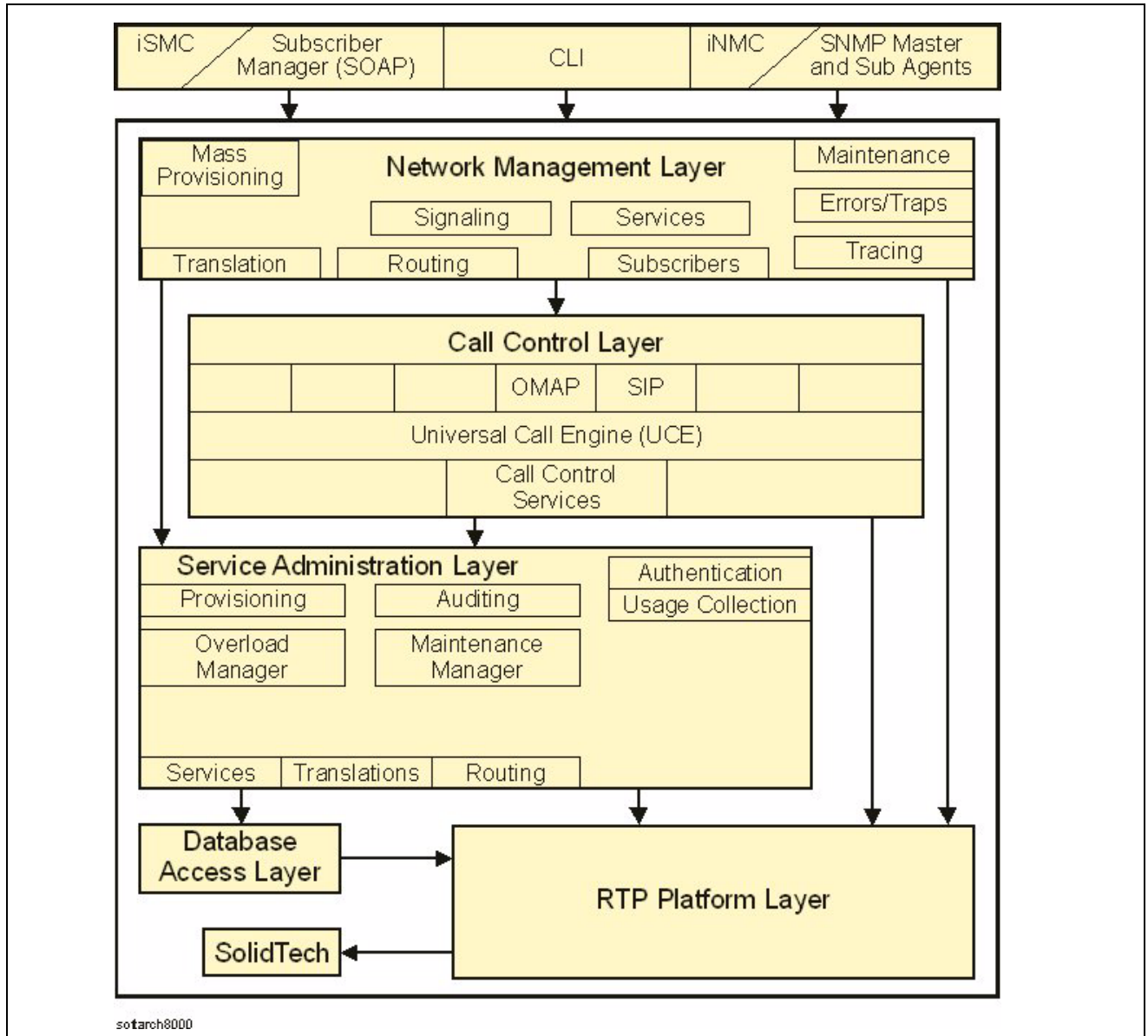


Figure 4-6 HiPath 8000 Software Architecture and Components

# HiPath 8000 Software Functional Overview

## HiPath 8000 Software Components

### 4.2.2.1 HiPath 8000 Active/Active Applications

The HiPath 8000 supports duplex active/active applications for cluster softswitches. During normal operation, the cluster operates in an active/active mode. In this mode, traffic is distributed evenly across the available nodes and across the available call processing instances within each node. Each node serves as a backup to the other node. During call processing, each process saves its contexts to the backup node at various points in the call.

Figure 4-7 shows a normal active/active mode scenario with the HiPath 8000 RTP contributing to system fault tolerance and scalability. When a hardware or software failure occurs, a backup node takes over the traffic of the failed node including the saving of stable calls. This is done by accessing the partner context pool.

(Note for graphic below: Digit Xtion = Digit Translation)

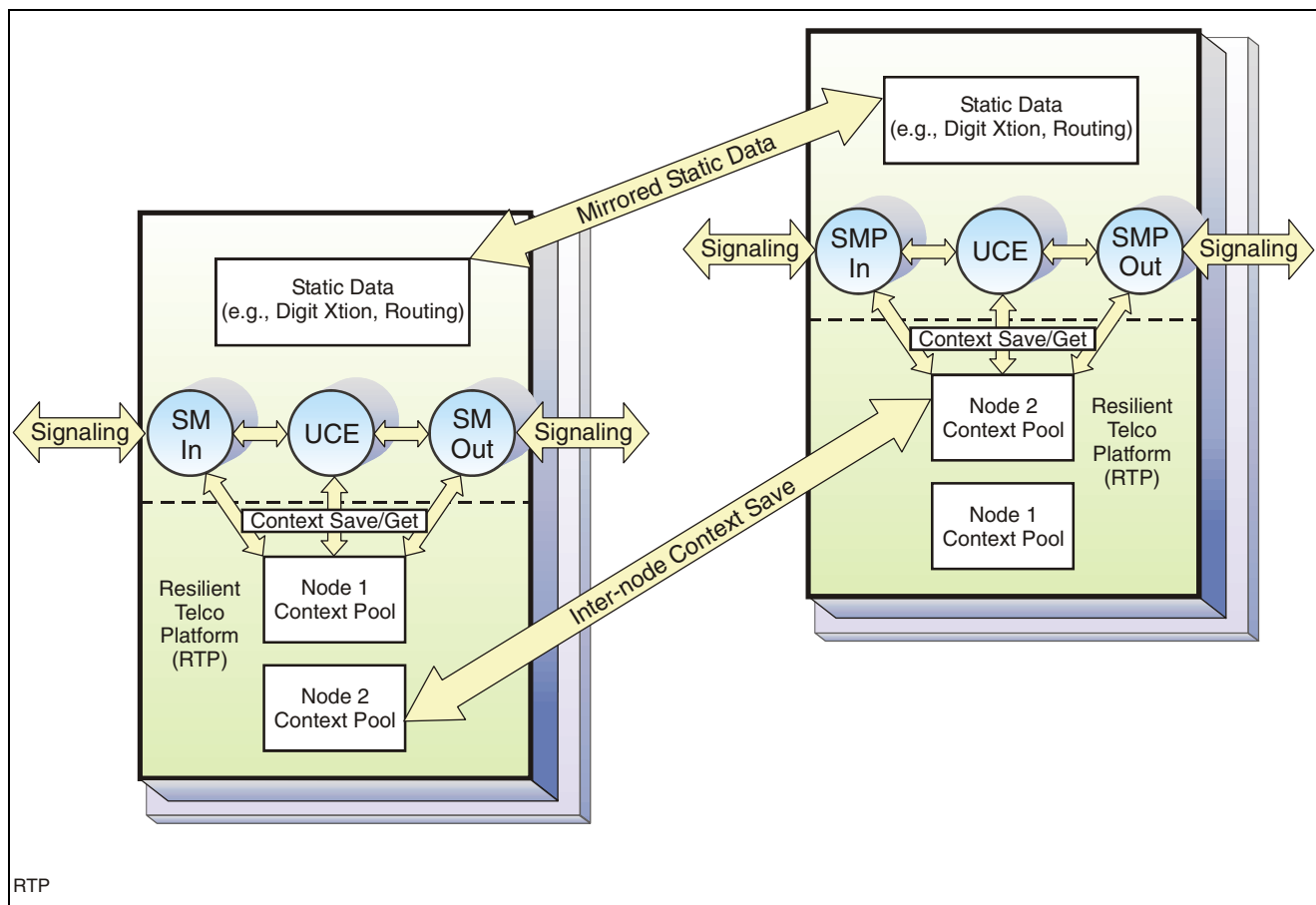


Figure 4-7 Normal Active/Active Mode with RTP Support

### 4.2.3 HiPath 8000 Call Control and Signal Processing

The HiPath 8000 call processing functions include the software components for bearer control, signaling processing, call control, signaling interworking, service control, and back-end database services. Figure 4-8 shows the overall software architecture of the HiPath 8000 call processing functions.

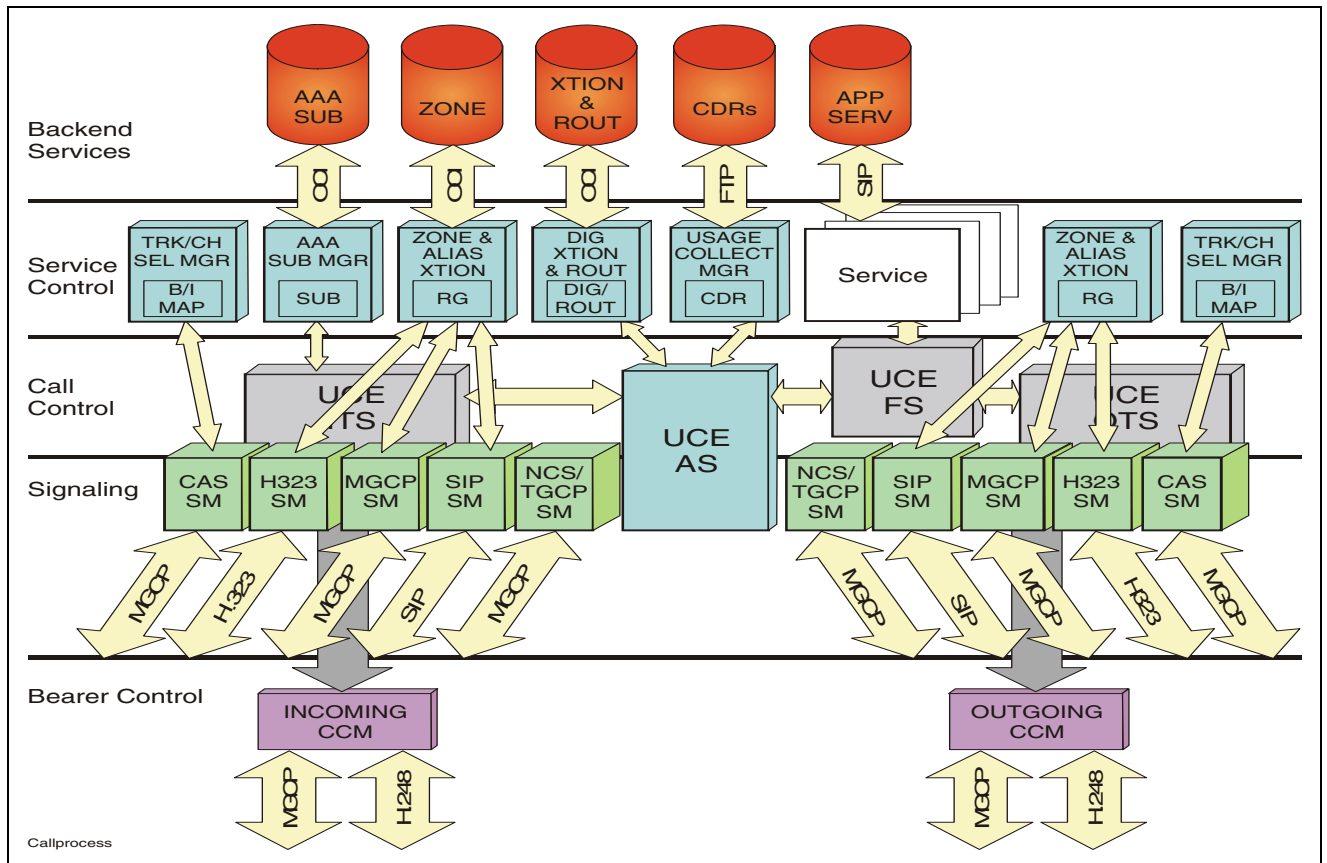


Figure 4-8 HiPath 8000 Call Processing Software Architecture

#### 4.2.3.1 Call Control

The key component of the HiPath 8000 call processing function is the protocol-independent Universal Call Engine (UCE). The UCE contains the generic switching functions of the HiPath 8000. It provides common logic to the signaling managers to route calls through the HiPath 8000.

Computer Support Telephony Application (CSTA) provides 3rd party call control into the HiPath 8000, which allows PC applications, HiPath ComAssistant to control calls to and from a co-located SIP phone. Currently, only SIP phones are being monitored. CSTA communication to the HiPath 8000 is through the Siemens CAP server platform.

#### **4.2.3.2 Service Control and Execution**

The HiPath 8000 provides a Service Logic Execution Environment (SLEE) to create, control, and execute native services typically supported on a Class 5 switch.

The supported native class supplementary services include Calling Number Display and Caller ID Blocking. Calling Number Display provides the calling party's directory number transparently. Upon handling a line termination, the service consults the subscriber's profile for the list of services to which the end user has subscribed. When a subscriber record indicates the Calling Number Display feature is enabled, the service passes the calling number for display. When the calling ID is indicated as blocked from the signaled information, as may be requested by the originating subscriber, the service does not display the calling ID information. Instead, an indication that the calling party number is private is displayed.

Caller ID Blocking is a service for originating subscribers. It prevents the display of a number at the terminating end.

The execution of native services is influenced by UCE events passed between the UCE components. These events can be observed, modified, or discarded to provide specific behavior modifications to basic call services. Services beyond basic call run under the control of UCE feature segment (FS) component.

Figure 4-9 shows the service control and execution environment.

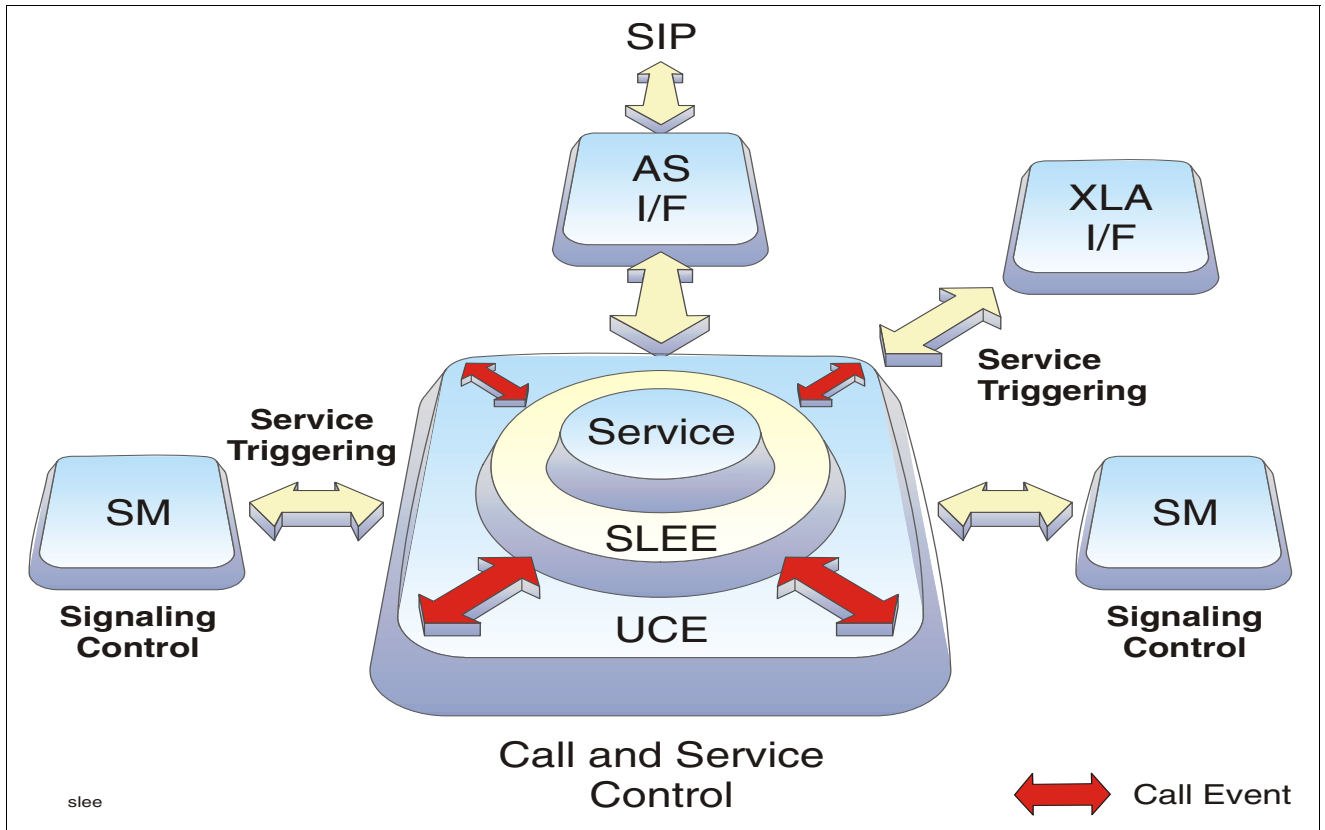


Figure 4-9 Service Control and Execution Environment

#### 4.2.3.3 Real-time Data Management

The HiPath 8000 supports memory based data management for realtime data access. It also supports dynamic data synchronization between nodes. This provides swift recovery response times when node failover occurs.

#### 4.2.3.4 Call Resource Auditing

The HiPath 8000 audits call resources. Audits are performed on a configurable, regular basis to ensure proper operation of the HiPath 8000.

### 4.2.4 Comprehensive Endpoint Support

The HiPath 8000 provides comprehensive endpoint support including POTS, SIP, and CAS.

## HiPath 8000 Software Functional Overview

### HiPath 8000 Software Components

#### 4.2.4.1 POTS

Plain Old Telephone Service (POTS) is the standard telephone service today. A next-generation switch must be able to support connections between POTS endpoints. A POTS endpoint, such as a POTS phone, is physically connected to a PSTN end office switch such as a Class 5 switch, a PBX, a Residential Gateway (RGW), or an Integrated Access Device (IAD).

The HiPath 8000 supports connections to POTS endpoints by interworking with the PSTN switch, a PBX and IAD indirectly through the media gateway (that is, Cisco SIP Gateway and HiPath 4000/HG3540 Gateway and RG 8700 Gateway).

#### 4.2.4.2 MGCP

The Media Gateway Control Protocol (MGCP) is an IP-based telephony protocol typically used between a Media Gateway Controller (MGC) and a Media Gateway (GW) to control connections between a PSTN and VoIP network. Initially for the HiPath 8000, the MGCP is used exclusively as the protocol for supporting announcements through the IP Unity Media Server.

#### 4.2.4.3 Session Initiation Protocol (SIP)

The Session Initiation Protocol (SIP) is an application layer protocol for the establishment, modification, and termination of conferencing and telephony sessions over an IP network. SIP is part of the overall IETF multimedia data and control architecture. It supports user mobility by proxying and redirecting requests to the user's current location.

The HiPath 8000 uses SIP for interacting with application servers to provide enhanced voice and IP telephony services and to control connections to SIP endpoints. The HiPath 8000 supports the SIP services in [Table 4-2](#).

SIP Services
Multiple types of call forwarding
Calling number delivery(with prepended PNAC, national, and/or international prefixes)
Flexible naming (e-mail address, individual's name, E.164)
Personal mobility
Terminal-type negotiation and selection
Caller and callee authentication
Blind and supervised call transfer
Invitations to multicast conferences

Table 4-2 SIP Services




SIP extensively uses the Session Description Protocol (SDP) to convey media capabilities and MIME encoding to facilitate formatting flexibility. It also uses a Border Gateway Protocol (BGP) algorithm, similar to BGP in IP routing, for stateless loop detection.

SIP uses many elements of IP protocols to create a seamless extension to ubiquitous Web paradigms. The main SIP elements mirror the client-server web server model. In SIP terminology, the User Agent Client is the caller, while the User Agent Server is the callee.

SIP transactions take place between User Agent Clients and User Agent Servers using SIP Proxy and Redirect servers. These servers provide personal mobility and mixed addressing resolution. SIP transactions consist of requests sent by User Agent Clients and responses sent by User Agent Servers.

### Transport Layer Security (TLS) Protocol

The TLS protocol (V1.0) provides encryption and data integrity between two communicating applications. TLS between SIP endpoints is supported.

 SIP signaling with TLS may also be referred to as SIPS.

Since TLS is applied on a hop-by-hop basis, end-to-end signaling security between SIP endpoints can only be ensured by HiPath 8000 when the originating SIP endpoint specifies the callee using SIPS Uniform Resource Identifier (URI) and the calling party is in the local administration domain. When SIPS URI is used, the system blocks the call when end-to-end TLS transport is not available between the caller and the callee, or between the caller and the administrative domain of the callee.

Using the HiPath 8000 system’s back-to-back user agent architecture, TLS is supported on the signaling connection between a SIP endpoint and the HiPath 8000 SIP signaling manager. See [Figure 4-12](#). End-to-end signaling security is achieved only when all hops of the signaling connection use TLS.

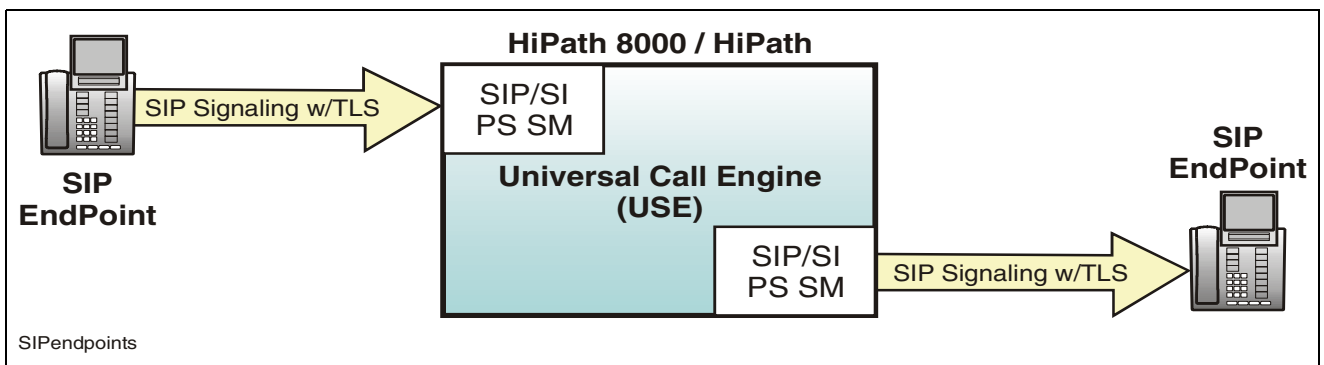


Figure 4-10 Hop-by-hop Application of TLS HiPath 8000 Back to Back User Agents

## HiPath 8000 Software Functional Overview

### *HiPath 8000 Software Components*

When the originating SIP endpoint specifies the callee using a SIP URI (rather than a SIPS URI), the system does not block a call when end-to-end TLS transport is not available. In this case, it becomes the responsibility of the customer to configure its network using only endpoint devices that support SIP over TLS in order to achieve end-to-end signaling security. SIP endpoints for which TLS support is required:

- optiPoint 410 S/420 S SIP Telephone
- hiPath 8000 SIP Softclient
- 3rd party SIP Telephone (for example, Cisco, Mediatrix, Polycom) and softclients (for example, Sigma) that supports TLS
- 3rd party media gateways (SIP<----> TDM gateway) that support TLS

### **SIP Call Examples**

This section describes two examples of SIP operation.

The first example establishes a call using a SIP Redirect Server. The second example establishes a call using a SIP Proxy Server. The calls are placed on a packet network with no PSTN interactions.

[Figure 4-11](#) shows a call setup using a SIP Redirect Server. In this example, **charlesd@bebo.com** is placing a call to **martinak@tool.com**. A description of the message sequence follows the figure.

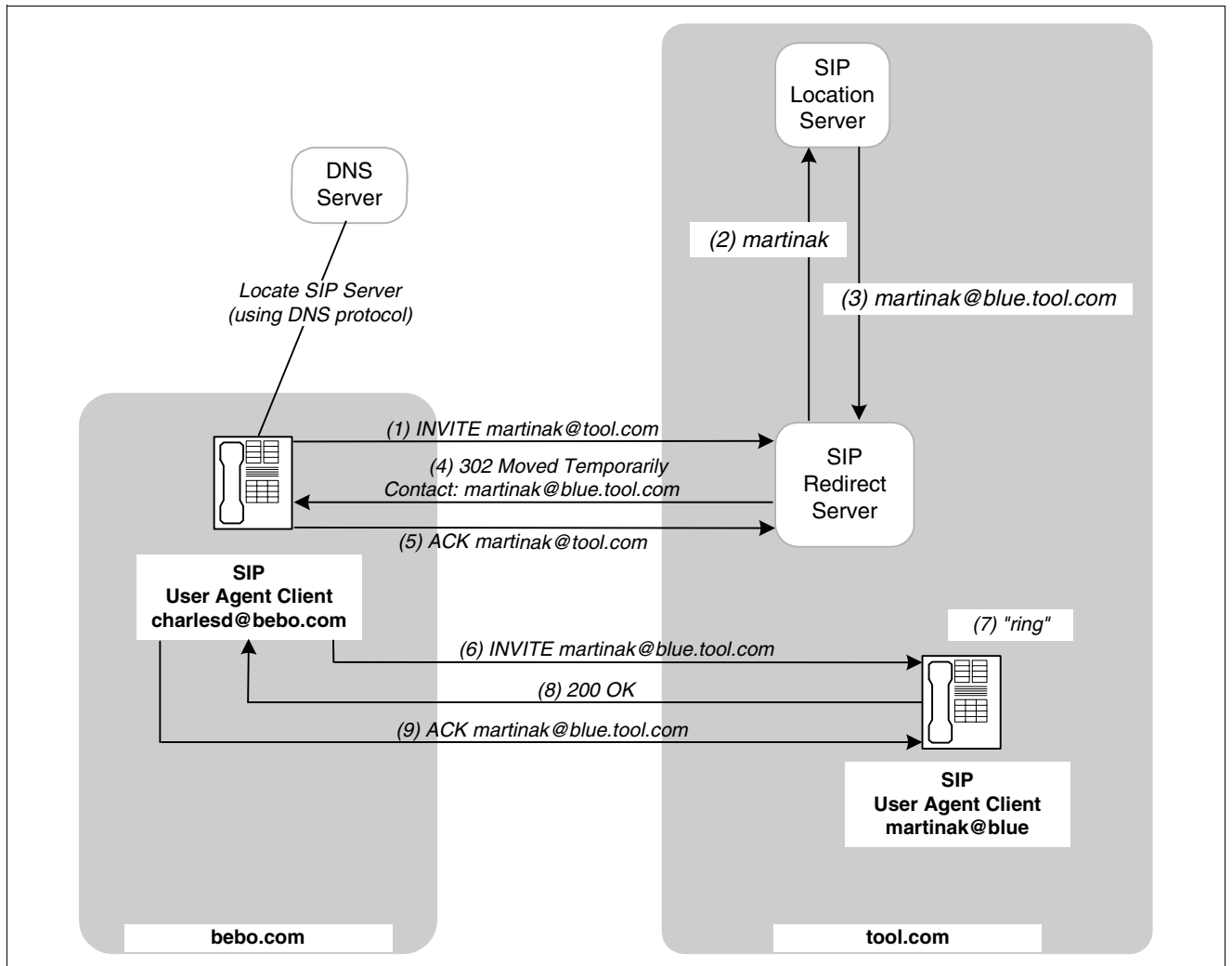


Figure 4-11 SIP Redirect Server Call Setup

The message sequence in [Figure 4-11](#) is as follows:

1. An INVITE message from charlesd@bebo.com which contains his contact information is sent to the SIP Redirect Server.
2. The SIP Redirect Server receives the INVITE message and sends the hostname to the SIP Location Server.
3. The SIP Location Server returns the current address to reach martinak@tool.com.

## HiPath 8000 Software Functional Overview

### *HiPath 8000 Software Components*

4. martinak@tool.com has moved from her normal location and registered this new information by sending a REGISTER method to the SIP Location Server. The SIP Redirect Server responds to the invitation from charlesd@bebo.com with a status code of 302, which indicates that martinak@tool.com has temporarily moved to a new address. Her new address is martinak@blue.tool.com.
5. An ACK message from charlesd@bebo.com acknowledges the SIP Redirect Server's response, which closes the INVITE transaction.
6. A new INVITE message is sent by charlesd@bebo.com to martinak@blue.tool.com.
7. The telephone for martinak@blue.tool.com rings.
8. When martinak@blue.tool.com goes off-hook, a 200 OK response is sent to charlesd@bebo.com.
9. A final acknowledgement message from charlesd@bebo.com to martinak@blue.tool.com indicates the call has been established.

Assuming a normal telephone call is established, an audio real-time transport protocol (RTP) stream flows between the two callers with bearer traffic. The call terminates with a BYE message which releases the call.

In [Figure 4-12](#), **charlesd@bebo.com** is placing a call to **martinak@tool.com** using a SIP Proxy Server. A description of the message sequence follows the figure.

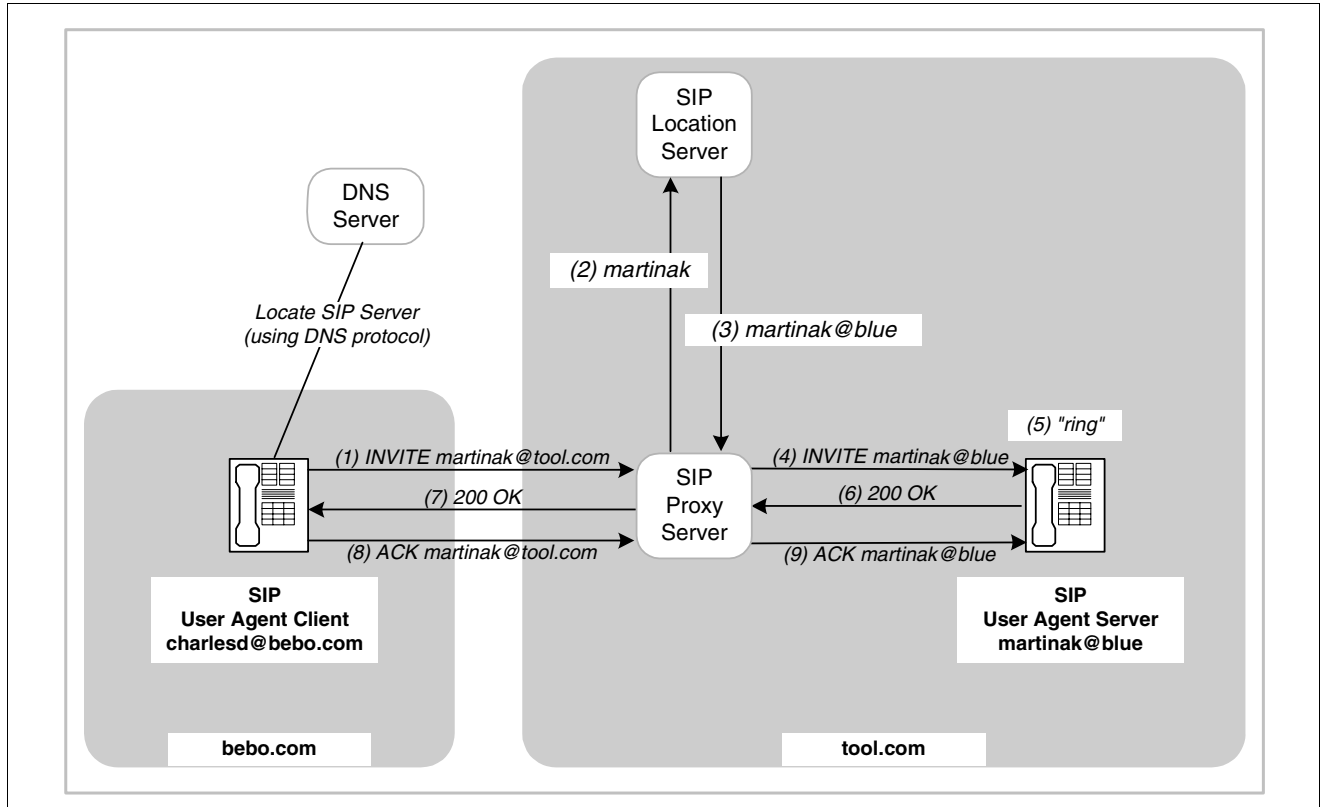


Figure 4-12 SIP Proxy Server Call Setup

The message sequence in [Figure 4-12](#) is as follows:

1. An INVITE message from charlesd@bebo.com which contains his contact information is sent to the SIP Proxy Server.
2. The SIP Location Server identifies that martinak@tool.com is now martinak@blue.com.
3. The SIP Location Server passes this information back to the SIP Redirect Server.
4. The SIP Redirect Server, acting as a User Agent Server, forwards the INVITE request to martinak@blue.com.
5. The telephone for martinak@blue.com rings and is answered.
6. The User Agent Server for martinak@blue.com sends a status code 200 OK response to the SIP Proxy Server.
7. The SIP Proxy Server sends a status code 200 OK response to the User Agent Client for charlesd@bebo.com.

## HiPath 8000 Software Functional Overview

### *HiPath 8000 Software Components*

8. An acknowledge (ACK) method retraces the path in the opposite direction through the SIP Proxy Server.
9. Another acknowledge (ACK) method retraces the path to the User Agent Server for martinak@blue.com and closes the call setup signaling.

## 4.2.5 Signaling Control and Processing

The HiPath 8000 supports the processing and interactions of the following signaling protocols. The next sections detail each signaling protocol.

- SIP-Q
- SIP

### 4.2.5.1 SIP-Q: QSIG Tunneled over SIP

The HiPath 8000 supports tunneling of QSIG/CorNet-NQ protocol over SIP protocol as a trunking interface, for example, between two HiPath 8000s or between the HiPath and RG8700 GW. This interface is called "SIPQ".

The SIPQ interface is intended to replace the NQ/QSIG over H.323 interface due to its lack of failover recovery. This first release of SIPQ is equivalent in functionality and feature support as the NQ/QSIG over H.323 interface with the additional support of sending a LIN when the call is an emergency call.

SIPQ - SIPQ pass-through is required, for example when a HiPath 4000 legacy user is routed over IP (i.e., SIPQ end-to-end via HiPath 8000) to another HiPath 4000 legacy user located a distance away (e.g., NYC - LA). This can save TDM costs for a customer.

The HiPath 8000 supports originating and terminating a call (i.e., via registered SIP device) sent/received over the SIPQ interface.

This feature addresses the interworking functionality necessary to provide SIP trunking with NQ/QSIG tunneling in order to interwork with:

- HP4000, and
- RG 8700.

This feature applies where one of the subscribers in a call is a SIP device and another party is behind a GW served by NQ/QSIG tunneling over SIP. A typical corporate network may consist of legacy PISNs/PBXs employing QSIG networking interconnected with an IP network employing SIP. A call can originate in either the QSIG or SIP network and can be interworked via a GW that provides translation/mapping between QSIG and SIP.

#### **4.2.5.2 SIP**

The HiPath 8000 uses the Session Initiation Protocol (SIP) to control calls between various SIP endpoints. SIP controls connections and calls between various endpoints such as:

- A SIP endpoint and a SIP Application Server (AS)
- SIP endpoints

The HiPath 8000 controls SIP endpoints. It implements a Back to Back User Agent (B2BUA) to control the calls between the two SIP endpoints.

The HiPath 8000 also includes a SIP registrar and SIP location services. The SIP registrar allows SIP endpoints to register with the HiPath 8000 and supply the mapping between the contact information and the present location at which that endpoint can be reached. The SIP location server allows the UCE to perform lookup requests for an E.164 number (public or private) and returns the current IP address for the corresponding contact.

An AS does not register with the HiPath 8000 SIP registrar. Instead, the AS is statically provisioned into the HiPath 8000 routing database based on service triggering criteria. A service could be triggered by the HiPath 8000 receiving a call with a particular dialed number, such as a 1-800 number. In this case, the HiPath 8000 simply routes the call to the AS using the SIP protocol.

Transport Layer Security (TLS) support between SIP endpoints is provided.

#### **SIP Over TCP**

The SIP implementation uses a UDP/TCP dispatcher to:

- Provide mediation between Unix UDP/TCP sockets and Resilient Telco Platform Inter Process Communication (RTP IPC).
- Handle IP address fail over.

Each UDP/TCP Dispatcher handles an IP address dedicated to SIP signaling. The dispatcher sends and receives UDP and TCP messages through Unix sockets. [Figure 4-13](#) illustrates the SIP Interface using the new TCP transport.

## HiPath 8000 Software Functional Overview

### HiPath 8000 Software Components

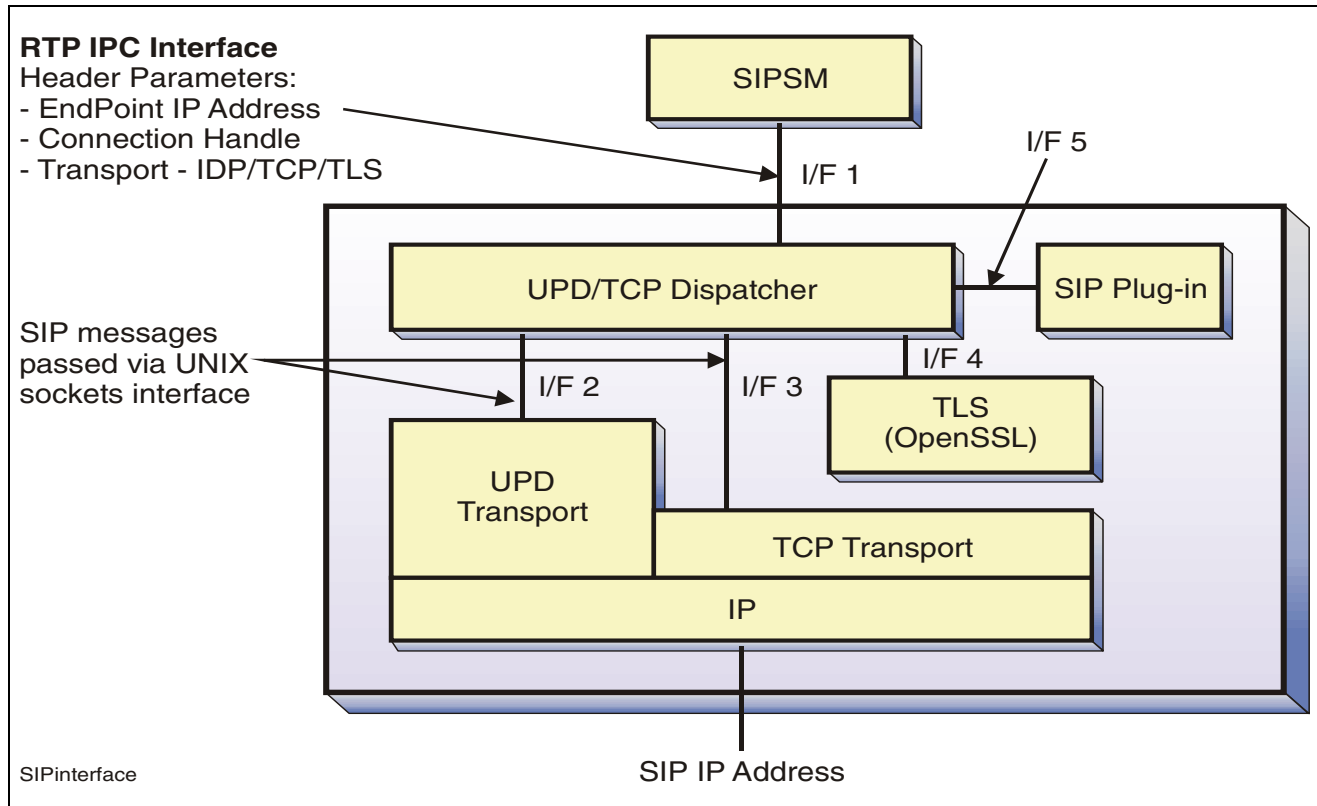


Figure 4-13 SIP Interface Block Diagram

Interface (I/F) 1 is provided by the RTP IPC, allowing the dispatcher to communicate to a SIP Signaling Manager (SIPSM) alias back-up group without knowledge of the physical location (CE\_1 or CE\_2) (cluster endpoints 1 and 2) of the SIPSM processes. The use of RTP IPC also allows the SIPSM to receive messages from dispatcher, UCE, timers, and so on, using a single IPC queue without the need for a mixed IPC socket communication mechanism. Additionally, interface 1 informs applications if a TCP connection fails and allows applications to disconnect TCP connections. The interface to the SIPSM (I/F 1) is performed through the existing UDP dispatcher with two new “header” parameters.

Interfaces 2 and 3 are Unix sockets which are supported.

Interface 4 is a set of library calls provided by OpenSSL.

Interface 5 is to the SIP plug-in which assembles the SIP messages read on interface 3.

The Dispatcher is a mediation device; it sends the receives SIP messages on interfaces 1, 2, and 3. The Dispatcher does not modify the SIP messages.

Endpoint IP address is already used by UDP dispatcher. The connection handle is a 32 bit integer used to identify a TCP connection. The transport type is UDP or TCP/TLS.



SIPSM is a multi-thread process; therefore, there may be only a single active process instance on each node, but there is also a standby process instance on each node.

## **4.2.6 Address Translation and Routing**

Address translation is the process of interpreting incoming digits and determining the appropriate destination or feature. The HiPath 8000 provides the following address translation and routing functions:

- Alternate routing
- Element mass provisioning for translation and routing
- E164 DN translation Public and Private - national, international, and subscriber
- Full node switch back enhancement
- Interchangeable NPA and NXX
- Most-matched digit translation
- Origin dependent routing
- Prefix digit translation — 1+, 101+, 011+, 01+, 0, 00, 0+ or any value barrier code such as “9” for off-net or “8” for on-net
- Private dialing and Numbering Plan (PNP) support
- Simultaneous support for 7-digit and 10-digit dialing (U.S. Market only; 7/10 digit dialing does not apply to ETSI which can be up to 14 digits)
- Vertical service code translation
- Zone Management
  - Alias Translation and Routing
  - SIP endpoint discovery

### **4.2.6.1 Alternate Routing**

The HiPath 8000 allows one or more alternate routes to reach a destination address, such as a E.164 destination number.

### **4.2.6.2 Element Mass Provisioning**

The element mass provisioning feature provides for the mass processing of provisioning commands. This feature only supports those commands that are available through the iNMC.

## HiPath 8000 Software Functional Overview

### *HiPath 8000 Software Components*

#### 4.2.6.3 E.164 Directory Number Translation

The HiPath 8000 supports national, international, and subscriber E.164 directory number translation. Digit translation is the process of interpreting incoming digits and determining the appropriate destination or feature. The features can include speed call and vertical services. When digit translation results in a feature, the feature is invoked.

Digit translation analyzes these types of numbers:

- E.164 international, national, and subscriber numbers
- FGD CAC (Feature Group D Carrier Access Codes)
- Dialed numbers that may or may not include prefixes

#### 4.2.6.4 Interchangeable NPA and NXX

The same NXX code can serve as both an office code (NXX) and an area code (NPA). Digit interpretation is based on subscriber dialing a prefix (0 or 1), critical timing when an ambiguous NXX code is recognized, or a combination of both. In some areas where these codes exist, 10 digit dialing is required to avoid ambiguity.

Use of the 0 or 1 prefix to denote 10 digit numbers avoids problems associated with critical timeout. However, this arrangement requires dialing of the home NPA code for 0+ (operator or credit card) calls within the home NPA. This problem arises with analog subscriber lines and ISDN lines with overlap signaling. Other interfaces are capable of unambiguously indicating the length of the digit string.

If prefixes are allowed for both 7 digit and 10 digit calls, then interchangeable NPA and NXX codes introduce ambiguity. For example, since 502 is both an area code and an office code, “0-502-6661” and “0-502-666-1234” cannot be distinguished before an analog subscriber dials the ninth digit. Critical inter-digit timing must be applied after the seventh digit to resolve conflict.

Conflict of interchangeable NPA and NXX codes is resolved by nature of address or code length. Nature of address is either signaled in from the previous switch or determined by prefix analysis. If the nature of address cannot be determined, code length is used to resolve the ambiguity.

“Nature of address” is an attribute of a call route that describes, basically, its type or its scope. Values for this attribute are:

- prefixed number
- subscriber number
- national number
- international number
- LRN (Location Routing Number)

- prefix-based number; and test call route

#### **4.2.6.5 Most-Matched Digit Translation**

In some countries, ambiguous codes are allowed. For example, in Germany, code 08 is the area code within Bavaria and code 089 is the area code of Munich. If digit string 089 is to be translated, the destination should be Munich; if a digit string 08x, where x is not equal to 9, the destination should be within Bavaria. Speed calling codes also introduce ambiguity. For example, in speed calling code 2 and NPA 201 are both allowed.

In the HiPath 8000, Most-Matched Digit Translation always searches for the longest matching digits to determine the destination and is used to resolve ambiguity in codes. For example, in speed calling digit translation does not stop at 2 to determine whether a speed calling code or NPA is dialed.

#### **4.2.6.6 Origin Dependent Routing**

Digit translation can translate the same destination code into different destinations based on originating rate area and/or originating class of service allowing originating rate area and/or class of service to affect routing decision.

#### **4.2.6.7 Prefix Digit Translation**

The HiPath 8000 supports the following prefix dialing schemes (provisioned for the US market):

- International Call Prefixes — 01 and 011  
01 + CC +N (S) N, 011+CC+N (S) N
- National and Toll Call Prefix — 1  
1+NPA-NXX-XXXX, 1+NXX-XXXX
- Operator Call Prefixes — 0 and 00  
0, 0#, 00, 0+NXX-XXXX  
0+NPA-NXX-XXXX (except 0+SAC+NXX-XXXX for selected SACs, for example, 800)
- FGD CAC (Feature Group D Carrier Access Code) Prefixes — 10 and 101  
10XXX, 101XXXX
- Private Numbering Plan which includes extension numbering up to 7-digits, L0, L1 and L2 region levels

## HiPath 8000 Software Functional Overview

### *HiPath 8000 Software Components*

#### **4.2.6.8 Private dialing and Numbering Plan (PNP) Support**

There is mechanism to simultaneously support translation and routing of one or more dialing and numbering plans including E.164 and private dialing and numbering plans. A private dialing and numbering plan (PNP) exists in a private network used by the subscribers belonging to a Tenant/Business/VPN group. For example, subscriber within a business group can dial each other by 4 digit extensions.

#### **4.2.6.9 Simultaneous Support for 7-Digit,10-Digit and 14-Digit Dialing**

Digit translation allows the end user to call the same E.164 destination by dialing either the destination's national number or subscriber number. For example, an end user can dial 561-955-1234 or 955-1234 to reach 561-955-1234 and digit translation translates 561-955-1234 and 955-1234 to the same destination. Also allows for extension dialing and regional dialing when applicable. For International Dialing, phone numbers are often written in this format: +44-(0)1224-XXXX-XXXX. This expresses the numbers used for both international and national long-distance calls. In the example, +44 indicates the country code, while (0) indicates the NDD (National Direct Dialing). When dialing from outside the country, the NDD would not be used after dialing the country code; when dialing from within that country, the NDD would be used, but the country code would not.

#### **4.2.6.10 Vertical Service Code Translation**

The Vertical Service Codes (VSCs) feature provides for user-dialed codes that allow access to customer access to features and services provided by local exchange carriers, interexchange carriers, commercial mobile radio service providers (CMRS), and so on. Services invoked by VSCs include call forwarding, customer originated trace, and many others. The format of a VSC is \*XX or \*2XX (touch tone).

#### **4.2.6.11 Zone Management**

The HiPath 8000 zone management capability provides alias translation, dynamic endpoint registration and unregistration, endpoint admission control, and gatekeeper discovery.

##### **Alias Translation**

The HiPath 8000 SIP gatekeeper performs alias translation to resolve the aliases to an IP transport address when it receives a list of destination aliases for an endpoint. If the gatekeeper manages the endpoint, the aliases are translated into the call signaling address and RAS address of the endpoint. If another gatekeeper manages the endpoint, the aliases are translated into the call signaling transport address of the far-end gatekeeper.

## SIP Endpoint Registration

SIP endpoints can dynamically register their aliases and transport addresses with a gatekeeper by sending an RRQ (Registration Request) message, or dynamically unregister themselves by sending a URQ (Unregistration Request) message to the gatekeeper. The gatekeeper grants the request with an RCF (Registration Confirm) or UCF (Unregistration Confirm) message, or declines the request with a RRJ (Registration Reject) or URJ (Unregistration Reject) message.

As part of their configuration process, all SIP endpoints register with the gatekeeper identified through the discovery process. Registration occurs before any calls are attempted and may occur periodically, and dynamically with dynamic IP data, as necessary (for example, at endpoint power-up). An endpoint sends a Registration Request message to the gatekeeper to register.

Dynamic endpoint registration data is maintained persistently in the database and in the XLA(Translation and Routing) shared memory for use during real-time call processing.

### 4.2.7 QoS Control

The HiPath 8000 uses MGCP to populate a number of connection control parameters to the media gateway to control Quality of Service (QoS) on the bearer capability. [Table 4-3](#) describes the QoS control parameters configurable through MGCP.

Attribute	Description
Codec	The encoding methods (G.711, G.723.1, G.729A, and G.726) the media gateway uses for VoIP calls.
Packetization Period	The packetization interval for a VoIP call, in milliseconds of speech to put into each packet.
Type of Service	Enables differentiated services when IP packets are routed through QoS-capable routers.
Resource Reservation	Reserves resources along the voice/data path. The values are: <ul style="list-style-type: none"> <li>● Guaranteed service</li> <li>● Controlled load</li> <li>● Best effort</li> </ul>
Silence Suppression	Automatically detects silence to prevent the transmission of empty packets. The options are on or off.

Table 4-3 HiPath 8000 QoS Attributes

## HiPath 8000 Software Functional Overview

### HiPath 8000 Software Components

#### 4.2.8 Operation, Administration, Maintenance, and Provisioning (OAM&P) Features

The HiPath 8000 provides the following OAM&P services:

- Service management provisioning through iSMC
- Mass provisioning
- Push and pull Call Detail Records (CDRs)
- Disaster recovery through backup and restore
- Rolling upgrade
- Authentication, Authorization and Accounting (AAA)

Figure 4-14 shows the HiPath 8000 OAM&P architecture.

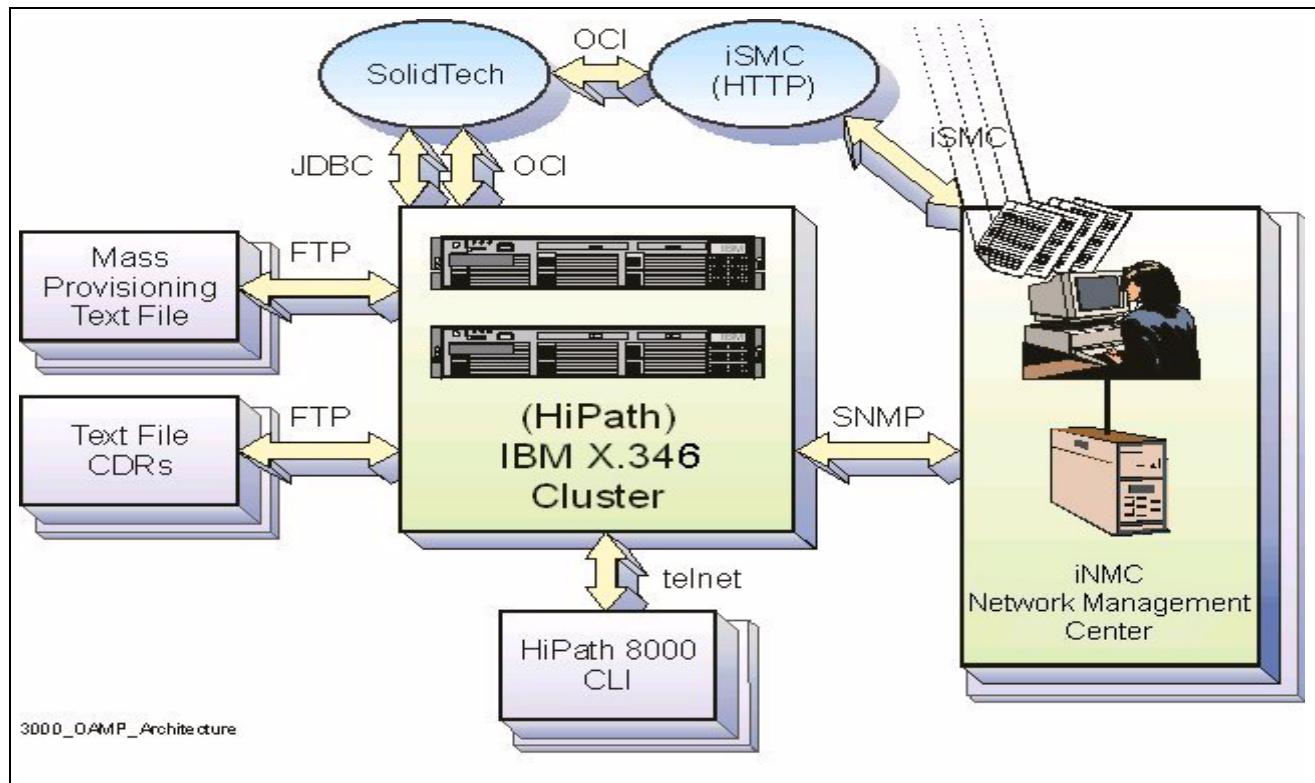


Figure 4-14 HiPath 8000 OAM&P Architecture

#### **4.2.8.1 iSMC**

The *iSMC* is a Web-enabled Service Management Center designed to provide users at a Service Provider's Service Center with information and provisioning control over subscribers' voice services. Service provider personnel can view current service provisioning for a particular subscriber, can view the historic service actions (subscription, activation, deactivation, modification) that were undertaken by the subscriber or on the subscriber's behalf (future requirement), and can provision service changes (subscription, activation, deactivation, modification) on behalf of the subscriber. *iSMC* can be installed by itself, but when Subscriber Self-Care is needed, the *iSSC* should also be installed.

#### **4.2.8.2 iSSC**

The *iSSC* is a Siemens provided application that enables web service support for service providers who want to give their subscribers the ability to manage their own services. It is intended to provide a rapid start for these providers, allowing them to customize the look and feel, the service options, and the packaging of services – and quickly roll out self-provisioning to their customers. For subscriber services and features supported by the HiPath 8000, *iSSC* screens are provided to enable users to subscribe and to modify the settings of the services to suit their personal preferences and needs. These are generic screens that the service provider wants to modify to have their own look and feel and to integrate into their existing Web pages; by providing these prototype pages and all the HTML, XSL and CSS documents to support them, the time it takes to make the services available through the service provider's web portal is cut to a fraction of the time it would take were they to create the pages from scratch.

#### **4.2.8.3 Call Detail Records**

The HiPath 8000 generates and maintains Call Detail Records (CDRs) for usage collection and billing purposes. The HiPath 8000 UCE maintains CDR information in the active call context, which can follow the call from process to process and node to node. At the end of every call, a CDR is generated. However, intermediate CDRs are also generated once every 30 minutes, and CDRs are generated intermittently for long duration calls, such as those that pass over midnight more than once. The RTP middleware has an integrated ticket handling capability that handles the individual CDRs.

The HiPath 8000 CDR handler manages the internal binary billing files through the RTP API and makes them available to a billing server. The CDR handler also converts and formats these internal binary billing files. An external agent can pull the completed and formatted billing files from the HiPath 8000 through FTP.

#### **4.2.8.4 Rolling Upgrade**

The Rolling Upgrade feature performs software upgrades without affecting service. Rolling Upgrades of the HiPath 8000 applications in a cluster can be performed as long as the new software is compatible with the old software. In this case, one node is stopped and upgraded

## HiPath 8000 Software Functional Overview

### *HiPath 8000 Software Components*

with new software. This node is restarted and then the other node is stopped, upgraded, and restarted. An online update mechanism for RTP can be used to upgrade RTP applications through the CLI. This procedure includes the use of mirrored disks and a fallback strategy.

#### **4.2.8.5 User Authorization, Authentication and Accountability**

The identity of all initiators, that is, human operators, applications and remote systems, must be verified. This verification is called peer entity authentication (short: authentication).

Authentication is done before a user is granted first access to a system, that is at the beginning of a session or association set up. The purpose of authentication is to make sure that the initiator is the one claimed Identification and secure authentication are sufficient to counter unauthorized system access. They are prerequisites for access control on resources.

Authentication can be achieved by a number of mechanisms that are often based on secret information only held by the communication partners. for example:

- Passwords
- Protected passwords (for example: encrypted passwords, one-time passwords, replay protected passwords)
- Authentication by chip cards (and user PIN)

Secure authentication requires the confidentiality of the (secret) authentication information, for example, a clear text password transmitted through an open network may be stolen by eavesdropping and used for masquerade attacks. A more secure authentication would require a stronger mechanism, for example, the use of replay protected passwords.

Data origin authentication assures that the source of data received is as claimed. Data origin authentication, if applied, is done for every data unit, for example, for every message, received. This can be accomplished by providing a digital signature for the data. Digital signature mechanisms can also guarantee data integrity, that is, make sure that the data was not modified by a third party.

The NMC supports a unique userID and password for each user. User authorization is controlled by assigning a user to an Access Profiles and Node Groups.

The NMC provides two mechanisms to control user permissions. The first is the Access Profile, which controls which NMC and NE functions the user is authorized to perform. In addition, inactivity timeouts may be provisioned on a Access Profile basis. The second mechanism is the Node Group, which controls which NE a user is allowed to access. The definition of both Access Profile and Node Group are administrable. These mechanisms allow the service provider to assign user privileges based on their operational organization and their corporate security policy.

The SMC supports a unique userID and password for each user. User authorization is controlled by assigning one or more user roles to the user to allow the service provider to assign user privileges based on their operational organization and their corporate security policy.



Accountability is the property that ensures that the action of a user may be traced back uniquely to the user. Accountability provides an internal proof that a certain communication or action did occur. This function counters the threats caused by incorrect orders and their repudiation inside the operating company.

Accountability requires Identification/Authentication and security audit mechanisms.

#### **4.2.8.6 Software Packaging**

The HiPath 8000 software uses modular UNIX packaging. A package is a collection of files with embedded configuration details that instruct the installing program on file attributes, locations, install and uninstall procedures, and system requirements. All System V UNIX systems support a package toolset that allows easy and robust installation or uninstallation of software applications.

#### **4.2.8.7 Backup & Restore**

The HiPath 8000 enables backup and restore of the system database and files through the iNMC Server. The Maintenance Manager Server (MMS) runs maintenance tasks (known as jobs) on the HiPath 8000. The MMS supports the starting, stopping, and querying of jobs through a client/server API. There are several MM clients supporting the jobs control interfaces. This includes an SNMP client, a CLI client, a menu-driven client called the Command Console, and a scheduler client to schedule jobs. The backup and restore procedures are controlled through any of these clients.

The iNMC is the primary administration tool to control jobs. It communicates with the MMS through the Maintenance Manager SNMP client. The iNMC provides a graphical user interface to control jobs and query job information.

The HiPath 8000 Assistant provides:

- Display of performed backups and restores
- Automatic and manual backup options
- Schedule generation for automatic backup

You can set the time and day for the backup. You can also set when the next automatic backup should be performed.

- Immediate activation of a manual backup

Afterwards you can view whether the backup was successful.

- Storage location selection option
- You can select the storage location (file system or database)
- Maximum number of backups

## HiPath 8000 Software Functional Overview

### *HiPath 8000 Software Components*

If the maximum number of backups has been performed, you must delete old backups before you can create new ones.

- Delete backups
- Restore from backups

Note that if you are restoring a file system, the restored files are copied to the location specified.

From there, you have to do a manual restoration.

## 4.3 HiPath 8000 Assistant Software

### 4.3.1 Software Deployment Details

The software deployment details below show the distinction between applications running on the HiPath 8000 server and applications running on separate hardware.

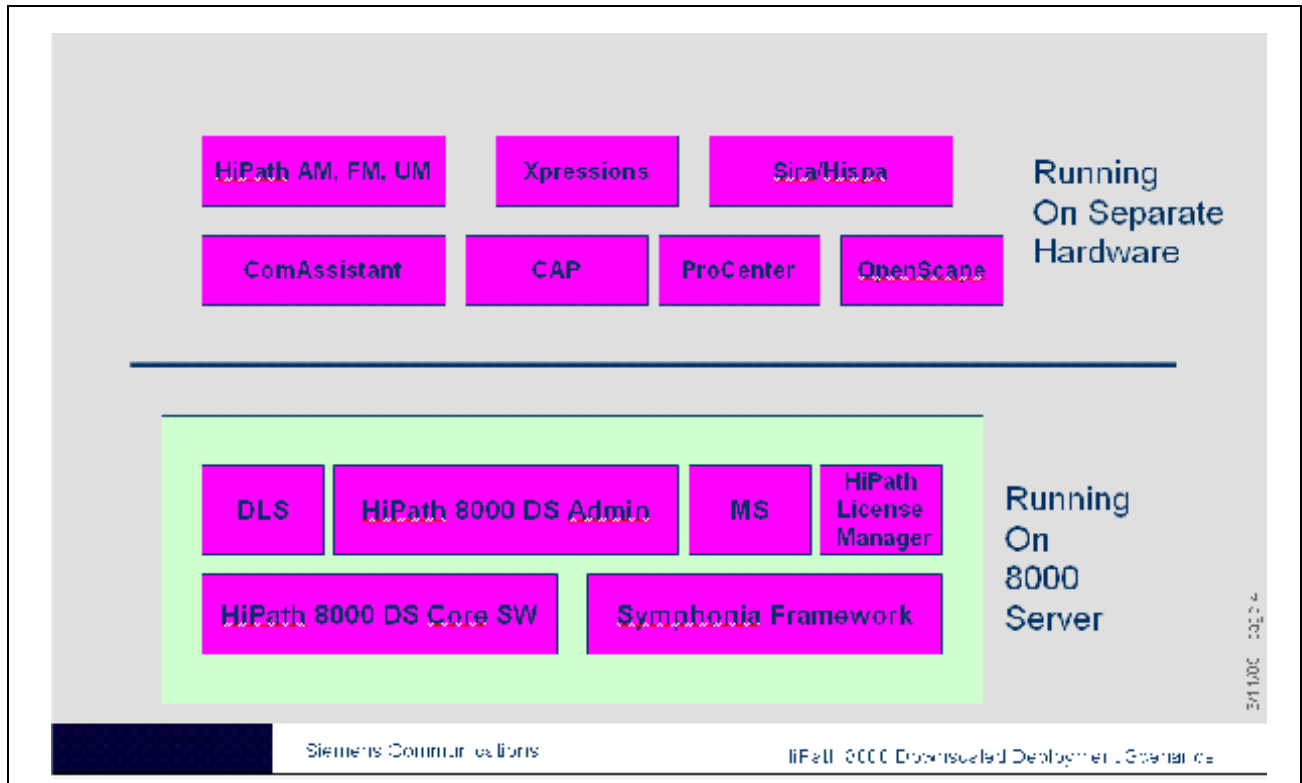


Figure 4-15 HiPath 8000 Assistant Software Deployment

### 4.3.2 HiPath 8000 Assistant – Context Overview

The HiPath 8000 Assistant application integrates into the HiPath 8000 Assistant UI FrameWork.

# HiPath 8000 Software Functional Overview

## HiPath 8000 Assistant Software

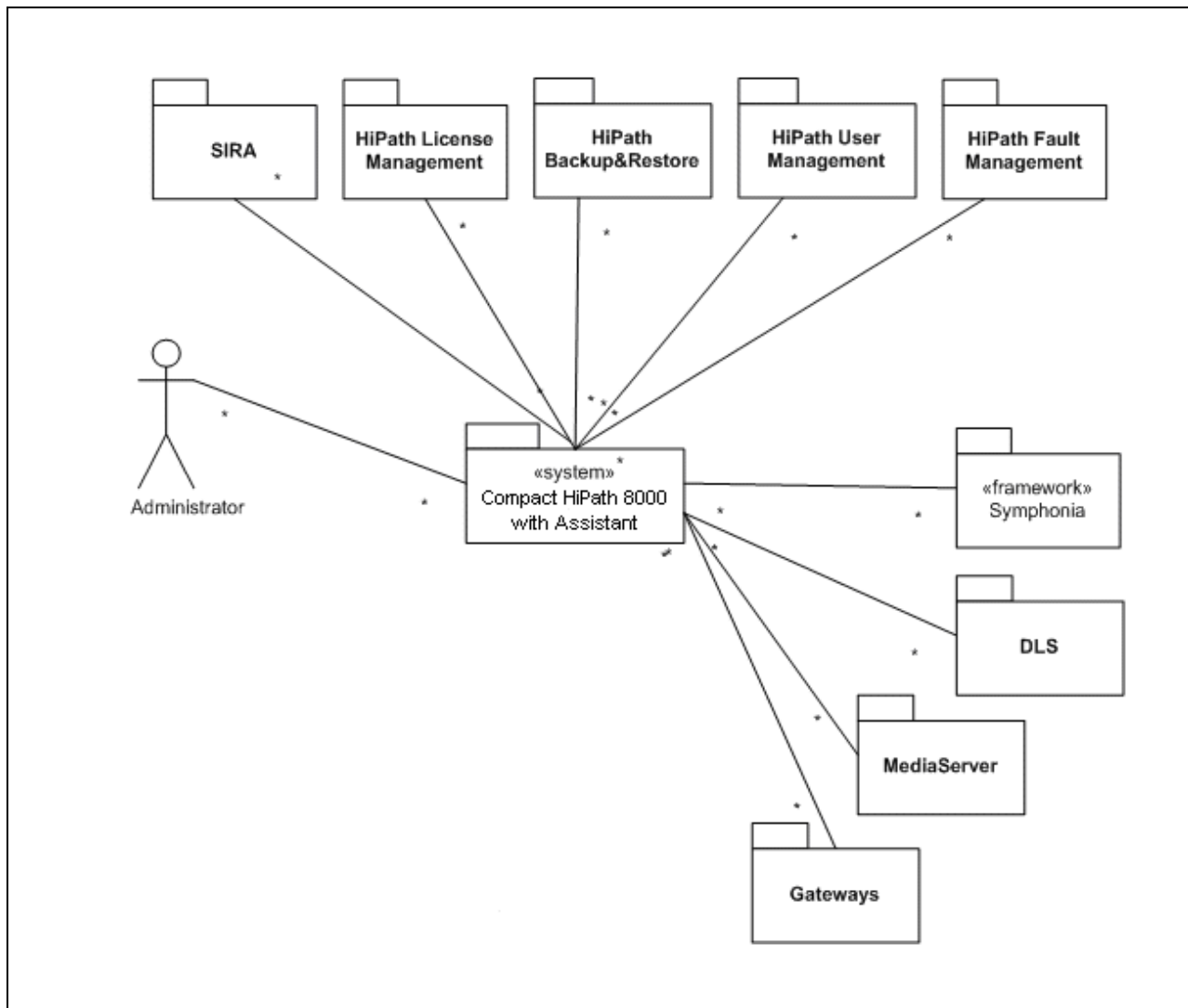


Figure 4-16 HiPath 8000 Assistant Software Context

## **5 Cluster Redundancy**

This chapter introduces the Cluster Redundancy functionality in the HiPath 8000. This includes identifying the ingredients of Cluster Redundancy and how they fit into the components of the HiPath 8000 and attain reliability goals. The HiPath 8000 failover strategy is also introduced.

### **5.1 Cluster Redundancy Concept**

Reliability is the primary goal of the HiPath 8000. A cluster is essentially a piece of operating system software that manages hardware reliability by using redundancy. A cluster package makes sure that operating system resources are reliable and manage their failover.

Clusters show a single system image to the operator, whereas network computers (such as a Microsoft Windows NT network) appear as a number of separate computers. Clustering is necessary as a base for a reliable softswitch.

In addition to the operating systems, cluster packages are provided to link the individual nodes into a cluster. They support the cluster interconnect and offer applications well-defined interfaces which are required for cluster operation. These interfaces include inter-node communication which is used by processes on different nodes to communicate with each other. Unlike other external communication interfaces that are available in every operating system, the inter-node communication supports redundant connections for availability reasons and a low latency protocol. A short latency period (i.e. the time required to send a message to another system and receive an acknowledgment) is just as important to the scalability of a cluster as the line throughput rate, though both are obviously closely linked. Additional functions are also available for cluster management.

Another important function of the cluster package is cluster administration. Because of associated interfaces, most of which are Web-based, system administration in the cluster is every bit as straightforward as for a standalone system. A central console, which is responsible for all nodes, simplifies this task considerably. The cluster package provides the network administrators with a single system image, hence they see the individual nodes and operating systems only if necessary.

A reliable component structure provides an effective base for cluster administration. The HiPath 8000 main hardware components include:

- IBM 345/346 Linux
- Ethernet Switch
- Remote Supervisor Adapter (RSA)

All these components work together to attain the following reliability goals:

## **Cluster Redundancy**

### *Cluster Redundancy Concept*

- Provide faster data replication and better performance for peak traffic in normal operation by using a two node Active/Active configuration; each node is acting as hot/standby for its partner. This configuration also insures against silent faults through continuous hardware/software monitoring and testing.
- Minimize node switch-over which reduces transient call loss and network connectivity outages. This is accomplished with redundant local disks, network connections for each node and power supplies. Each node also contains duplicated Ethernet cards which ensure that the physical path for the external communication with one node is backed up by a second path (2nd Ethernet port on different Ethernet card and 2nd LAN switch).
- Static load sharing provides a fast and reliable busy/idle handling since only the node writes the busy/idle and call status for subscriber, or feature server.
- Effective component management through process configuration control using process and alias groups.

## 5.2 Cluster Redundancy System Components

The HiPath 8000 works with a number of hardware components. [Figure 5-1](#) reflects a situation where the IBM systems connect to the external network via both Ethernet switches. Sections 5.2.1 and 5.2.2 refer to [Figure 5-1](#), which illustrates one version of system architecture for the HiPath 8000.

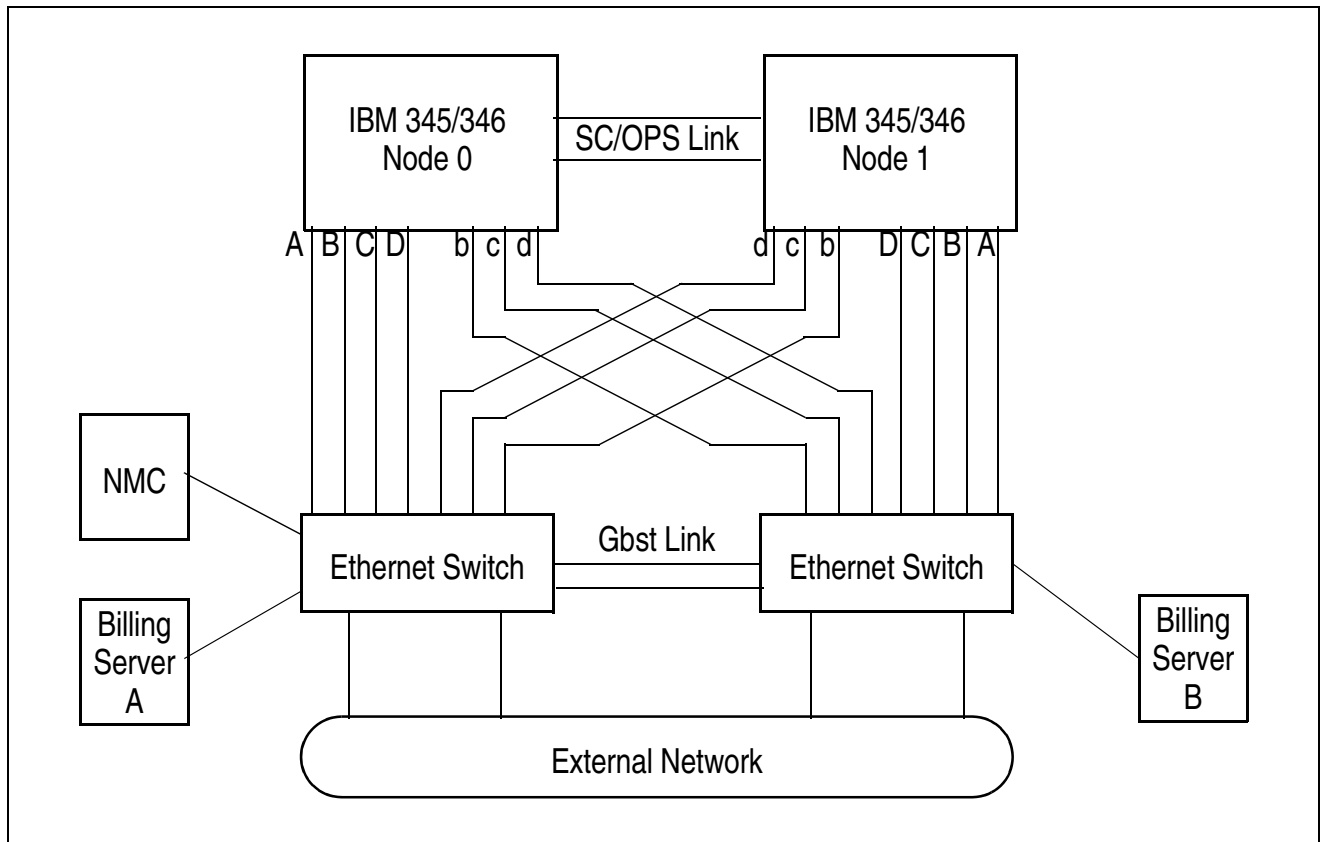


Figure 5-1 Example of a HiPath 8000 System Architecture Configuration

### 5.2.1 IBM 345/346 Linux

Two IBM 345/346s form the core of the HiPath 8000. Each configured IBM two Intel® Xeon™ processors up to 3.6GHz with 533MHz front-side bus speed. Up to eight GB of DDR memory, 5 PCI (4 PCI-X) slots, up to 6 hard disk drives and an integrated dual Ultra320 SCSI with RAID-1 for data protection

The base operating system on the IBM is SuSe LINUX Enterprise Server 9 (SLES-9).

Each IBM has eight 100 Megabit Ethernet links set up as four pairs, and controlled by Fujitsu-Siemens PrimeCluster. A redundant pair of cross-over cables interconnect the IBMs. A separate link labeled “A” from each IBM to each ethernet switch is for RSA. Three pairs connect

## Cluster Redundancy

### *Cluster Redundancy with Node Separation*

to the Ethernet switches and are labeled as “A/a”, “B/b”, “C/c” and “D/d”. The upper case letter depicts the active link, and the lower case letter depicts the standby link. These pairs correspond to RTP, Billing, and Call Processing and Network Management, respectively.

### 5.2.2 Ethernet Switch

The two Ethernet switches are layer 2 switches that allow several devices to interconnect. As can be seen in [Figure 5-1](#), the IBM systems connect to the external network via both Ethernet switches. This process gives the system a measure of redundancy, hence protecting it in the event that one of the Ethernet switches fails.

### 5.2.3 Remote Supervisor Adapter (RSA)

With clusters, there is always the necessity to resolve the situation where two nodes of a cluster think that they are in charge of the same resources and functions (e.g., when the two nodes cannot communicate). In this situation (sometimes referred to as “split brain avoidance”), it must be ensured that a node can only become active when the other node has been stopped unconditionally.

The “split brain avoidance” mechanism of PrimeCluster requires a safe hardware interface to eliminate (e.g., power down or reboot) a node. An additional PCI board, IBM’s RSAII (remote supervisor adapter) allows automatic server shut down.

## 5.3 Cluster Redundancy with Node Separation

Geographic node separation reduces the risk of total loss of voice services when one of the nodes is out of service due to a fire, flood, hurricane, building damage, etc. The HiPath 8000 provides node separation via redundant fiber optic cable as shown in [Figure 5-2](#).

Each node has six Ethernet links that are paired and bonded to support the following three redundant connections from each node:

- Management (Bonding\_dev0: eth0 and eth5)
- Signaling (Bonding\_dev1: eth2 and eth6)
- Billing/CDR (Bonding\_dev2: eth 4 and eth 7)

In addition, two additional links are used for Cluster Communication.

Split brain is corrected by sending an SNMP command to the RSA board of the partner node in order to power down that node. A timing mechanism is used in conjunction with the SNMP command to prevent both sides from killing each other, so that just one node powers down and the other node remains active.



**Cluster Redundancy**  
*Cluster Redundancy with Node Separation*

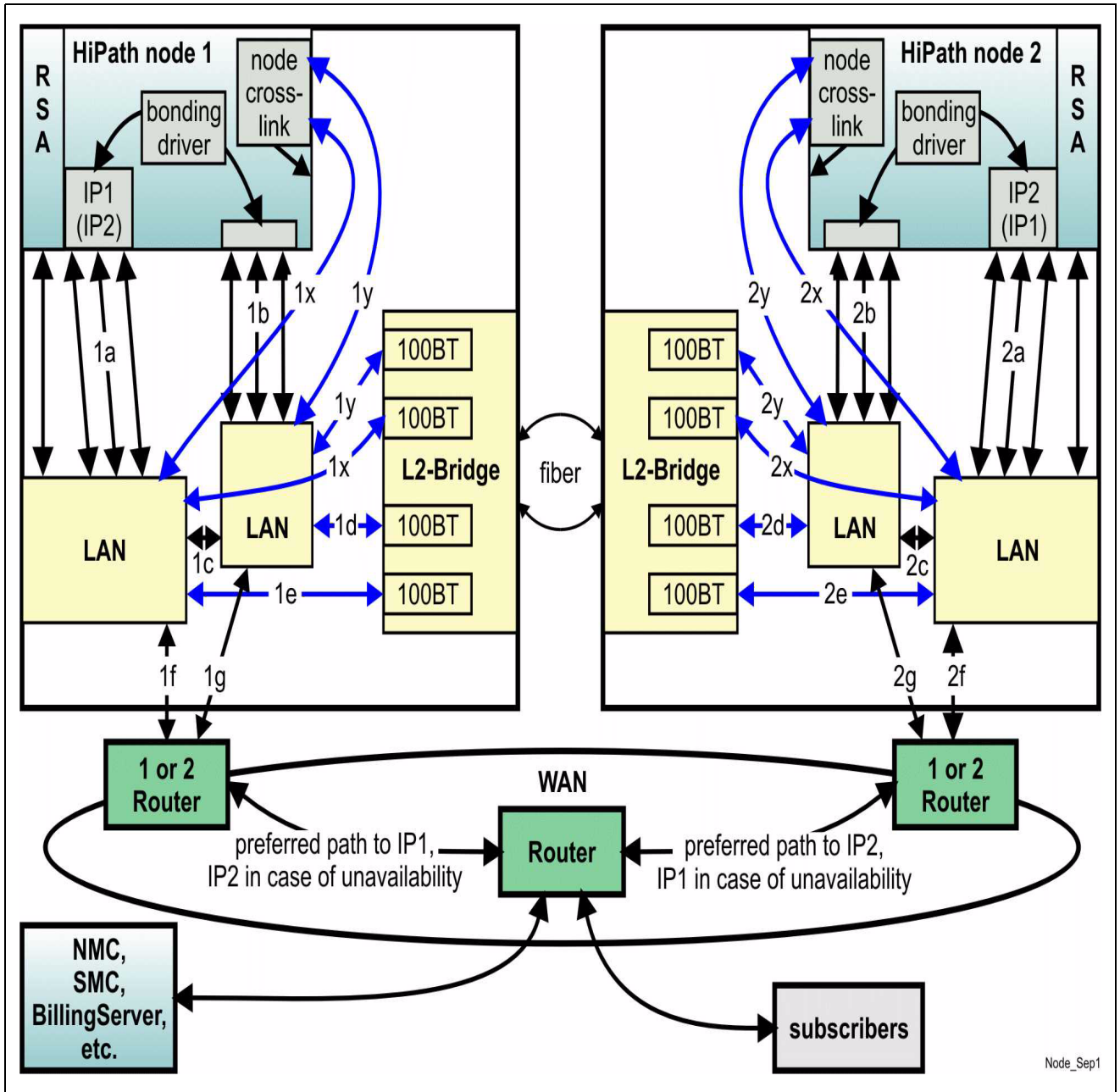


Figure 5-2 Cluster Redundancy Node Separation

## Cluster Redundancy

### *Cluster Redundancy Basic Functionality*

The following is required to support a general solution for node separation:

- Two redundant layer-2 connections between the two locations where the nodes are located.
- Two layer-2 LAN switches at each location with connection to the routers of the WAN.
- Layer-3 router connections to each site with rerouting capability of the same IP destination address to the partner site.
- A secure layer-3 connection between the two locations to carry the SNMP traffic between each node and its partner RSA. The RSA board does not offer built-in security for the RSA connection, therefore security for this connection will be provided using external equipment, for example, by providing a secure tunnel by using a Cisco router for the RSA to partner node connection.
- Each HiPath 8000 node is connected to the WAN for OAM&P, signaling, and billing/CDR. For redundancy reasons the connection to the routers is run via two LAN switches. Switch-over is performed by the Linux bonding driver.
- The cluster interconnect of the two HiPath 8000 nodes are connected with two 100BaseT Ethernet connections via a redundant layer-2 bridge.
  - This connection needs to transport ARP messages between the two locations. This requires the same VLAN(s) for the related virtual HiPath 8000 addresses of both nodes at both locations. Otherwise a router failover would not be detected by one of the HiPath 8000 nodes.
  - The connections have to run through different LAN switches to assure that the cluster interconnect fails when both LAN switches are out of service.
- The HiPath 8000 RSA card is connected with the partner HiPath 8000 node via SNMP over the WAN. This allows the HiPath 8000 node to power down its partner in case both links of the redundant cluster interconnect go down ("split brain avoidance").
- Installation of two IPUnity media servers (one at each node site) is recommended to prevent loss of media functions (i.e., tones and announcements) in the event of a location failure.

All redundant links use separate physical paths for maximum reliability. In addition, the RSA connection uses a separate physical path from the redundant cluster interconnect links.

## 5.4 Cluster Redundancy Basic Functionality

The HiPath 8000 provides a very large enterprise Real Time IP System that includes a SIP-based hosted real-time communication overlay network application that can be deployed and managed from a customer's data center. The HiPath 8000 is located in a very large enterprise data center and serves small, medium and larger enterprise locations that are distributed.

The HiPath 8000 solution supports advanced multi-media and multi-modal services, advanced applications as presence, instant messaging and others and tightly integrated mobile workers into one seamless enterprise network. [Figure 5-3](#) illustrates the high-level architecture of the IBM X.345/346 Linux system, which is characterized by complete redundancy with no single point of failure.

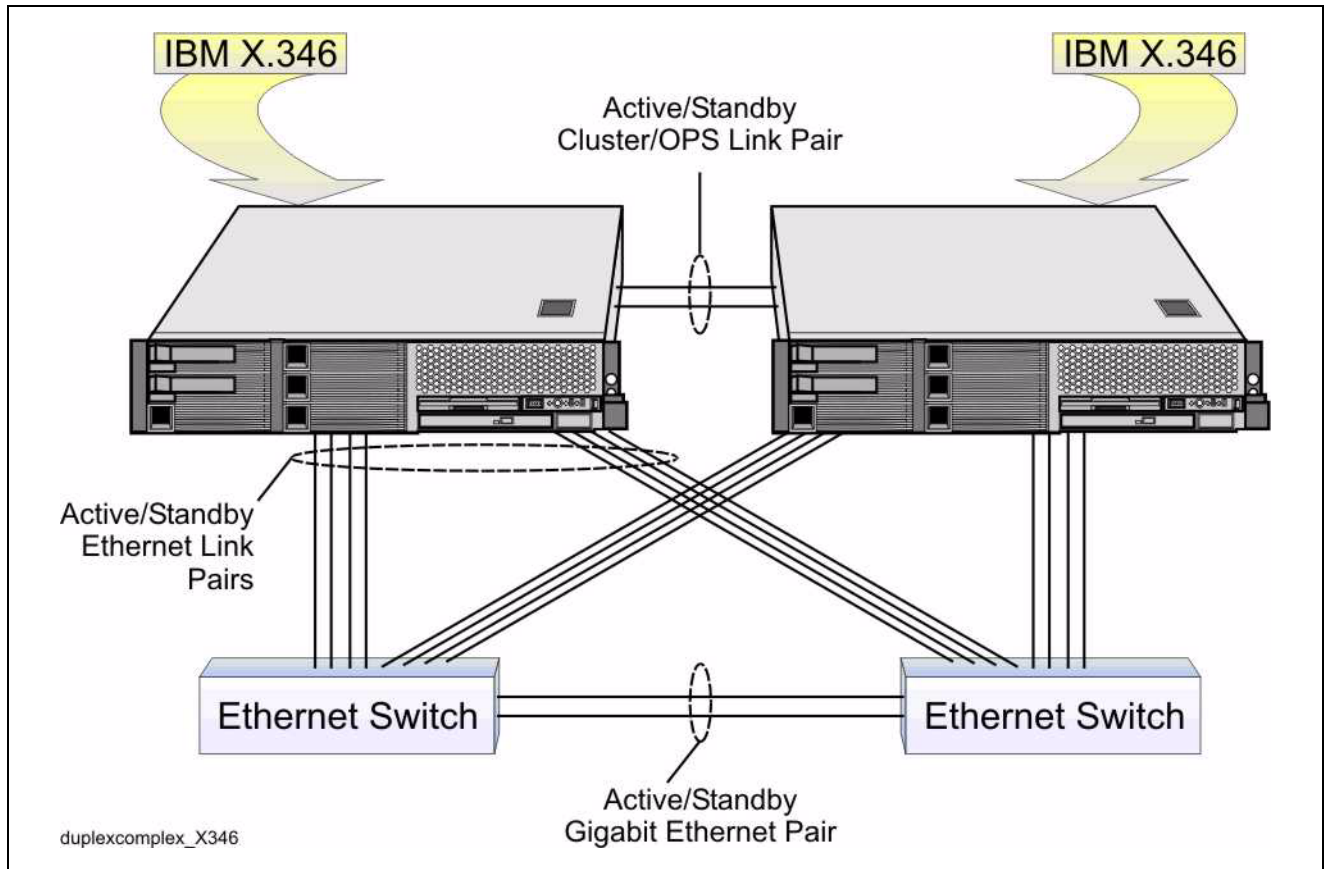


Figure 5-3 HiPath 8000 Redundancy Configuration

The system database uses SolidTech, which is a non-sharing database with data replication on both nodes. The SolidTech database attaches to the chief database, which may be located on its own node or its partner's. In case of a node failure, the application may lose the database connection, but the Linux software automatically reattaches itself.

At the heart of HiPath 8000 V2.1 are fully redundant proxy registration servers (real-time media transaction controllers) that operate on an industry-standard Linux server over a Quality of Service managed network. This application can reside and be managed from a data center like any other traditional data application.

[Figure 5-4](#) provides a detailed illustration of the clustered connectivity.

## Cluster Redundancy Process Configuration

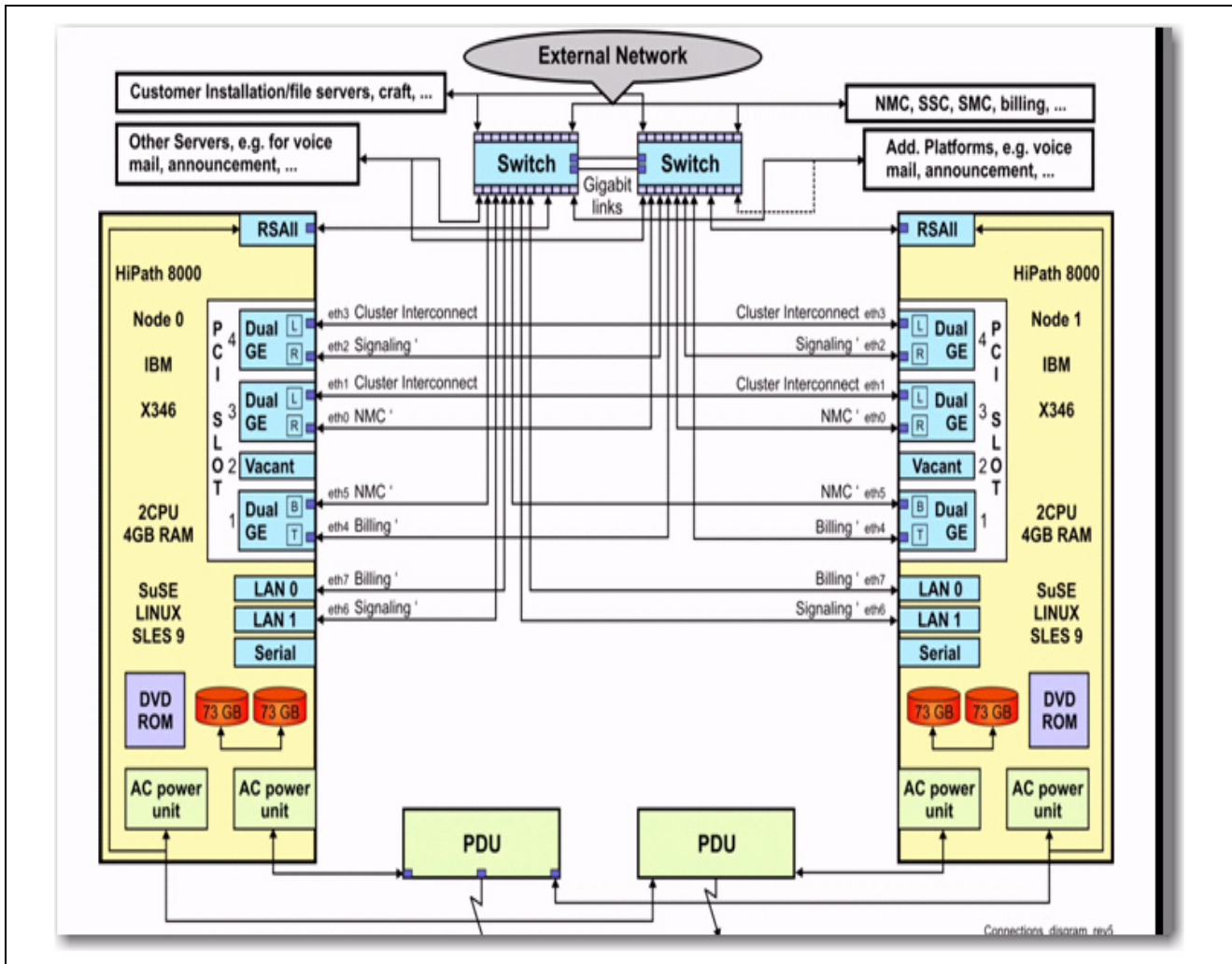


Figure 5-4 HiPath Redundancy Configuration

### 5.5 Process Configuration

The HiPath 8000 uses the Fujitsu-Siemens Computers Resilient Telco Platform (RTP) to run and manage the processes necessary for configuration, call processing, performance monitoring, and system maintenance. RTP provides redundancy and load sharing capabilities by enabling multiple Computing Elements (CE), or logical nodes, within the system. While one process may be running on one CE, another process may be running on another CE within the system. Because the RTP can initiate multiple instances of the same process, different instances of the same process may run on different CEs within the system.

Table 5-1 defines process elements of the HiPath 8000 implementation of RTP services.

<b>Element</b>	<b>Description</b>
Standalone Process	HiPath 8000 processes (or programs) that come up at switch startup that are not part of RTP process groups.
Configured Process	HiPath 8000 processes (or programs) that come up at switch startup that are part of RTP process groups.
Process Group	One or more processes or instances of processes with similar functions.
Process Alias	A single identifier representing one or more processes.

Table 5-1 Process Elements



The files described in the following sections are read by RTP only when the “CreateRTP” command is executed. When they are read, RTP writes the contents into the SolidTech database for later use by the “StartRTP” command.

RTP processes can be monitored to ensure that the RTP is functioning correctly and to detect and troubleshoot process issues if RTP problems occur. The NMC and CLI display detailed status information about Standalone Processes, as well as about Configured Processes, which are processes that are included in Process Groups. In addition, the NMC and CLI display information about the Process Groups that organize multiple processes or instances of processes with similar functions.

The NMC and CLI also display information about all the Aliases configured within the system. Each Alias represents one or more processes via a single identifier.



Processes and aliases may be started and stopped manually only from the CLI.

### 5.5.1 RTP Startup Groups and Dependencies

The most basic task of the node manager during startup is to launch the local RTP processes. The two means to control the order in which they are launched are startup groups and dependencies among these groups.

The descriptions of both the groups and the dependencies are stored in database tables, and can be configured by means of \*.tcn files, and the CLI. Although this configuration applies to all nodes in the RTP cluster, startup and checking for dependencies among groups are handled for each node separately.

## **Cluster Redundancy**

### *Process Configuration*

A startup group is a (possibly empty) set of RTP processes that controls startup and shutdown of a node. RTP distinguishes between sequence and parallel groups. In a sequence group, you can control the startup order of processes within that group. There is no such order in parallel groups.

The means to control the startup order between groups are the dependencies. A dependency may be defined between two arbitrary groups, but cycles in the set of dependencies are of course not permitted. The node manager does not start a group before all groups it depends on are in running state. A process is said to be running if its process state is RTP\_NM\_RUNNING. The definition when a group is in state RTP\_NM\_GRP\_RUNNING depends on whether it has members or not. If it has, the condition for it to be running is precisely that all its member processes must be running. An empty group is considered to be running if all groups it depends on are running and the platform is starting up. (The latter definition also applies if an empty group depends on an empty group.)

The construct of an empty group mainly facilitates the definition of dependencies. RtpReady is an example of an empty group, and defining a dependency to it actually introduces to all RTP platform processes, since RtpReady depends on all groups.

### **5.5.2 RTP Alias Groups and Members**

RTP process groups that can be used as addressable units in the RTP inter-process communication are called alias groups or simply aliases. Aliases are defined in database tables that list their properties and their members. An RTP process may be a member of more than one alias. It is not allowed to define an alias member that is itself an alias.

Alias play an important role in the RTP process management. The node manager needs to keep track of alias configurations. Whenever an RTP process starts or terminates, there is a change in the configuration of all aliases that the process is a member of. A process may change its active memberships, e.g., reduce its alias memberships step by step during a shutdown to terminate in a controlled manner. An RTP process that is listed as a member of an alias needs to call RtpNmReady to become an active member. An alias can be used for RTP inter-process communication if at least one of its members is active.

There are eight types of aliases, and the resolution of an alias name into an active member name depends on the alias type. The types are

- Equal load distribution
- Local equal load distribution
- Exclusive local equal load distribution
- Local best queue
- Broadcast
- Remote broadcast

- Backup alias
- Persistent backup alias

The alias types have the following meanings and resulting resolution strategies:

#### **5.5.2.1 Equal Load Distribution**

The message is sent to a single member. The members are addressed one by one in a round-robin fashion. The next member in turn is selected as the receiver.

#### **5.5.2.2 Local Equal Load Distribution**

The message is sent to a single member. The members on the local node are addressed one by one in a round-robin fashion. The next local member in turn is selected as the receiver. If there is no local member, a remote member is selected according to equal load distribution.

#### **5.5.2.3 Exclusive Local Equal Load Distribution**

The message is sent to a single member. The members on the local node are addressed one by one in a round-robin fashion. The next local member in turn is selected as the receiver. The selection fails if there is no local member.

#### **5.5.2.4 Local Best Queue**

The message is sent to a single member. The member on the local node with the largest amount of available space in its queue is selected as the receiver. If there is no local member, a remote member is selected according to equal load distribution.

#### **5.5.2.5 Broadcast**

The message is sent to all members of the alias.

#### **5.5.2.6 Remote Broadcast**

The message is sent to all members of the alias, which do not run on the local node.

#### **5.5.2.7 Backup alias**

A backup alias is an RTP group of processes that defines a configurable failover hierarchy of its members. The two roles determining the dynamic behavior are:

- The primary receiver: A message directed to the backup alias is always sent to the primary receiver.



## Cluster Redundancy

### *HiPath 8000 Failover Strategy*

- The secondary receiver: The next member in the alias group that is prepared to take over the task of the primary receiver in case the latter is no longer available.

Only members with queue status "fully available" may become primary or secondary receiver. To simplify the discussion, instead of speaking of a process with queue status "fully available", we simply say that the process is "fully available".

A process becomes "fully available" when it calls `RtpNmReady` or `RtpNmChangeAliasMembership` with mode set to `RTP_NM_ATTACH_BACKUP_ALIASES`.

A process is no longer "fully available"

- if it is explicitly stopped, or
- if it calls `RtpNmDetach`, or
- if it explicitly detaches from its aliases (by calling `RtpNmChangeAliasMembership` with mode set to `RTP_NM_DETACH_ALL_ALIASES`), or
- if it fails and cannot be restarted, or
- if the node it is running on crashes.

### 5.5.3 Contexts

A context is data stored in memory. Contexts may, for example, be used to store "consistency points" and so allow for non-stop programming. A consistency point is the current status of a job.

The context manager is responsible for managing these contexts. In principle, it should be possible to store contexts in a database. For performance reasons, however, this is not a suitable option. Therefore, the concept of mirroring (replication) context data on another cluster node has been chosen: One node holds the master copy of the context and another one the backup copy.

A context is unique throughout the cluster. Context Type definitions can be found in the file "SrsCommon.h" as "eSrsContextType". Context parameters are fully defined in file "RtpCtx.parm". All contexts are created with "Mode=Static".

## 5.6 HiPath 8000 Failover Strategy

The primary focus of the HiPath 8000 failover strategy is to preserve stable calls and billing data, and to ensure that resources are not left in a hung condition. In this context, "hung" means unable to be accessed without restarting a device, gateway, or even the system itself.




In all of the following descriptions, it is assumed that if a backup component (hardware or software) fails while it is acting on behalf of a primary, and before the primary has been restored to service, then calls may be lost and/or service may be affected. The depth of the service degradation will depend on the specific component that has failed.

### 5.6.1 Process Failover

Any single process instance failure will not be service affecting, with the possible exception of the call (context) which is being processed at the time of the failure. Each call context of a particular type is accessible by all process instances of that same type. For example, all UCE contexts are accessible by all UCE instances.

In a cluster system, if the last process instance of a type fails on a node, then the backup instances on the backup node will take over. If the last process instance of a type fails on the last active node, then service will be affected as shown in [Table 5-2](#).

 [Table 5-2](#) assumes that there are at least two instances of every process.

Failing Process	Consequence
Universal Call Engine	All calls dropped with a loss of the last 30 minutes of CDRs.
CSTA Signaling Manager	All CSTA calls dropped and new call attempts denied.
AAA Manager	All calls requiring authorization denied.
CDR Handler	CDRs accumulate until process is restarted.
XDM	SIP calls blocked.

Table 5-2 Failing Processes

### 5.6.2 Node Failover

In a cluster system, if a node fails, then stable calls (those in conversation state) will be preserved but unstable calls may be dropped. If the failing node is the last active node in the system, then all ongoing calls and their related billing data will be lost.

### 5.6.3 Ethernet Card Failover

In addition to the on-board 10/100 Ethernet port, the system will accommodate three dual 10/100 Ethernet (QFE) cards. Also, a 10/100 port resides on the SCSI card. These cards are configured as follows:

## Cluster Redundancy

### HiPath 8000 Failover Strategy

Main board	RTP and NMC primary
SCSI card	Billing primary
QFE0 Port 0	PrimeCluster / SolidTech backup
QFE0 Port 1	Call Processing primary
QFE0 Port 2	
QFE0 Port 3	RTP and NMC backup
QFE1 Port 0	PrimeCluster / SolidTech backup
QFE1 Port 1	Call Processing backup
QFE1 Port 2	
QFE1 Port 3	Billing backup.

#### 5.6.4 Ethernet Switch Failover

In a cluster system, both Ethernet switches actively handle call data. The two Ethernet switches allow several devices to interconnect. As can be seen in [Figure 5-1](#), the IBMs have duplicate connections to both Ethernet switches.

If an Ethernet port on any one of the system components fails, that port is switched to its duplicate port connected to the other Ethernet switch. Any traffic on that system component will go to the new Ethernet switch on its path, via the gigabit link, to the first Ethernet switch and continue to its original destination.

For example: if Port A on Node 1 fails, all the data will switch to Port a on Node 1. The data will then pass from the Ethernet switch connected to Port a, through the Gbit link, to the Ethernet switch connected to the failed port, Port A. The data then continues on its intended route.

If a complete failure occurs in the Ethernet switch that is carrying active call data, each system component detects the failure and switches its links to the other Ethernet switch so no data is lost.

The Linux Bonding Driver provides an Ethernet port switch-over function similar to NAFO or IPMP. Two Ethernet ports, preferably on different components of the same node, have the same Ethernet address. The bonding driver provides three options:

- Act-stb where stb port is more or less visible (only one used);
- Act-act, some kind of port aggregation (only supported by some LAN switches);

## 6 Element and Network Management

This chapter describes the element and management features for the HiPath 8000.

### 6.1 Element and Network Management Overview

Management of the HiPath 8000 is supported based upon two configuration options using the following methods:

Standard HiPath 8000 configuration

- simple network management protocol (SNMP) version 3
- a command line interface (CLI)
- an element management system called the Network Management Center (iNMC)
- a subscriber management system called the *iSMC/iSSC*

Compact HiPath 8000 configuration

- simple network management protocol (SNMP) version 3
- a command line interface (CLI)
- an internal element and subscriber management system using the HiPath 8000 Assistant

iNMC is a Java-based application that provides a graphical user interface (GUI) to augment traditional Command Line Interface (CLI)- and Simple Network Management Protocol (SNMP)-based methods of configuring the HiPath 8000. The iNMC user interface provides a graphical view of network operations and stores configuration information in an object database.

For subscriber management, two additional management components extend a Web-based interface to HiPath 8000 Administrators and their subscribers. These components are called *iSMC* and *iSSC*, respectively.

*iSSC* is a toolkit for providing call feature control to subscribers through a Web portal. In essence, *iSSC* provides a SOAP/XML interface into selected feature configuration subsystems on the HiPath 8000. When integrated into a Web portal, subscribers have the option to configure their features (for example, call forwarding, caller rejection, and so on.) through the Internet, in addition to through the conventional telephone keypad interface.

*iSMC* is a superset of the *iSSC*. It provides personnel with the ability to control all subscriber-related capabilities and features. Some features and capabilities are only accessible through the *iSMC*.

The **HiPath 8000 Assistant** is a web-based application running within a browser. It provides a cost effective IP-based system for the 300 - 5,000 user Enterprise that seamlessly interworks with the entire HiPath portfolio.

## **Element and Network Management**

### *Element and Network Management Overview*

Its functionality allows the user to:

- Create, modify, and delete HiPath 8000 Assistant users
- Create, modify, and delete Business Groups (BGs)
- Create, modify, and delete subscribers (BGLs)
- Create, modify, and delete Numbering Plans (NPs)
- Create, modify, and delete DNs (Directory Numbers)
- Create, modify, and delete End Point Profiles (EPPs)
- Subscribe to, activate, modify, deny, and unsubscribe from services
- Create, modify, and delete Hunt Groups (HGs)
- Create, modify, and delete Call Pickup Groups
- Generate and view the Security and Provisioning logs
- Add, modify, and remove intercepts
- Generate and view BG Call Statistics

HiPath 8000 Assistant architecture is characterized by the following properties:

- Single and comprehensive tool for complete administration and maintenance
- Single node
- Trainable to Level 1 Technician & Customer Administrator
- No redundant data
- Web-based client
- Integration of external tools
- SuSE Linux Enterprise Server 9.x

### **6.1.1 Comprehensive Management Tools**

The HiPath 8000 provides an RTP-based system with the following management applications and services:

- Platform
  - Operating System
  - RTP Node Manager

- Event Manager
- Logging
- Tracing
- Statistics Manager
- Signaling
  - Universal Call Engine (UCE)
  - SIP SM
  - MGCP SM
- Translation/Routing
  - PSTN routing, destination, trunks, gateway
  - Zone/Endpoint Management
  - Digit Translation and routing
- Services
  - Authorization, Authentication, and Accounting (AAA) Manager
  - Usage collection
  - User security management
  - IP Security

#### **6.1.1.1 Network Element Management System (EMS)**

The HiPath 8000 uses the Network Element Management System (EMS) for configuration, provisioning, fault, performance, and maintenance management. The EMS consists of these components:

- SNMP and MIB-2 agents. The SNMP interface is based on SNMP v2.
- A UNIX Command Line Interface (CLI) that is available through a local console or SSH session.
- A graphical, SNMP tool called the Network Management Center (iNMC) to manage applications and services. Also, there are Java applets to manage the base RTP system.

You can manage the HiPath 8000 from a Windows system that hosts an iNMC client. For details on the iNMC, see [Section 6.5, “iNMC Overview”](#).

## **Element and Network Management**

### *Element and Network Management Overview*

#### **6.1.1.2 Configuration Management**

The HiPath 8000 configuration management function discovers network devices and provides trend analysis, thresholds, and data warehouse capabilities.

The HiPath 8000 uses the capabilities of the RTP to store configuration data in initialization files on the disk. These files can be read by applications at start up time or any time after the RTP indicates the data has changed.

#### **6.1.1.3 Fault Management**

The HiPath 8000 fault management function provides real-time monitoring and reporting on all alarms. In the HiPath 8000, the RTP Event Manager generates events and alarms.

Events are marked by a unique event ID containing information, for example the severity level, that details the event. Alarm objects reflect the current state of the cluster. A separate alarm manager process changes the states of the alarm objects when specific events occur.

The logging function writes events to a permanent database. To filter logging events, the RTP Event Manager is integrated into the network management system and events are forwarded to the central network management console.

Each node has an event handler process to gather and process events logged at different instances. The event handler executes the defined filter operations (escalations, event suppressions) and distributes the events to the event manager, the SNMP agent, and other related processes. Only one event manager process is active in the cluster.

In the event of a node failure, a backup manager process logs the events to the database and transfers them to the alarm manager and other interested processes. Based on the rules in the database, special events can trigger state changes in the alarm objects processed by the alarm manager.

Furthermore, the RTP provides a critical event handling mechanism. Special critical events use a second independent and secure event path. They are detected and handled in the library used by the application processes. These special, critical events are administered using the management function API. For all subsystems, special processes are provided for passing external events to the event handler transparently.

### **6.1.2 Managing the HiPath 8000**

The HiPath 8000 provides SNMP and CLI interfaces for element and network management. The SNMP interfaces are provided through SNMP agents running on the HiPath 8000. The GUI-based element management applications, with the SNMP agents, interface to the iNMC or to the HiPath 8000 Assistant.

The CLI has two modes: a menu-driven mode and expert mode. The menu-driven CLI is based on the Resilient Telco Platform (RTP) CLI menus. The expert mode CLI is command-driven and used for mass provisioning.

### **6.1.3 Software Upgrades**

During an update installation, any changes to the HiPath 8000 software or applications are incorporated online.

The HiPath 8000 software is upgraded through the RTP management functionality. Each node in the cluster is first stopped, the rolling upgrade is carried out locally, and then the node is restarted (rolling update).

The HiPath 8000 rolling upgrade facility offers a fast fallback option in the event of errors. The effectiveness of this fallback method depends on the hardware and database used (different mirroring techniques for shared disk and shared nothing databases). Before each rolling upgrade, a backup should be taken so that the system can be restored in an emergency. For more information on the Rolling Upgrade feature, refer to [Section 4.2.8.4](#).

### **6.1.4 Local and Remote Administration**

Local administration of the HiPath 8000 is through the iNMC server and CLI.

Remote administration of the HiPath 8000 can be performed through secure interfaces with the CLI. Subscriber Management can be performed remotely through web sessions with iSMC and iSSC.

## 6.2 Billing and Back Office Integration

### 6.2.1 Call Detail Records

The HiPath 8000 collects call information through the Usage Collection component. This data is formatted and accumulated into Call Detail Records (CDRs). In addition to records of call attempts, CDR files can contain long call audit records and change of time audit records. CDRs are useful for invoice creation, network monitoring, assurance of meeting service level agreements, and network planning.

You can use your own billing system to retrieve the CDRs. This can be done using these methods:

- The AMA Mediation Server (available as an optional product in the U.S.A.) or another external platform to translate the CDRs into standard Telcordia AMA format or other common billing formats.
- Your own billing server to retrieve the CDR files directly from the HiPath 8000. This allows you to perform complex billing mediation and CDR storage.
- FTP to transfer the CDR files manually from the HiPath 8000.

#### 6.2.1.1 Billing File Format

The billing (CDR) files are formatted with header and trailer information and can contain call and audit records. [Figure 6-1](#) shows the billing files format.

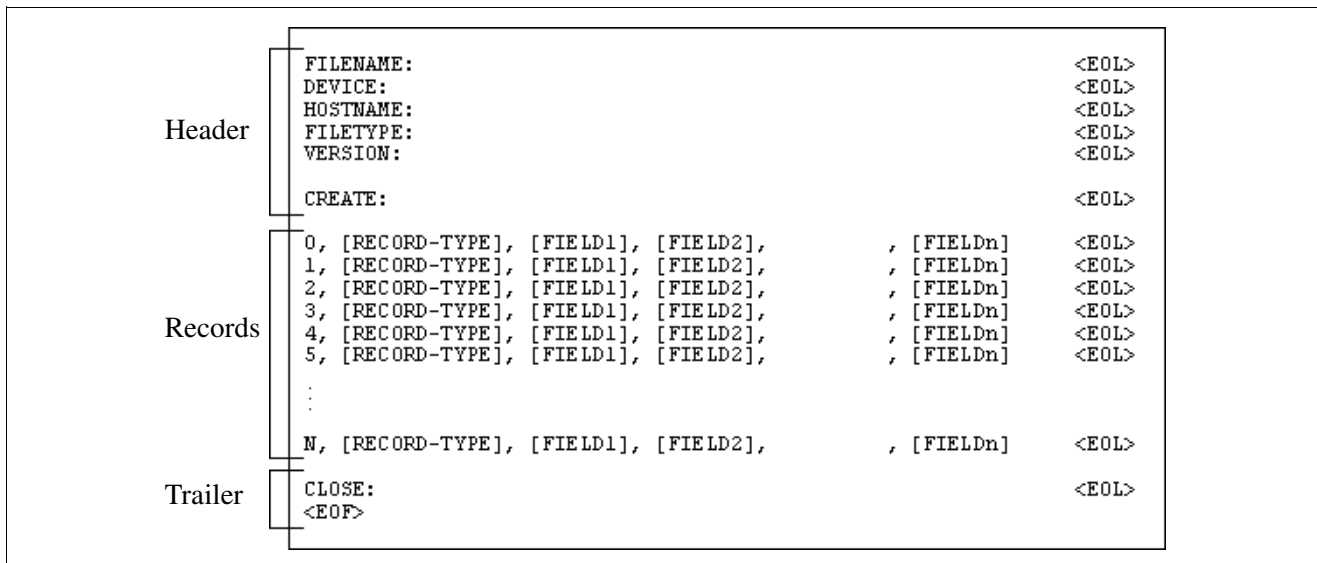


Figure 6-1 Billing Files Format



For details on billing files and the call and audit record fields, see the *HiPath 8000 CDR Reference Manual*.

### 6.3 Script Capabilities

External CLI scripts can be applied from standard and common scripting languages that generate output in the CLI syntax.

### 6.4 Security Features

#### 6.4.1 CLI

The RTP implements its own user management, that is, creation, modification and deletion of users, password handling, handling of privileges, and so on, and is completely managed by the management function API. RTP also controls the user access to the management functionality (user identification and authorization).

The CLI requires a user profile for all users who access the HiPath 8000. A user with administrator privileges creates the user profiles.

The components and privileges of a user profile depend on the platform. [Table 6-1](#) lists the user profile components.

User Name	A minimum length of 1 character. Maximum length of 36 characters.
Password	A minimum length of 8 characters. Maximum length of 36 characters.
Privilege	Determines the access a user is granted. The privileges are: <ul style="list-style-type: none"><li>• stdop — Read only access.</li><li>• maxcust — Read/write access. This is the maximum authorization level for clients.</li><li>• maxint — Read/write access. This is the maximum authorization level for RTP integrators.</li><li>• super — This is for Siemens internal use only.</li></ul>

Table 6-1 HiPath 8000 CLI User Profile Components

## 6.4.2 iNMC User Security and Management

The HiPath 8000 interfaces to the iNMC by means of SNMP and FTP. The HiPath 8000 supports SNMPv1, SNMPv2, and SNMPv3. SNMPv2 is used for the iNMC interface.

From the iNMC Main screen, you can access the user management feature. It allows you to manage iNMC security by creating iNMC users, each of which has the following properties and characteristics:

- A unique user name and password
- One or more assigned node groups, indicating the devices to which the user has management and/or viewing access
- One or more assigned access profiles, indicating the objects and iNMC tools to which the user has read/write, read only, or no access

### 6.4.2.1 Node Groups

Node groups define sets of devices to which iNMC users have viewing and/or management access. You assign node groups to access profiles to associate access to groups of devices. Then, you assign access profiles to iNMC users, thereby limiting the management and viewing access of these users to only the node groups included in their assigned access profiles.

### 6.4.2.2 Access Profiles

You can create access profiles to define the privileges, node groups, and inactivity timer for each iNMC user. If desired, you can assign the same access profile to multiple iNMC users. After you have created a series of access profiles, you assign these profiles to iNMC users. Each access profile consists of the following components:

- Node groups — You specify the devices to which a iNMC user has access by assigning one or more node groups to the access profile(s).
- Viewing and management privileges — When defining an access profile, you specify an access level for each management object and iNMC tool. Possible access levels are read/write, read only, and no access.
- Inactivity timer — For each access profile, you specify the inactivity timer for the users to whom you assign the profile. The inactivity timer prevents unauthorized access to the iNMC when an authorized user leaves an iNMC client unattended. If a client remains idle for the amount of time set as the inactivity timer, the user must log into the client again.

### 6.4.3 iSMC User Management

The HiPath 8000 interfaces with the iSMC by means of Simple Object Access Protocol (SOAP). Configuring the HiPath 8000 and the iSMC to transfer SOAP over IPsec provides security for this interface.

Every user who works with the iSMC is given a user name and password that is assigned by a user called SuperAdmin or by another user who has been assigned the role of User Management. In addition, the SuperAdmin assigns roles to users. Roles enable users to perform various iSMC functions.

An iSMC user can be assigned all roles or none. Users with no assigned roles can only login; they cannot perform any other functions.

#### 6.4.3.1 Users and Roles

Roles enable users to perform administrative or maintenance functions. These roles are assigned when a user is created and can be modified at any time. The roles cannot be created. The iSMC is installed with the following two users that enable you to begin using the iSMC immediately:

1. SuperAdmin
2. NormalAdmin

Table 6-2 below lists the roles for each of these users.

User Name	Roles	Purpose
SuperAdmin	User Management Administrator Business Groups Security Log Provisioning Log	Provides access to User Management and Administrator functions, as well as the Provisioning and Security logs.
NormalAdmin	Administrator Business Groups Provisioning Log	Provides access to Administrator function and Provisioning Log.

Table 6-2 iSMC Users

The passwords for these users are the same as the user name.

## Element and Network Management

### Security Features

Once the SuperAdmin creates users, he or she can assign the following roles to them.

Role	Description
User Management	Can add, modify, and delete iSMC user accounts.
Administrator	Can retrieve, create, modify, disconnect, and delete DNs (subscriber profiles). This user can also modify service-related parameters and add, modify, and delete business groups.
Services	Can modify service-related parameters, but cannot create, modify, disconnect, or delete DNs nor can they view non-service-related DN parameters.
Business Groups	Can add, modify, and delete Business Group accounts.
Security Log	Can view the iSMC security logs of all users in the User Management role. This log records all login attempts, session timeouts, logouts, and any associated messages.
Provisioning Log	Can view the iSMC Provisioning Log, which records actions taken by the iSMC Administrator and any associated messages.

Table 6-3 iSMC User Roles

### 6.4.4 iSSC Security

The iSSC is a toolkit providing screens and associated interfaces to the HiPath 8000 to support subscriber self-management. The iSSC toolkit allows the service provider/enterprise customer to integrate self-management of HiPath 8000 based subscriber features into their web portal. The customer's web portal provides the security features and the customer is responsible for the security of the web portal.

#### 6.4.4.1 Management Security

The responsibility for iSSC management interfaces is split between the Web Portal provided by the service provider and the iSSC toolkit provided by Siemens.

The Web Portal is responsible for:

- Secure customer interface for customer self management (HTTPS)
- Secure craft interface for platform and application management

The iSSC toolkit is responsible for securing the machine-to-machine interface between the iSSC and the HiPath 8000.

The interface between the iSSC and the HiPath 8000 is XML over SOAP. To protect the interface as well as to block unauthorized access to the iSSC interface at the HiPath 8000, IPSec is used to protect the interface.

## 6.4.5 Transport Layer Security (TLS) Services

TLS is an application-independent security protocol and can operate transparently to the protocols which run on top of TLS. TLS offers the following security services:

- Connection-oriented data confidentiality
- Connection-oriented data integrity
- Unilateral (for server-client) as well as mutual authentication of the TLS peers (server-server)

Besides confidentiality, integrity, and data origin authentication, TLS also provides key management. The TLS protocol works above the transport layer, thus intermediate firewalls cannot interpret the encrypted data. Because TLS is session-oriented protocol, the TLS key management establishes security sessions that define the security parameters applied for the protection of higher-level application data. For more information on TLS support, refer to [Section 4.2.4.3, “Session Initiation Protocol \(SIP\)”](#). For more information on SIP over TCP, refer to [Section 4.2.5.2, “SIP”](#).

## 6.4.6 HiPath 8000 Assistant Security

Cryptographic techniques and authorization together represent a lion’s share of IT-security mechanisms:

- Cryptographic techniques address scenarios where attackers have direct access to the raw bits that are representing information.
- Authorization addresses scenarios where access to raw bits has to pass through some layer of system functionality (called reference monitor in the following).

The security architecture for HiPath 8000 Assistant provides security services based on cryptographic techniques as well as authorization services.

Among the security services based on cryptographic techniques, the service of authentication represents the nucleus. Authentication is the process of establishing confidence in the truth of claims such as *“I am John Doe”*, *“This information is from me”*. It is the most fundamental cryptographic security service since it addresses the most fundamental security issue in IT (informally: *“how to distinguish right bits from wrong bits”*) and is a prerequisite for other security services in distributed IT-environments.

## 6.5 iNMC Overview

The iNMC is a graphical, tree-oriented network management interface to configure and manage the switches. The iNMC components include a iNMC server, iNMC client(s), and Alarm Server. For the HiPath 8000, there are Java applets to manage the base Resilient Telco Platform (RTP) system.

The iNMC server and client software run on Windows and Solaris systems. Figure 6-2 shows the iNMC structure.

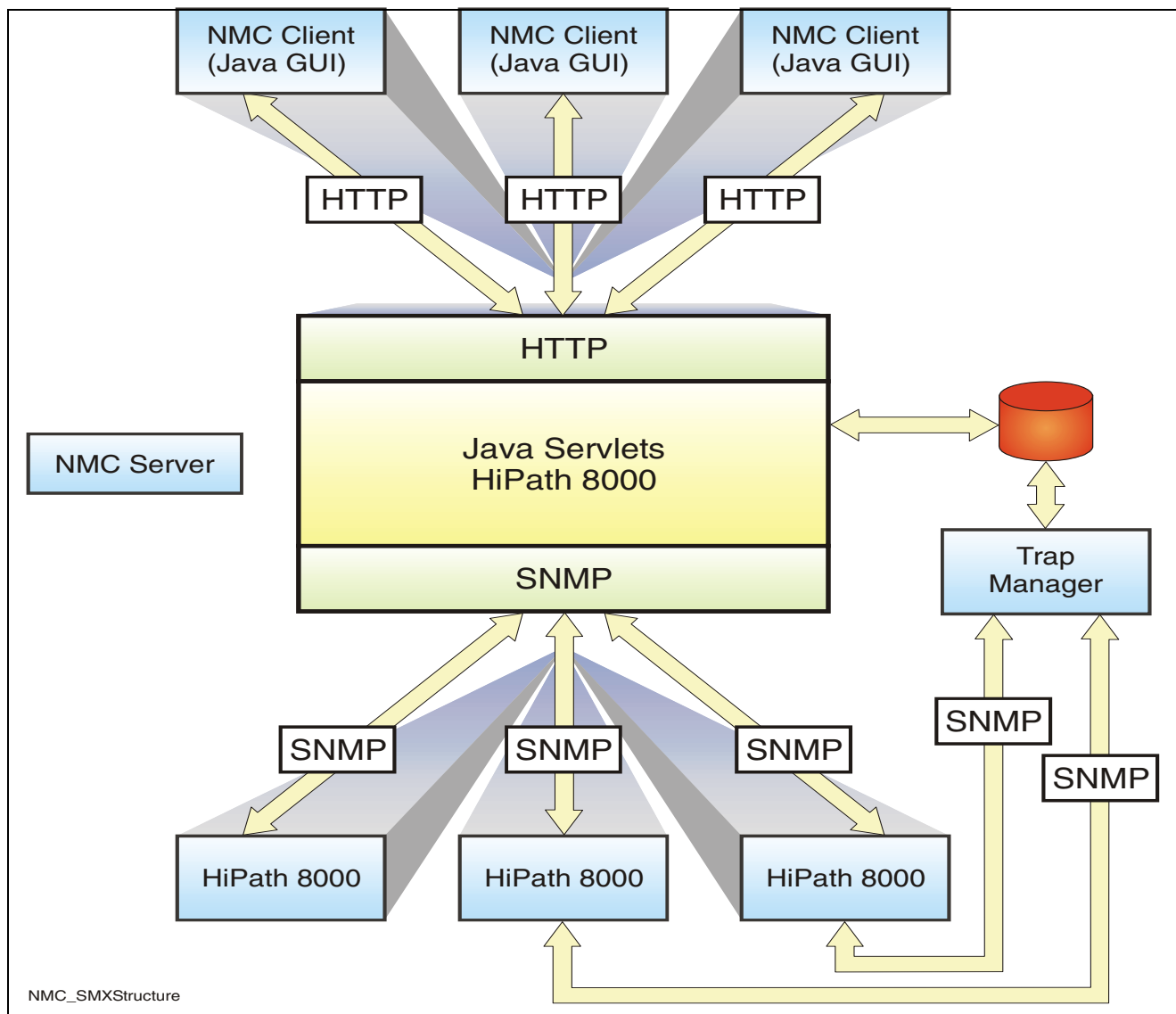


Figure 6-2 iNMC EMS Structure

### 6.5.1 iNMC Main Screen

The iNMC Main screen is a split window. At the top of the screen is a menu bar containing several menus for device configuration and maintenance. A navigation tree comprised of devices, objects, groups, and collections is displayed on the left side of the window.

When you select an element in the navigation tree, one or more tabs appear on the right side of the window. Each tab contains information for the selected element. In addition, when an element contains multiple objects (such as the Link Sets collection), the iNMC displays a Name list column between the navigation tree and the tab display. In this Name list, you select the specific object to view and/or modify.

The Help menu provides access to the iNMC Help system, as well as information about the iNMC software version and how to contact Siemens Support Personnel. A status bar at the bottom of the iNMC Main screen displays the iNMC server to which your client is connected and a polling icon that indicates when the iNMC polls a specified managed device.

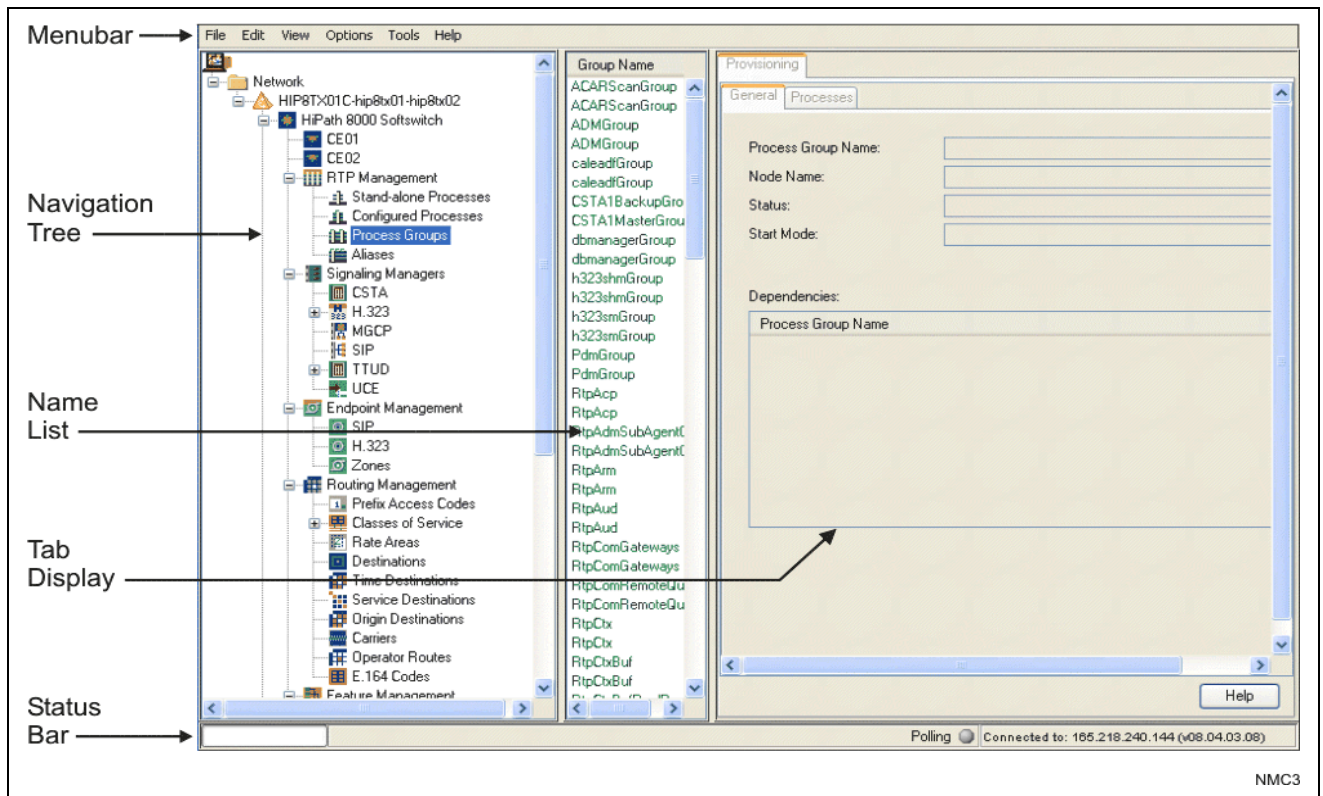


Figure 6-3 iNMC Main Screen Components

## 6.5.2 iNMC Clients Per iNMC Server

The number of user profiles you can add to the iNMC database is unlimited. However, it is recommended that you maintain no more than the following number of open iNMC client windows attached to a single iNMC server:

- Window Server — 100 maximum
- Windows Workstation — 40 maximum

## 6.6 HiPath 8000 Assistant

The HiPath 8000 Assistant is a Web-enabled Telecommunications Service Management Center. It provides instructions on creating, modifying, and deleting HiPath 8000 Assistant user accounts; creating, modifying and deleting Business Groups; creating, modifying and deleting subscribers; subscribing to and activating services, modifying services; and unsubscribing from services. It also enables you to create and manage EndPoint Profiles and to add, modify, and remove intercepts.

### 6.6.1 HiPath 8000 Assistant Home Page

The screenshot displays the HiPath 8000 Assistant web interface. At the top, there is a navigation bar with 'Open', 'Tools', 'Tasks', 'Settings', and 'Help'. Below this is a secondary navigation bar with 'Home', 'Administration', 'Global Numbering Plan', 'Business Group', and 'Reporting'. The user is logged in as 'administrator@system (System Administrator)' with a 'Log out' link. The main content area is divided into three sections:

- Current Alarms:** A section with an 'Actions' dropdown and a play button. Below it is a table with columns for Device, Critical, Major, Minor, and Total. The table shows data for Framework, HiPath 8000, Media Server, and RG8700. A 'View All Alarms' button is located below the table.
- System Load:** A section with a warning icon and text: 'If the load exceeds 70%, a sanity check is necessary.' Below this are progress bars for CPU 0 and CPU 1, each with two sub-bars (A and B) and a percentage value.
- Software Level:** A table with columns for Device, Latest Patch Set, Assistant, and Siemens\_Shared\_Services. The data shows: 8000 (10.01.01.ALL.22), Latest Patch Set (PS0004.E01), Assistant (2.0-0145), and Siemens\_Shared\_Services (1.0.0-1).

At the bottom of the page, there is a copyright notice: 'Copyright (C) Siemens 2005 Corporate Information | Privacy Policy'.

Figure 6-4 HiPath 8000 Assistant Home Page



## 6.6.2 HiPath 8000 Assistant Navigation Area

The **Navigation Area** and the **Content Area** are located directly beneath the **Navigation Bar**, adjacent to each other, and occupy the main part of the screen.

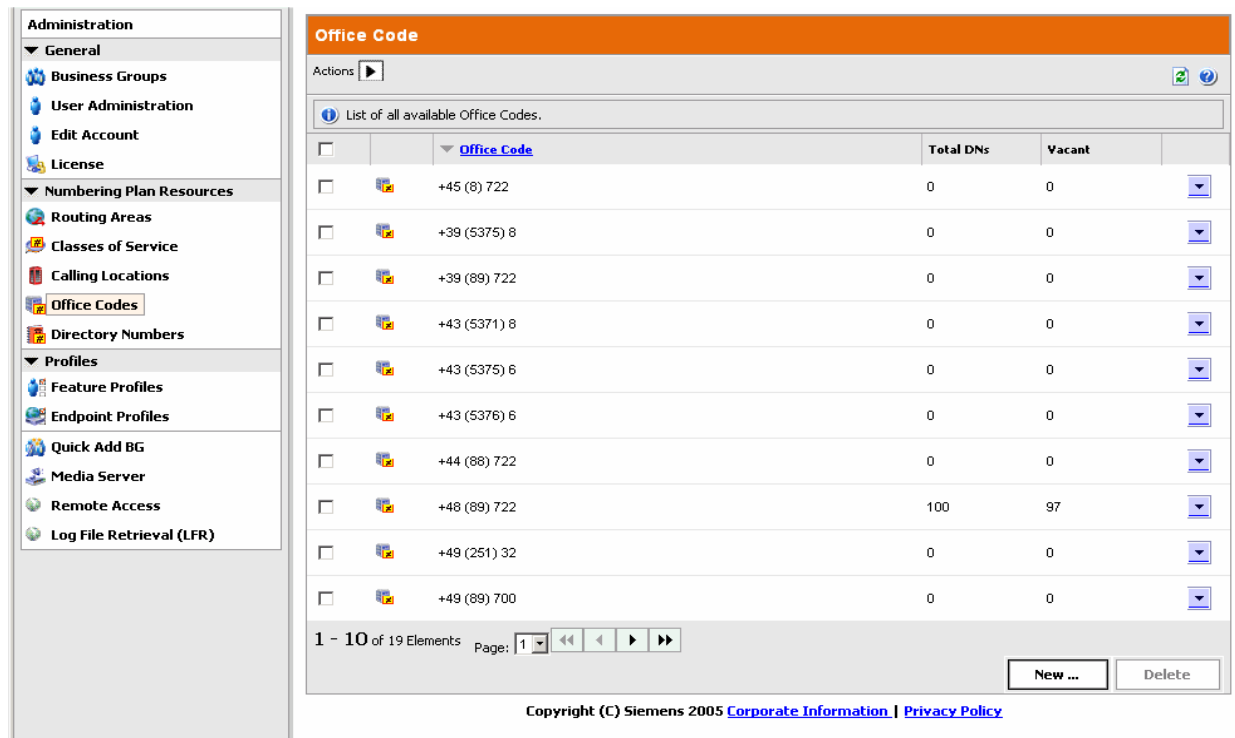


Figure 6-5 HiPath 8000 Assistant Navigation Area

### 6.6.3 Menu Structure of the HiPath 8000 Assistant

<b>Menu Item</b>	<b>Submenu Item</b>
<b>Open</b>	
	Dashboard View
	System Management View
	License Information
	HiPath 8000 Command Line Interface
<b>Tools</b>	
	Export Configuration Data
	Export Administration Data
<b>Tools</b>	Export Private Numbering Plan
	Backup Archives
	Create Backup
	Backup Schedule
	Backup Settings
<b>Tasks</b>	
	Quick Add Business Group
	Quick Add PSTN Gateway
	Quick Add PABX Gateway
	Change Password
<b>Settings</b>	
	Alarm Destinations
	Configuration Files
	Media Server Configuration
<b>Help</b>	

Figure 6-6 HiPath 8000 Assistant Menu Structure

## **6.7 Provisioning**

### **6.7.1 HiPath 8000**

#### **6.7.1.1 Mass Provisioning**

Prior to starting call processing, and after system installation, the mass provisioning function remotely populates and configures the HiPath 8000 databases to provision large numbers of subscribers without using the CLI menu. Mass provisioning is remotely performed using the expert mode CLI commands through FTP, then executing the file's commands on the HiPath 8000. This capability includes the provisioning of HiPath 8000 and iSMC entities. PlaNet8000 is used as a Database Generation Tool.

#### **6.7.1.2 Private Numbering Plan**

The private numbering plan is a customized plan for the business group customers. A business group is assigned with a private numbering plan and all subscribers belonging to that business group are governed by the private plan.

The routing and dialing pattern of the private numbering plan apply to all subscribers within the same business group. Therefore, all subscribers within the business group is capable of dialing off net. Subscribers can make long distance US calls by dialing 9 + 1 +10 digit DN. Subscribers can make international calls by dialing the 9+011+Country Code + DN. In order to restrict one or some subscribers from calling long distance or international calls, assign the Toll Restriction (TRS) or Station Restriction (SR) service to the subscribers.

The private numbering plans are created through iSMC, the valid Id range is 2 to 999. A private number plan cannot be shared among different business groups.

#### **6.7.1.3 Rolling Upgrades**

The rolling upgrades feature performs software upgrades without affecting service. You can run rolling upgrades of HiPath 8000 applications in a cluster as long as the new software is compatible with the old software. In this case, one node is stopped and upgraded with new software. The node is brought back up, and the other node is stopped, upgraded, and brought back up.

**Element and Network Management**  
*Provisioning*

## 7 Main and Extended Interface Components

In addition to the HiPath 8000 Hardware, Software and Element Management System described in previous chapters, this chapter describes the Main and Extended Interface Components for the HiPath 8000. These include:

### VoIP Border Controller Systems

- Juniper Networks®

### Firewalls

- Cisco PIX 535

### Media Servers

- Integrated Media Server
- IP Unity Mereon 6000 Media Server
- Convedia CMS 1000

### Applications

- HiPath ComAssistant S
- OpenScape
- Xpressions VM

### Endpoints

- optiPoint 410 S/420 S standard SIP
- optiClient 130 S
- SIRA

### Gateways

- RG 8700 V1.1 Survivable Media Gateway
- HiPath 4000 HG 3540 SIP-Q Gateway
- Cisco SIP Gateway
- Survivable Branch Offices
- RG 2700 Survivable Gateway

## Main and Extended Interface Components

### VoIP Session Border Controller

#### 7.1 VoIP Session Border Controller

VoIP Session Border Controller provides security and control for calls originating from the Internet. The HiPath 8000 Release 2.0 is supported by Juniper Networks® (Figure 7-1). The VF 1000 provides the ability to scale up to 1000 concurrent calls.

All VoiceFlow systems support all of the popular VoIP protocols and are compatible with standard and popular VoIP endpoint and network equipment. The VoiceFlow series of products are derived from a common technology platform and thus, all support the following functionality:

- Security—VoIP Firewall, Network Address Translation (NAT), Firewall Traversal, Call Admission Control, Network Asset Protection
- Service Assurance—QoS monitoring and routing, Packet Marking, Call Gapping, Bandwidth Management, Multiple Protocol Support (SIP,SIP-Q, MGCP), Network and VoIP Endpoint Transparency
- Management—Remote Monitoring, VoIP Endpoint Configuration & Management, SLA Reporting

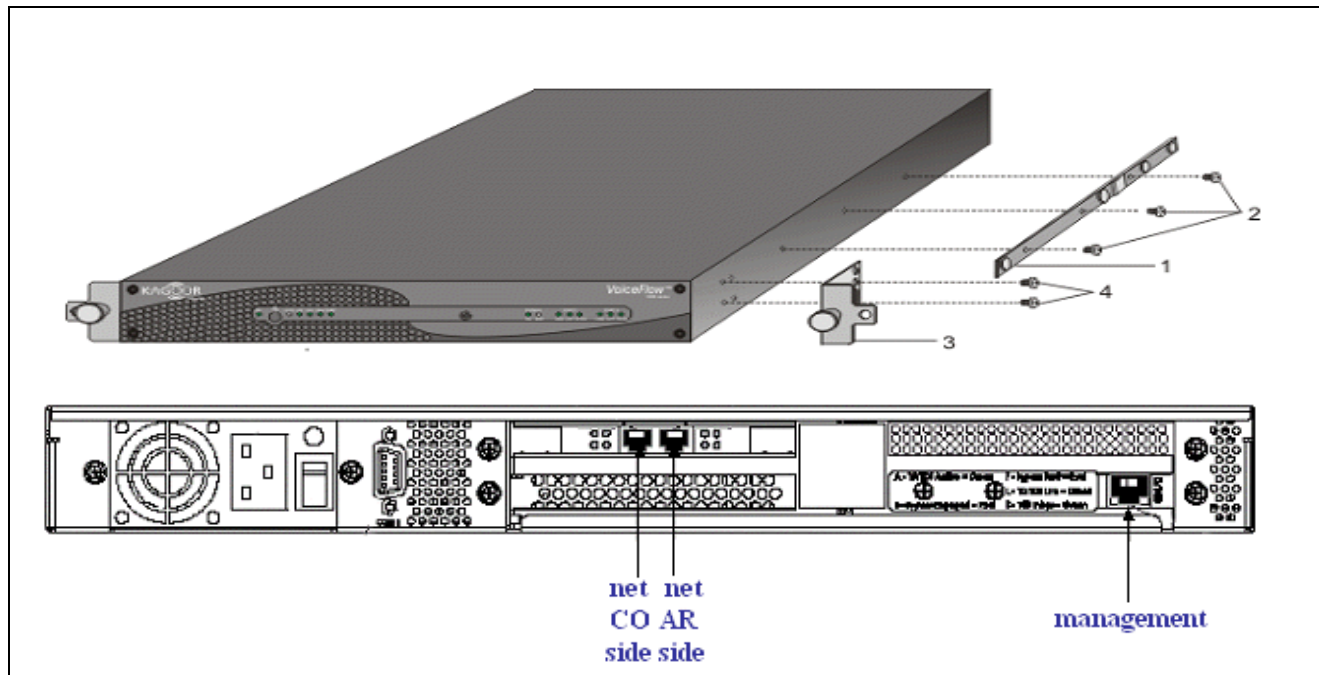


Figure 7-1 Juniper VF1000 Front and Back View

## 7.2 Firewalls

Various Firewall products are used to provide security to the system. The most common is the Cisco PIX 535 Security Appliance (Figure 7-2). It delivers security for service provider networks, in a high performance, purpose-built appliance.

The Cisco PIX 535 modular three-rack-unit design supports up to ten 10/100 Fast Ethernet interfaces or nine Gigabit Ethernet interfaces and redundant power supplies, making it an ideal appliance for businesses that need the highest levels of performance, port density, reliability, and investment protection. It also delivers up to 1.7 Gbps of firewall throughput with the capability to handle more than 500,000 simultaneous sessions

The PIX 535 “Unrestricted” (PIX 535-UR) model, extends the capabilities of the family with support for stateful failover, additional LAN interfaces, and increased VPN throughput by means of integrated hardware-based VPN acceleration. It includes an integrated VAC or VAC+ hardware VPN accelerator, 1 GB of RAM, and support for up to ten 10/100 Fast Ethernet or nine Gigabit Ethernet interfaces. The Cisco PIX 535-UR also adds the ability to share state information with a hot-standby Cisco PIX Security Appliance for resilient network protection.

The Cisco PIX 535 “Failover” (PIX 535-FO) model is designed for use in conjunction with a PIX 535-UR, to provide a high-availability solution. Using the same hardware as the PIX 535-UR, it operates in hot-standby mode acting as a complete redundant system that maintains current session state information.



Figure 7-2 Cisco PIX 535 Firewall

# Main and Extended Interface Components

## Media Servers

### 7.3 Media Servers

#### 7.3.1 Integrated Media Server

The integrated Media Server provides the compact HiPath 8000 system with tones and announcements and is for small to medium-size enterprises supporting 300-5000 subscribers.

This software-only server solution is fully integrated into the system server hardware.

The integrated Media Server supports redundancy and can be managed by the integrated HiPath 8000 Assistant V2.0 or by an iNMC/iSMC administration server.

The Media Server consists of the following basic, logical components:

- MCP Service
- Media Processing Service
- Announcement Creator Service
- Announcement Management Service

The following figure illustrates these components and their interfaces schematically.

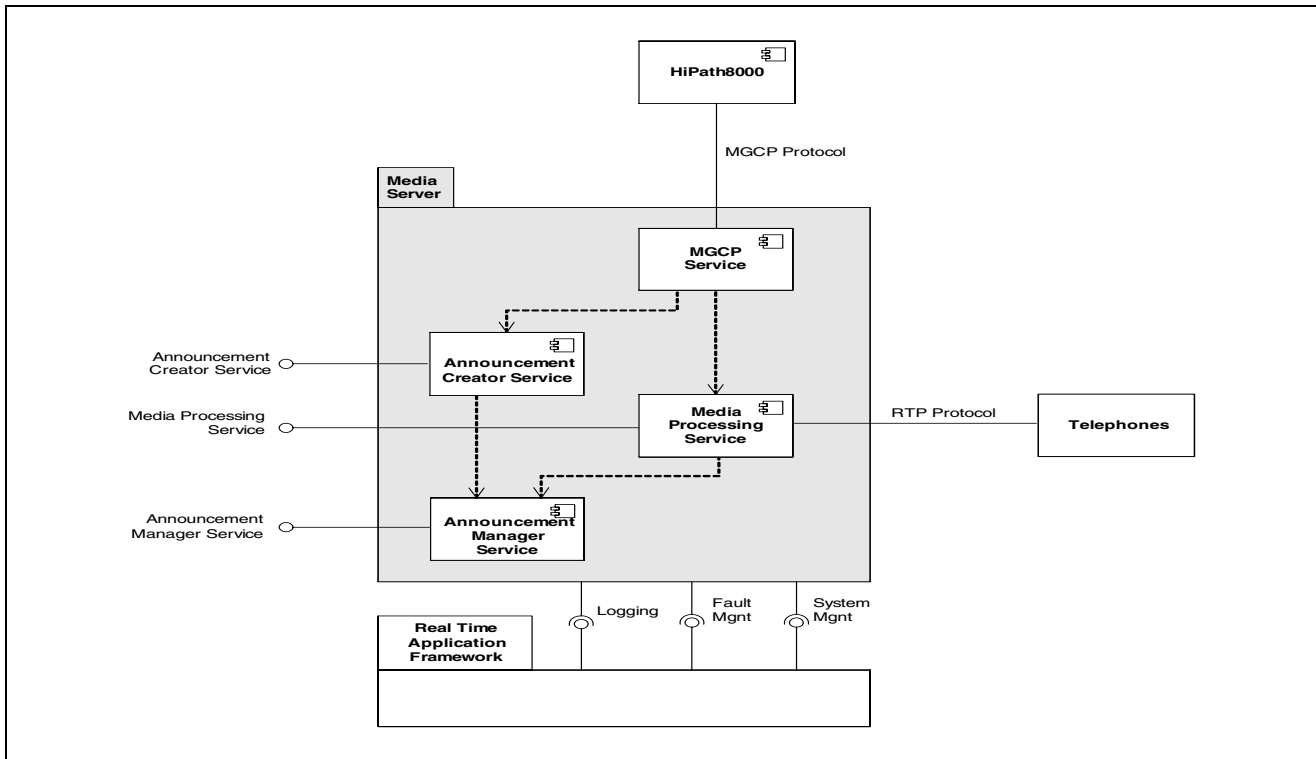


Figure 7-3 Compact HiPath 8000 Assistant Media Server



The Media Server is based on the Real Time Application Framework. This platform provides the Media Server with different basic structures of which logging, error- and system-management are currently used via the corresponding interfaces. For example, the HiPath 8000 Assistant accesses the settings of the Media Server component via the system management interface.

The following interfaces are also available.

- **MGCP Protocol**  
Enables the communication of the MGCP service via the MGCP protocol. A HiPath 8000 can send MGCP commands to the Media Server and receive replies to these commands via this interface. This communication is interpreted by the Media Server in its function as Media Gateway. For more information please refer to the *HiPath 8000 Assistant Service Manual*.
- **RTP Protocol**  
Enables the communication of the Media Processing Service via the RTP protocol. The actual media and DTMF streams, sent and received by the Media Server, are routed via this connection. For more information please refer to the *HiPath 8000 Assistant Service Manual*.
- **Announcement Manager Service**  
is an interface to the Announcement Manager Service. Media Server announcement administration is accessed via this interface. For more information please refer to the *HiPath 8000 Assistant Service Manual*.
- **Media Processing Service**  
is an interface to the Media Processing service of the Media Server. This interface manages the real-time transmission of different data formats. For more information please refer to the *HiPath 8000 Assistant Service Manual*.
- **Announcement Creator Service**  
is an interface to the Announcement Creator service. The dynamic generation of announcements is controlled via this interface. For more information please refer to the *HiPath 8000 Assistant Service Manual*.

### 7.3.2 IP Unity Mereon 6000 Media Server

The IP Unity product consists of three components: a Mereon 6000 media server, one or more application servers, and network-attached storage (NAS). Note, one HiPath 8000 can support multiple Media Servers.

The Mereon 6000 media server (see [Figure 7-4](#)) is the terminating point of RTP streams from subscribers. It contains the codecs that perform mixing, audio record and playback. It is a stateless device in that it allocates media channels when commanded to by the softswitch or by the application server, but does not attempt to maintain call state.

## Main and Extended Interface Components

### *Media Servers*

The application server offers voicemail or conferencing.

The network-attached storage (NAS) is an NFS-mounted device that serves as a holding area for pre-recorded messages.

The flexibility of this product allows it to take many forms. The Mereon 6000 is a dedicated chassis whose capacity is dictated by the number of media cards inserted. The applications servers and NAS can easily be located on a single Solaris platform, or they could also be distributed across separate Solaris platforms and disk arrays. The choice should be based on specific customer configurations.

#### **7.3.2.1 IP Unity Mereon 6000 Media Server Hardware**

The IP Unity Mereon 6000 Media server hardware provides:

- Standard Rack Mount
- 10-slot Card Cage
- Two types of boards:
  - Media Processor Card (MPC) that contains digital signal processing (DSPs) for media channel reservation
  - Shelf Controller Card (SCC) that support eight Ethernet ports
- SCC and MPCs interconnected by backplane ATM switch fabric
- Two Center Slots (4&5) host the Shelf Controller Cards (SCCs), one active and one standby

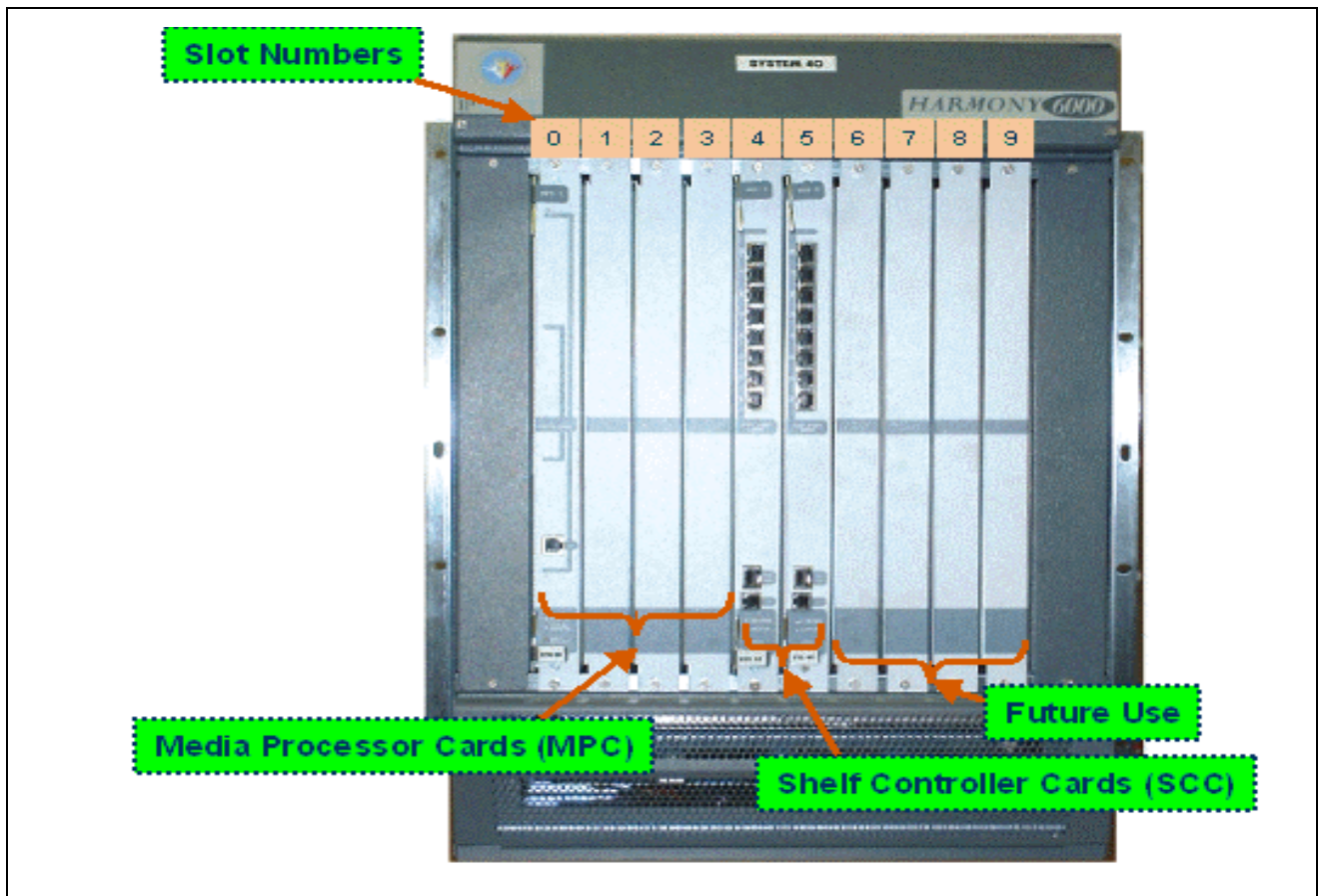


Figure 7-4 IP Unity Mereo 6000 Chassis

The Media Server hardware design is based on packet/cell switching and processing technology similar to that found in today's leading Ethernet switch and router products. This fundamental design compatible with other IP transport devices, plus the ability to interoperate with T1/E1 networks through an adjunct chassis, ensures that the Media Server can coexist in a variety of complex IP network and blended network configurations supporting various physical media, topologies, and protocols.

The Media Server deploys several specialized processors such as DSPs for audio signal processing, vector processors for speech engines, and general-purpose processors to handle the various signaling protocols required to establish calls and respond to application requests. Each of these specialized computers is integrated within a single platform and can be "mixed and matched" to meet the specific feature requirements of the service provider.

One unique specialized computing device in particular, known as a Network Processor, provides superior benefits to the media server. The NP is responsible for strictly controlling the type of packets entering and leaving the media server. Because of their specialization, NPs inspect packet flows at extremely high speeds making routing decisions, providing security

## Main and Extended Interface Components

### *Media Servers*

from network DoS attacks, and prioritizing traffic to prevent degradation of subscriber audio and video due to delay or loss. The Media Server is unique from many other media servers on the market because it dedicates an NP to each of its bearer and signaling interfaces.

The Media Server is physically packaged in a single chassis containing field replaceable, hot-swappable hardware and upgradeable software. It is both NEBS and NEDS level 3 certified. Both hardware and software create a high availability combination through redundant component support, extensive runtime audits of system health, and recovery actions.

Another key feature of the Media Server is that it was designed to accommodate the use of both internal and external resources, making them transparently available to each subscriber. For example, audio (such as for conferencing) is recorded on external network attached storage devices, which is far more reliable and manageable than local disk drives. Announcement audio can be fetched from a web server using a URI. Speech recognition and text-to-speech engines can be located within the platform, or just as easily on external servers as the system control and data paths have all been designed to be flexible.

#### **7.3.2.2 IP Unity Applications**

The IP Unity Mereon 6000 Media server is the network element providing:

- Tone and Announcements
- Conferencing Service
- Music on hold
- Interactive Voice Response – for auto attendant
- Three and six way station conferencing
- Transcoding between codecs

In order for the HiPath 8000 and the IP Unity Mereon 6000 to interoperate correctly, announcements provided by Siemens must be placed on the network-attached storage.

In most configurations, the IP Unity media server also includes an application server that provides voicemail services and conferencing services. This same application server usually holds the tones and announcements that are needed by the media server. On the application server, a file directory is NFS-mounted so that it can be treated as a local file system by the Mereon 6000 operating system.

The support of IP Unity MS/AS V3.1 provides POVM TUI services to the HiPath 8000. The IP Unity Application Server (AS) is a software platform on which IP Unity applications run, e.g. Unified Messaging (UM) which includes the Plain Old Voice Mail (POVM) component.

IP Unity Plain Old Voice Mail (POVM) is the component of the Unified Messaging (UM) application that is currently used for VoIP@Home solutions. The POVM extension product verification environment include (1) Voice Mail accessibility from any phone (on-net or off-net) with all standard TUI menu options and sub-options, and (2) initialization, configuration and management of the POVM application component via the UM configuration interface.

Intercepts are branches in the normal progress of a call processing. Calls that cannot be routed or that need more input on the part of the caller are diverted, in many cases, to a media server where a recording can be played back to the caller.

On the HiPath 8000 there are many pre-defined intercepts that are integrated into the call processing code. When an intercept condition is encountered, the HiPath 8000 usually relies on an outside element to provide a treatment for the intercept. Treatments are a collection of tones and/or announcements, and can be defined for each intercept. When a number is delivered to the HiPath 8000 that it cannot route, the HiPath relies on the media server to playback the appropriate wave file. The call is then torn down by the HiPath 8000.

### 7.3.3 Convedia CMS 1000

The Convedia CMS 1000 provides tones and announcements and supports the functionality of many HiPath 8000 features. (Currently, the Convedia Application Server is not supported).

Convedia's media servers provide media processing engines for basic and advanced network services in fixed, wireless and enterprise networks based on packet voice technologies.

Convedia offers an SNMP v2c compliant interface provides iNMC access.

The CMS-1000 is a 1 RU, 19" rack mountable, self contained media server. A system comes with 100 G.711 RTU licenses. Additional G.711 RTU licenses, to a maximum of 300 G.711 ports can be added to this system. The system is upgraded solely through the addition of RTU licenses; no additional hardware is required to move from 100 ports to the maximum capacity of 300 G.711 ports. Multiple CMS-1000's may be deployed in a network if more than 300 G.711 ports are required.

Convedia's media servers support two sources of provisioned announcements - internal and external storage. Internally, the Media Server supports a maximum of 50,000 provisioned announcements. When announcements are stored externally, there is no limit on the number of supported announcements. For external NFS, each MPC card will support up to 8 different external NFS servers. For External HTTP, each MPC card will support an unlimited number of HTTP servers.

# Main and Extended Interface Components

## Applications

### 7.4 Applications

#### 7.4.1 ComAssistant S (TM)

ComAssistant S (TM) 8000 (Figure 7-5) is a Web-based application that delivers powerful desktop call control as well as filtering and routing of incoming communication - voice calls, e-mails and voicemails - based upon presence and rules.

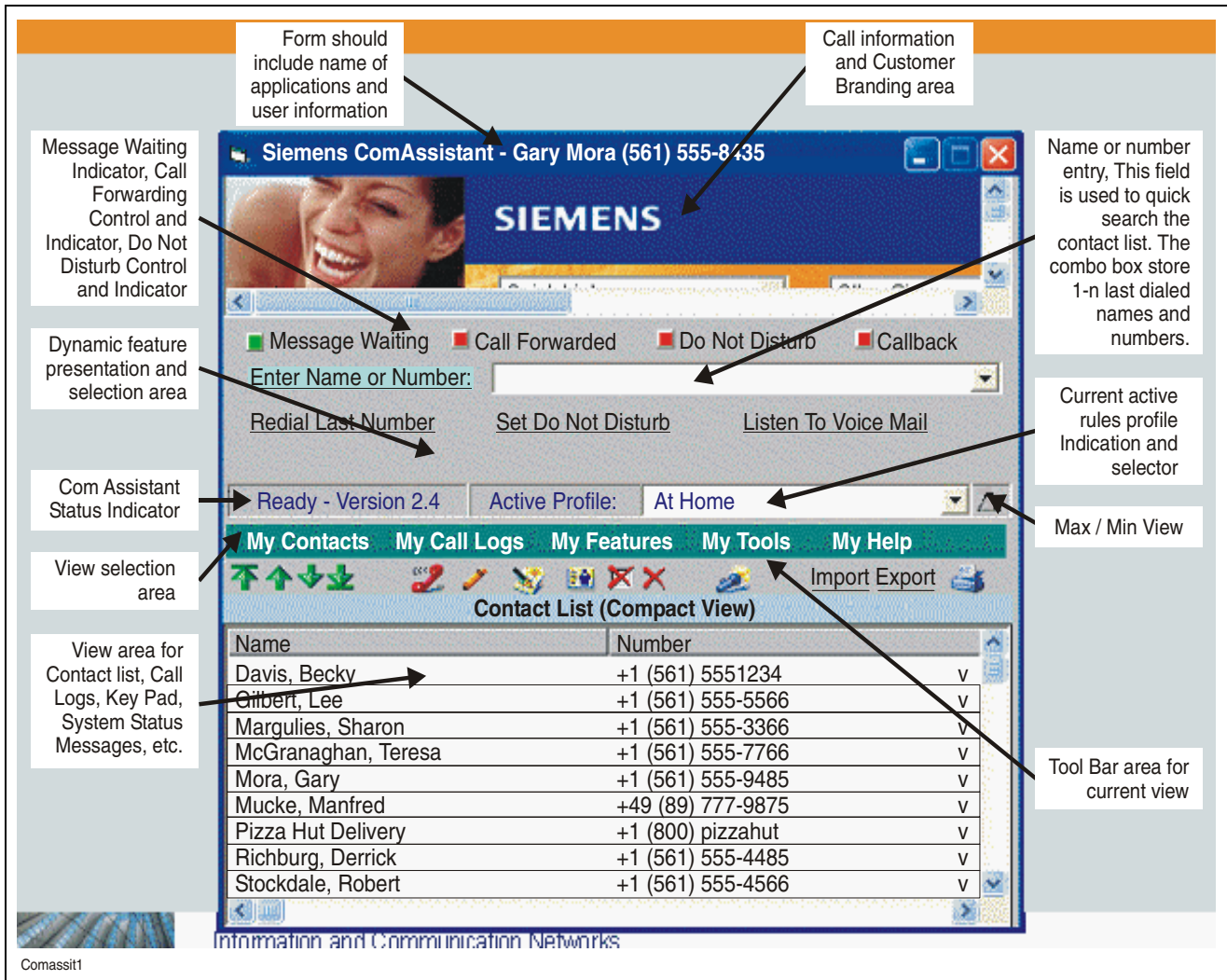


Figure 7-5 ComAssistant

HiPath ComAssistant filters incoming communication, be it voice or e-mail, for user efficiency. Comprehensive, browser based features, such as click-to-dial, call statement generation, LDAP address book search and one number service for office and mobile communications, optimize workflow processes. It also provides features such as multiple time zones, message waiting indicators and MGCP feature support.

The following are the highlights of this feature:

- Attendant Class Mark - added in Administration to denote member of attendant group
- Queuing UCD, prioritization - allows for calls to be presented in logical order to attendant groups
- Auto call Selection - allows the attendant to be presented with calls based on administration generated rules
- Auto call presentation reason - type of call presented
- Post call timing - administration selected timer for presentation of next call
- Additional CDR data - calls per queue, etc.
- CSTA enhancements - routing devices, queued, snapshot, logical device capabilities
- Attendant status - available, unavailable, etc.

## **7.4.2 OpenScope**

In partnership with Microsoft, Siemens provides an integrated communication solution that addresses the issue of information overload—too much information and too many communication devices. Siemens HiPath OpenScope provides a new level of communication intelligence by offering a unified user experience where systems and devices interact with one another.

HiPath OpenScope is an open, presence-aware, real-time communications software suite designed to quickly and easily synchronize people and information to facilitate action or decision-making. HiPath OpenScope helps enterprise customers take control of the escalating costs of business transactions by eliminating unproductive steps in the communications process and enhancing the conferencing and collaboration capabilities of the information worker community.

## **7.4.3 Xpressions VM**

Xpressions VM is Siemens' Enterprise Networks preferred Unified Messaging. Xpressions VM is currently being used by enterprise install based customers; and today Xpressions is connected to the Siemens Legacy and convergence platforms as the Enterprise messaging solution. The Integration of Xpressions to the HiPath 8000 provides a logical migration path from legacy and convergence platforms to the 8000 platform.

With the introduction of Xpressions V5.0, new security features including signaling encryption and payload security provide the Xpression users with more protection.



## Main and Extended Interface Components

### Endpoints

## 7.5 Endpoints

### 7.5.1 optiPoint 410 S/420 S and WL2 S Standard SIP

optiPoint 410 S/420 S standard SIP uses the SIP for connections to VoIP communication systems. You can use the IP phone in the same way as you would use a normal telephone - the only difference being that you're making it through a data network. The optiPoint 410 S/420 S standard SIP is equipped with a 10/100 Mbit/s mini switch (on some models). The PC workstation can be directly connected to the LAN through the mini switch - and you have only one wire to the desktop.

The optiPoint 410 S/420 S family of SIP phones offers a wide range of features. With up to 18 LED function keys, a tilting, two line LCD display, hands-free function and interactive user guide through optiGuide, phoning is simply more convenient. Features updates are carried out simply with software downloads.

SIP V6.0 enables software distribution and configuration of the phones to be done via DLS (Deployment Service) tool. Plug and Play of the phones via DLS User Mobility enables a user designated as a visiting user to log onto a mobility-enabled phone and have the phone automatically configured with all the attributes of the visitor's phone.

### 7.5.2 optiClient 130 S

The optiClient 130 S is a software client that mirrors the functions of the optiPoint telephone. Voice-over-IP utilizing the SIP standard has been enhanced to provide customers with all current IP features directly on the PC as a software solution.

A variety of media, such as data, e-mail and internet are pulled together on one interface. During calls, it is possible to input data into application programs, or to access data from the PC. Teamwork is likewise simplified, as the drag & drop function enables you to set up conferences involving several participants, simply and intuitively. 3-way video conferencing provides another presentation option.

optiClient 130 S administers, among other things, the personal address book and performs functions such as Application Sharing, allowing users to communicate in parallel over the LAN and jointly view or process documents. Via the client, users also operate important voice features such as call deflection, forwarding, toggling, call hold/resume, and DTMF suffix dialing.

For HiPath 8000V2.2, Remote User Capabilities provides user of a HiPath 8000 communication system the ability to use their phone other than in their office where they would typically use their soft client, OptiClient. In this environment, the user will be reached when a caller calls the published office phone number.



## **7.6 Gateways**

### **7.6.1 RG 8700 Survivable Media Gateways**

The Siemens RG 8700 Survivable Media Gateways provide scalable and standards-based gateway platforms that mediate TDM traffic (in circuit-switched, fixed, or mobile switching networks) to the packet world with carrier-grade reliability. The initial RG 8700 Version 1.1 is an RG 8716 with 16 T1/E1 circuits (Note, future RG 8700 versions introduce RG 8708 and RG 8702 with 8 and 2 circuits respectively) offers seamless normal and survivability modes with continuous 911 access; automatically invokes survivability mode when host connection is lost and continues to maintain active calls and 911 services while handling the switching of new calls.

As a key component of the HiPath 8000 family of next generation networking solutions and applications for the enterprise environment, the RG 8700's use the same administration tools as the HiPath 8000, thus making administration easier and more cost effective. In addition, this combination of compatible software creates a comprehensive VOIP network with connectivity to legacy equipment and under the support of one vendor.

The RG 8700 V1.1 has a separate set of documentation that included:

- RG 8700 System Installation Guide
- RG 8700 Troubleshooting Guide
- RG 8700 Provisioning Design Worksheets
- RG 8700 Configuration with CLI Guide
- RG 8700 Config and Admin using NetManager iNMC
- RG 8700 NetManager iNMC Server Install, Admin, and Utilities Guide

## Main and Extended Interface Components

### Gateways

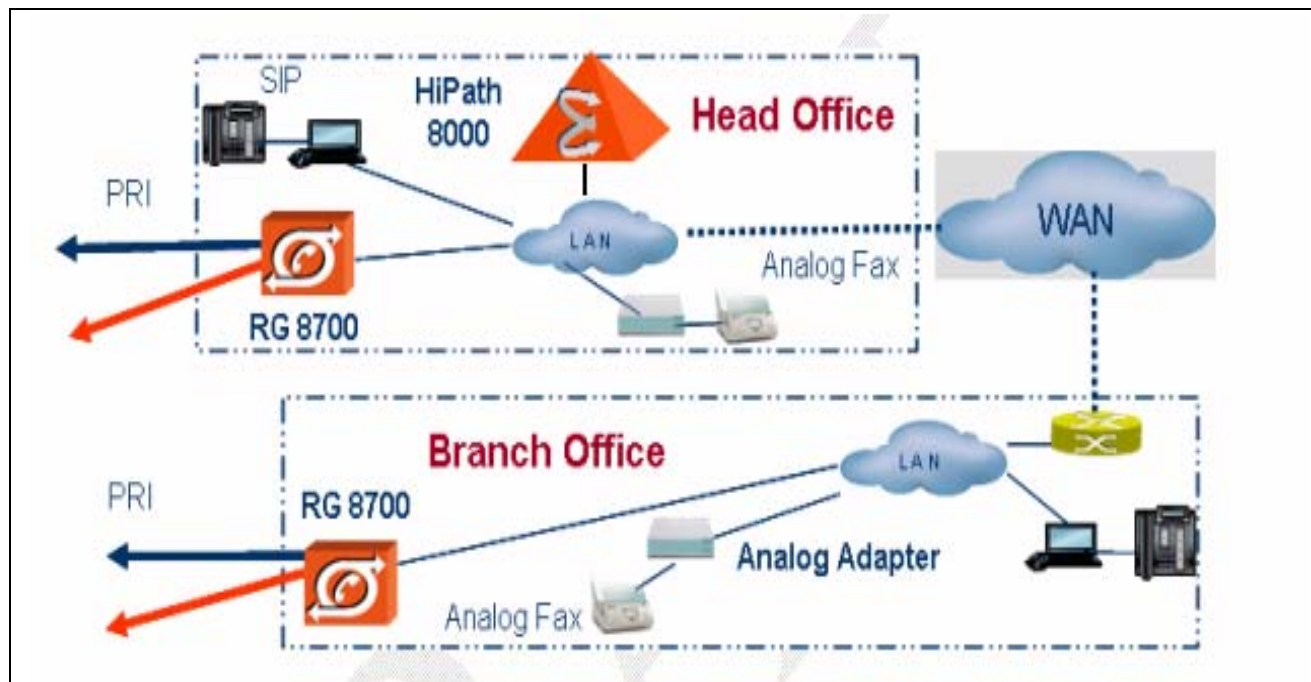


Figure 7-6 RG 8700 Deployment in Head and Branch Office Environments

#### 7.6.1.1 Steps to Assign an RG 8700 on the HiPath 8000

Use the following steps to assign an RG 8700 on the HiPath 8000:

1. Create an End Point Profile on the iSMC using New EP Profile tab with specific RG 8700 name for End Point Name.
2. Create SIP Endpoint on iNMC using Endpoint Management -->SIP-->General:
  - Endpoint Name must be unique and appears only in NMC
  - Make sure Registered is checked
  - The Fully Qualified Domain Name must also be assigned in the DNS server.
  - the Endpoint/Subscriber Profile: should be the End Point Name created on the iSMC
  - Click Aliases Tab and add IP address under Name
3. Create Destination in NMC using Routing Management -->Destinations-->General:
  - Assign Destination Name and Numbering Plan Name
  - Use Add Route button using SIP Endpoint Name as the Route Name

4. If necessary, create Numbering Plan, Prefix Access Codes, Destination Codes and Location Code in iSMC
5. Create objects for routing in RG 8700 (See Section 10 of the RG 8700 Configuration with CLI Guide).

### 7.6.2 HiPath HG 3540 Serves as a SIP Gateway

The HiPath HG 3540 interconnects SIP-Q endpoints on IP-based networks to telephones on public circuit-switched networks, serving as a gateway.

The HiPath HG 3540 provides:

- Processing of incoming and outgoing calls between circuit-switched networks and local-area networks (LAN)
- Protocol translation services between the SIP-Q and ISDN standards
- Support of trunking through IP networks (that is, full support for and transparent transmission of all ISDN features of the configured ISDN protocol)

The integrated HiPath HG 3540 Voice over IP (VoIP) trunking solution is a central component of the HiPath 4000 IP convergence platform. The HG 3540 Gateway is a new-generation VoIP gateway. It supports the networking of two or more HiPath 4000 systems through a corporate IP network infrastructure. Voice data is transferred in packets through LAN/WAN networks. The uniqueness lies in the fact that the HiPath HG 3540 VoIP trunking solution supports voice-based network protocols such as SIP-Q. A SIP-Q gateway interconnects SIP-Q endpoints on IP-based networks to non-SIP-Q entities (for example, telephones on public circuit-switched networks). It provides the protocol translation between different transmission formats, communications procedures, and audio codecs.

The HiPath HG 3540 VoIP trunking solution can be configured in a point-to-multipoint voice and data network to provide companies operating at numerous dispersed locations with a high degree of network function transparency.

Each management station running TCP/IP and a compatible Web browser can access the HiPath HG 3540 with password authorization. The HiPath HG 3540 includes an embedded Web server.

### 7.6.3 Cisco 2621XM Multiservice Router for SIP Gateways

Redundant 2621 routers ([Figure 7-7](#)) provide the demarcation point into the PSTN. Two 100BT links provide connection from the L2/L3 Ethernet switch. Each 2621 has 4 configurable slots. There is 1 slot available for a Network Module, 1 slot available for an Advanced Integration Module and 2 slots for Integrated Wan Interface Cards. There are also 2 fixed 10/100bT interfaces. The 2621s can be deployed in pairs for box redundancy.

## Main and Extended Interface Components

### Gateways

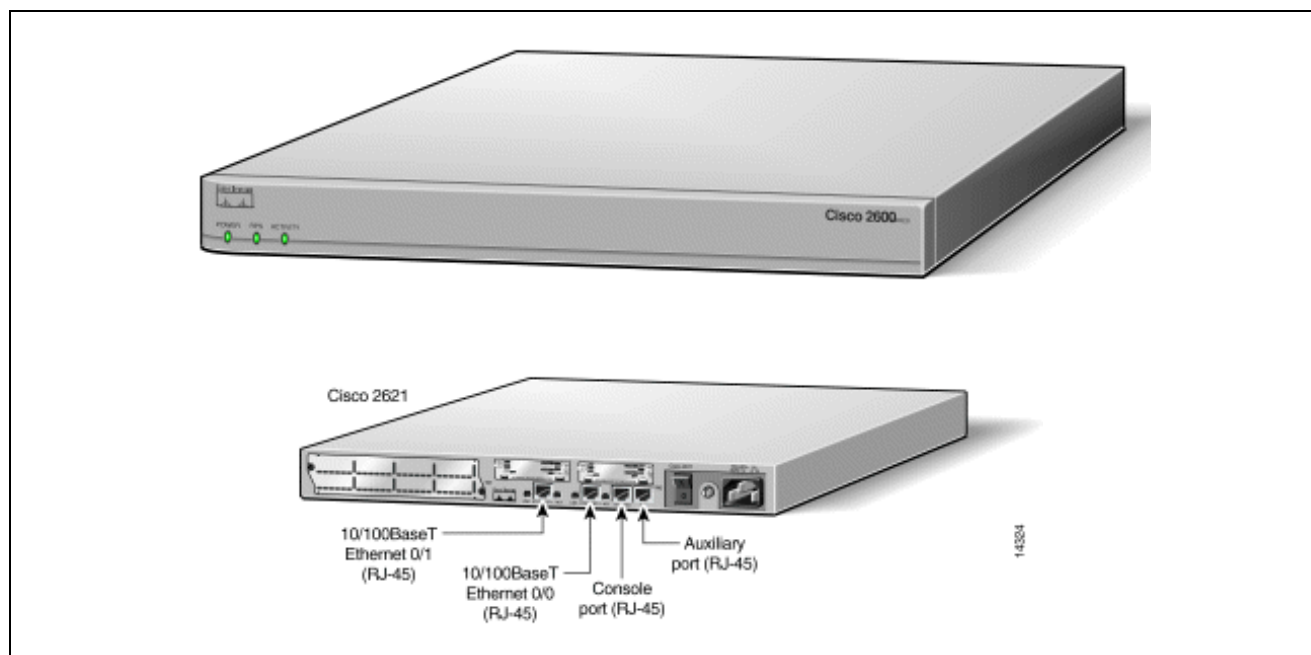


Figure 7-7 Cisco 2621 Front and Rear

### 7.6.4 Secure Infrastructure for Remote Access (SIRA)

SIRA (Secure Infrastructure for Remote Access) is a tool for Technical Service to connect to the customer devices through third party products (for example, PCAnywhere) using the connection data (phone number, login information) stored in the SIRA database.

### 7.6.5 Survivable Branch Office

When the WAN connection to the HiPath 8000 goes down, from a small (under 100 subscribers) branch office perspective, then the branch has to be able to continue with basic telephony. That means:

- Internal SIP to SIP calls can be made
- Calls to the PSTN work
- Incoming calls can be received from an alternate CO trunk

To provide this backup, [Figure 7-8](#) shows the recommended Branch Office configuration.

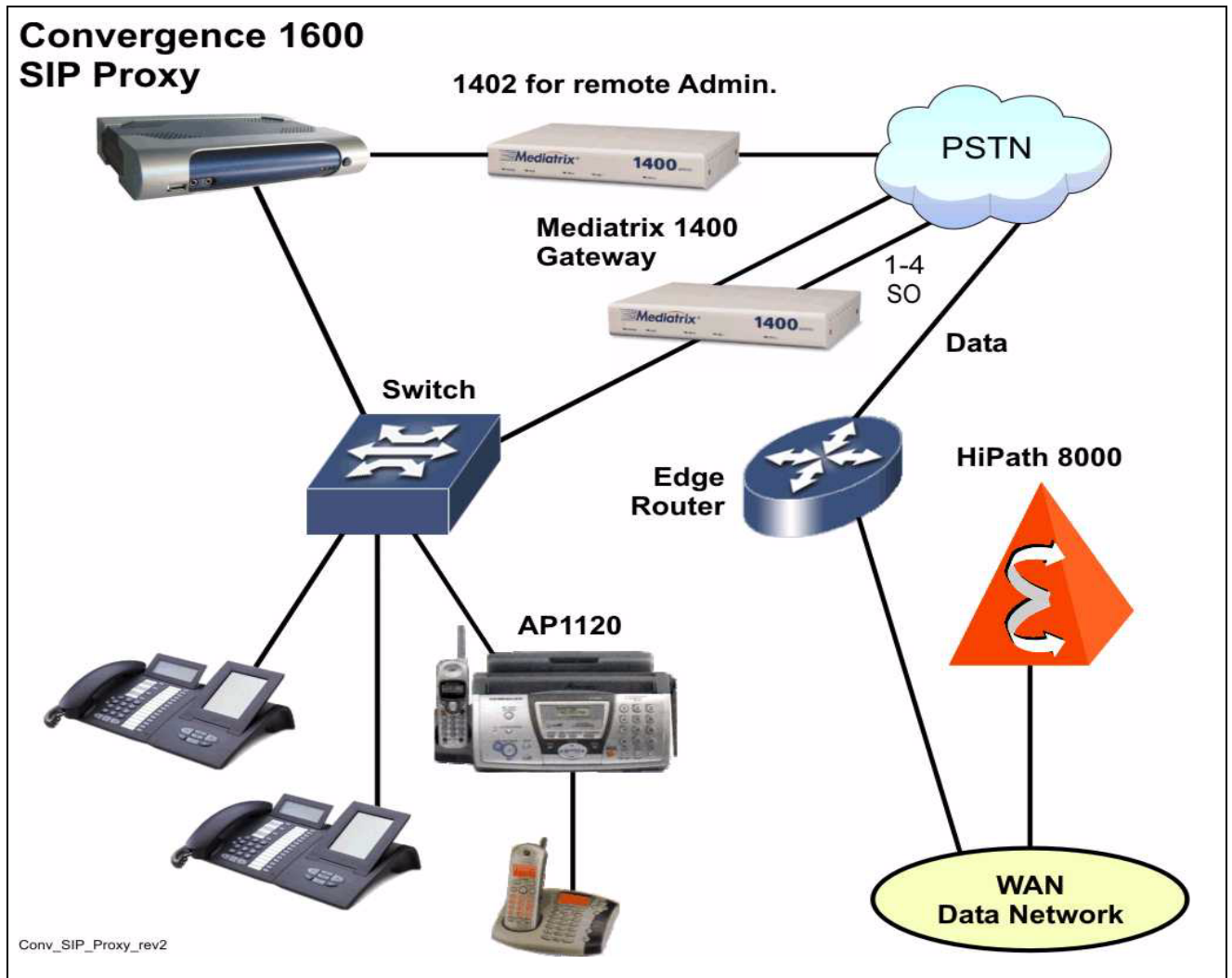


Figure 7-8 Branch Office Configuration

Each branch office has a Convergence 1600 SIP proxy, IP phones (oP400, oP410/20, oP600) and analog adapters AP1120 for Fax and analog modem connections. The phones (and gateways and analog adapters) use the proxy server to resolve their SIP addresses. The proxy server takes the registrations from the phones and passes them to the HiPath 8000 through the WAN. Only when the HiPath 8000 does not respond in a timely manner, does the local SIP proxy take over and try to mediate the call. Once connectivity to the HiPath 8000 is re-established, the proxy forwards the requests to the HiPath again as normal.

## **Main and Extended Interface Components**

### *Gateways*

In the case of failover, calls to the PSTN is routed by the proxy through the Mediatrix 1400 to the locally connected trunks. Similarly, incoming calls on these trunks is forwarded to the respective endpoints through the local SIP proxy. Once the HiPath 8000 takes over again, PSTN calls are routed through the WAN to the central gateway at headquarters.

Note that HiPath 8000 calls from a branch office to another location in an Enterprise network have to be controlled in order to guarantee speech quality of the media stream that is routed over the bandwidth-limited (i.e., bottleneck) link that connects that branch office to the WAN. If the quality is not guaranteed due to insufficient bandwidth, then the call is re-routed via the PSTN gateway at that branch office, if possible, or it has to be denied. This function is known as Call Admission Control (CAC). CAC is now supported by the Comdasy's Convergence 1600 and 2600 SIP proxy with HiPath 8000.

### **7.6.6 RG 2700 Survivable Branch Office**

RG 2700 is a survivable media gateway (SMG) for cross-site networking. It is designed to facilitate the connection of branch offices to the central corporate network and the use of network-wide resources by the branch offices. In organizations with a head office and small/medium-sized branch offices, the gateway provides a guaranteed connection to the central HiPath 8000 system for up to 30 the subscribers in branch offices.

RG 2700 automatically uses a standby dial-up connection if the IP network fails and keeps a stock of important station data so that the SIP phones in the branch offices remain in operation. In a survivability scenario, accounting data is stored locally and made available to HiPath 8000 applications.

The gateway comes with a built-in router and offers a large number of functions for straightforward integration in an existing LAN infrastructure.

## 8 System Performance and Sizing

This chapter describes the performance criteria for HiPath 8000. For more detailed information on performance, see the HiPath 8000 Network Planning Guide.

### 8.1 Assumptions

The performance criteria were measured under controlled lab conditions to ensure consistency across platforms. Where accurate measurements are not yet available, an indication is given which explains whether the figure being quoted is an estimate, an expectation, or derived in some other way.

IBM's Model x345 eServer reached end-of-life in December 2004. While Siemens continues to support it, the Model x346 eServer will now be the platform going forward for the HiPath 8000 deployment.

#### 8.1.1 Call Modeling Criteria

A call model is characterized as a selection of signaling protocols (SIP, MGCP, ...) and traffic patterns. [Table 8-1](#) shows the HiPath 8000 V2.1 protocols and the columns indicate where the protocols are actually used.

Protocol	Used for Subscriber Lines	Used for Trunks (Gateways)	Used Inter-Switch	Note
SIP	X	X	X	
MGCP				Media Server Only
SIPQ (CorNet NQ over SIP)		X	X	HiPath 4000 and Inter-switch
CSTA	X			Interface to ComAssistant

Table 8-1 HiPath 8000 V2.1 Protocols

In addition to protocols, there are three distinct traffic pattern configurations used to provide performance data. These configurations can use any combination of the above but only the following combinations in [Table 8-2](#) were used. Note, since the compact HiPath 8000 is a new offering, this configuration was not used to obtain performance data.

## System Performance and Sizing

### Assumptions

Model	Protocols	Comment
Enterprise (basic)	SIP / SIPQ / CSTA	HiPath 8000 - single switch with GW and Media Server
Enterprise (Network)	SIP / SIPQ / CSTA	HiPath 8000 - multiple switches in a network
Enterprise (compact 300 - 5000 users)	SIP / SIPQ / CSTA	Compact HiPath 8000

Table 8-2 HiPath 8000 Protocols and Configurations

The basic switch configuration [Figure 8-1](#) reflects a typical Enterprise user.

In the network configuration [Figure 8-2](#), the primary impact is that tandem traffic must be taken into account. Tandem traffic can use either SIP or SIPQ, in any mix.

Although the compact HiPath 8000 [Figure 8-3](#) was not directly used in the performance model, the primary performance impact is that the administration tools (iNMC and iSMC replacement) as well as the media server are co-resident on the same server (using the same server) as the HiPath 8000.

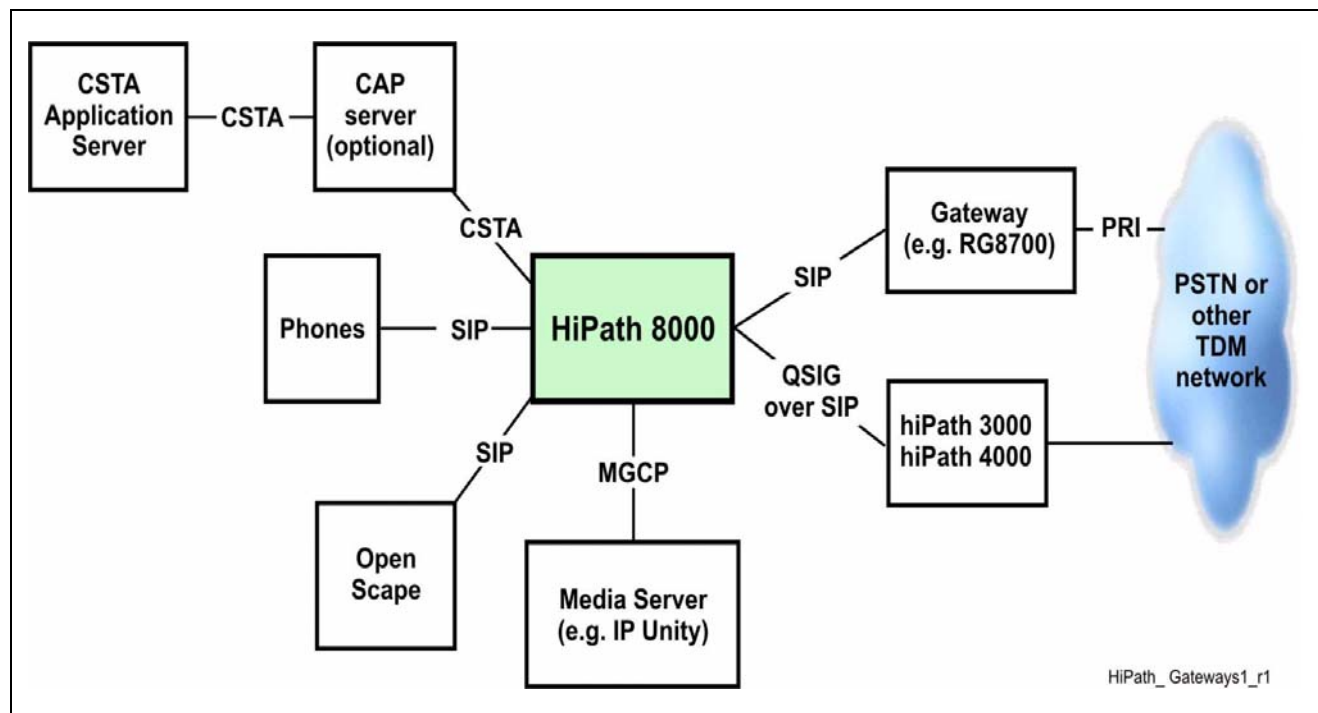


Figure 8-1 HiPath 8000 Enterprise Single Switch



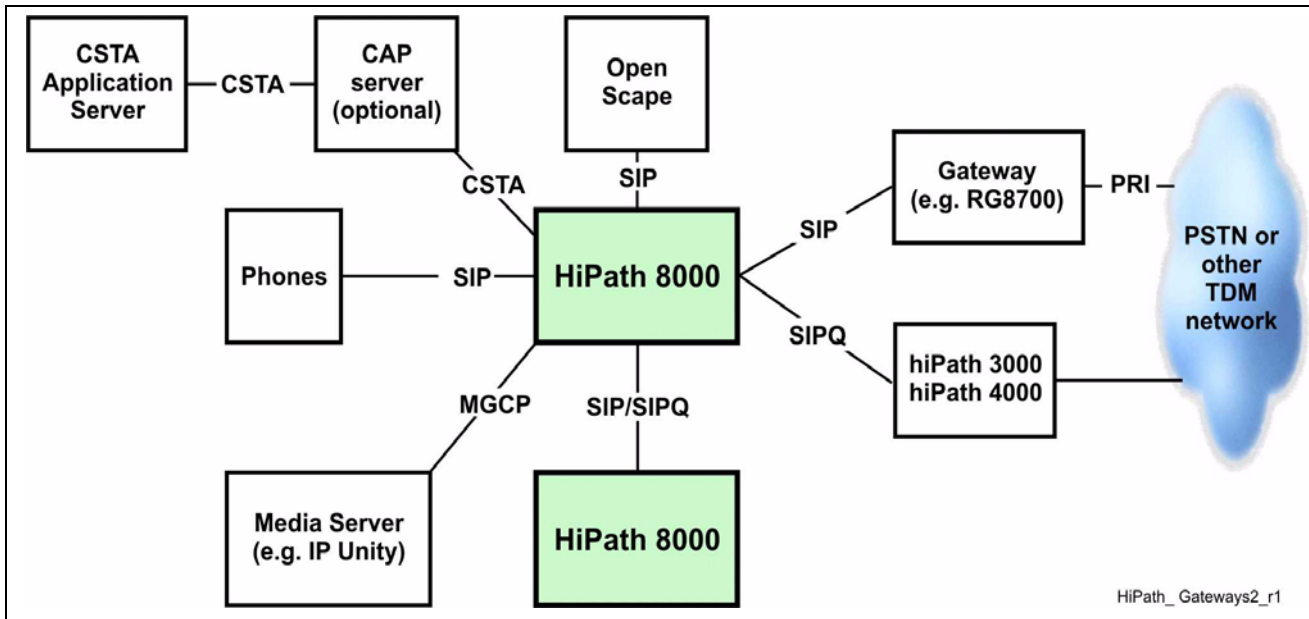


Figure 8-2 HiPath 8000 Enterprise Network

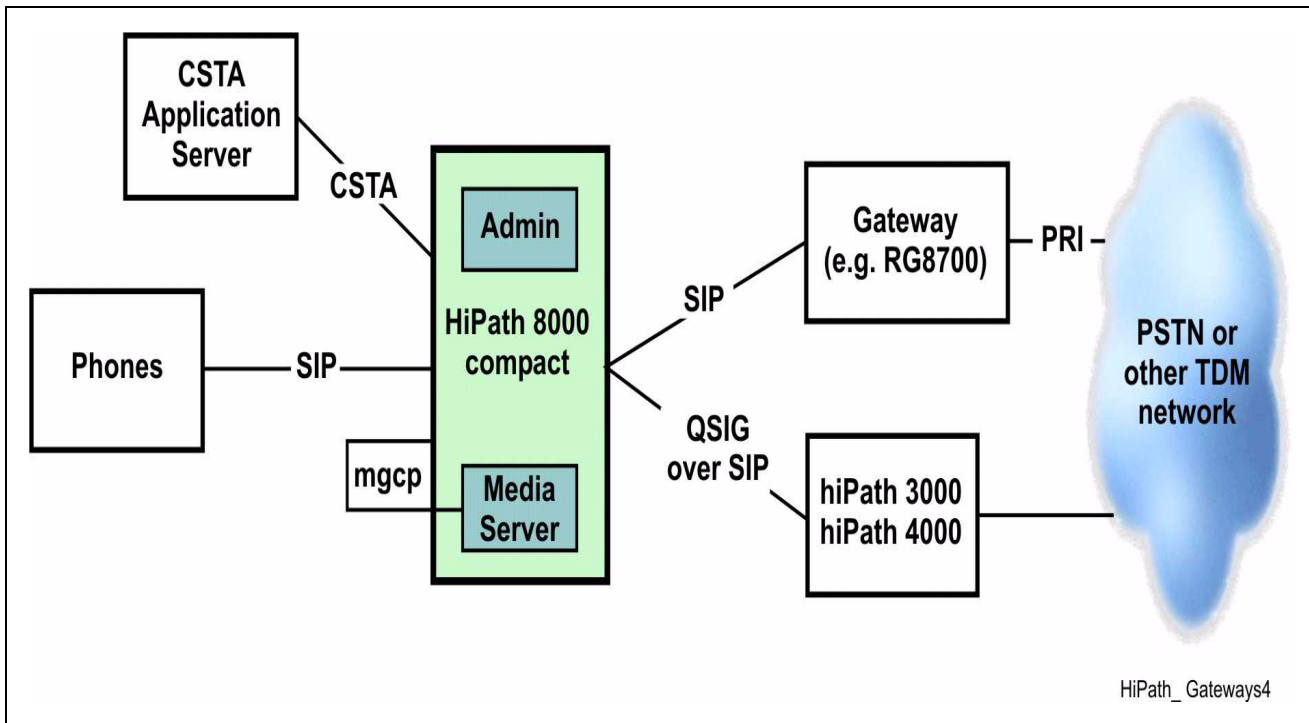


Figure 8-3 Compact HiPath 8000 Enterprise compact Switch

## System Performance and Sizing

### Performance and Sizing Data

#### 8.1.2 Performance as a Function of Number of Messages

The assumption of our call performance model is that the usage of HiPath processing power of each call and each feature is related to the number of external messages (in and out).

So the only input for the performance prediction is the number of messages per protocol type for each line and trunk half call and the number of additional messages for each feature usage per half call.

#### 8.2 Performance and Sizing Data

##### 8.2.1 Overall Performance

Performance testing of Version 2.0 in numerous configurations has yielded the following base performance number. The IBM x346 server is rated (by IBM) at 2400 transactions per second.

158 calls per second \* 14 messages per call = 2212 messages per second

<b>ACTUAL TEST MEASUREMENTS (Version 2.0)</b>	<b>Calls per Second</b>
Basic SIP to SIP call Capacity (single node) UDP	158
Basic SIP to SIP calling with Digest Auth activated	123
Basic SIP to SIP calling with TCP/TLS transport without Digest Auth activated	165
CSTA provisioned on all lines (but no monitors active)	140
CSTA provisioned and monitoring active on all lines	125
CSTA make call (click-to-dial) with monitoring on all lines	100
Basic Keypad Calling (1 line appearance per line)	119
SIP-Q calls	100
Keypad Calling (2 line appearances per line)	85

Table 8-3 Overall Performance

<b>Resource</b>	<b>Limitations</b>
IPUnity Version 2.7	limited to 30 calls per second
IPUnity Version 2.7	maximum 3072 channels (only tested to 2000 channels)
TLS sockets	10,000 endpoints per node with TLS enabled.
Trunks / Off net Calls	10,000
Subscribers	100,000
Simultaneous Stable SIP Calls	12,500 - 20,000

Table 8-4 Trunk and Subscriber Limitations

## 8.2.2 MTBF of Hardware

Table 8-5 shows the IBMx345/346 MTBF hardware that includes installed PCI cards and the shared disk arrays.

<b>System</b>	<b>Calculated HW Availability for Two Nodes</b>
IBM x345/346	99.9997%

Table 8-5 Server Availability for IBM

## 8.2.3 Number of Ethernet Interfaces

Table 8-6 shows the fixed number of 10/100/1000 BaseT ethernet interfaces.

<b>Platform</b>	<b>Fast Ethernet</b>
HiPath 8000 V2.1	8/16

Table 8-6 Number of Ethernet Interfaces

## 8.2.4 Database Sizing

Table 8-7 provides all the necessary database sizing data.

## System Performance and Sizing

### Performance and Sizing Data

Attribute	x345/x346
<b>ADM Data</b>	
bg_attendant_num_t	1,000
bg_business_grp_t	1,000
bg_dial_plan_t	1,000
bg_main_num_t	1,000
bg_svc_t	1,000
bg_svc_access_code_t	50,000
Retailer_profile_t	10,000
Sub_endpoint_index_profile_t	100,000
Subscriber_profile_t	100,000
subscriber_sip_profile	100,000
system_sip_profile	1
teen_child_t	75,000
teen_parent_t	25,000
Timezone_t	1,000
KeySet_info_t (No of Subscribers * 0.7)	70,000
Line Appearances (No of Key Sets * 1.8)	126,000
<b>RTM Data</b>	
ntm_ctrl	1,000
ntm_tgrp_ctrl	1,000
Signal_profile	1,000
<b>SDM Data</b>	
Service_data_t	100,000
<b>XDM Data</b>	
Endpoint and Alias Tables (for SIP/SIP-Q endpoints)	
One alias (6-to-11 digits), one contact (19 or 20 characters)	105,000
One alias (6-to-11 digits), two contacts (19 or 20 characters).	91,500
One alias (10-to-14 digits), two contacts (30 and 33 characters).	74,100
Alias_suffix_t	3,000

Table 8-7 Database Sizing(Sheet 1 of 4)

**System Performance and Sizing**  
*Performance and Sizing Data*

<b>Attribute</b>	<b>x345/x346</b>
Gatekeeper_t	1,000
Carrier Destination and Routing Table (No bad_alloc exceptions until 10,000 (i.e., 0000 to 9999) carriers, each with 9 routes)	10,000
Class_service_t	30,000
E164 Code (4-to-8 digit lengths, 9 diff numbering plans; approx same for 6-to-10 digits and 22 No. plans)	203,000
e164_day_schedule	1,000
E164 Destination and Route Tables	
Two routes (7-digit insert DN)·	54,100
Three routes (Phase 2 routes w/insert DN)	41,400
Three routes (all routes w/insert DNs)·	41,400
Eight routes (three routes w/insert DNs)	19,100
e164_dest_route_link	10,000
e164_dest_schedule	1,000
Office Code and Home DN Tables	
40 office codes all starting w/5618xy, 4-digit subs	275,800
40 office codes 20 starting w/5618xy and 20 w/7328xy, 4-digit subs·	275,800
40 office codes 10 starting w/5618xy, 10 w/7328xy, 10 w/5558xy, and 10 w/6668xy, 4-digit subs	275,500
E164_ip_dest_t	10,000
e164_period_schedule	30,000
e164_time_dest	10,000
Intercept and Treatment	
Two treatments per intercept (45 chars annld)	94,000
Two treatments per intercept (80 chars annld)	77,000
isdn_provision_t	20,000
Ntm_code_control_t	1,000
OPC_t	n/a
Prefix Access Code	
22 No. plans, 1-to-4 digit lengths	35,300

Table 8-7 Database Sizing(Sheet 2 of 4)

## System Performance and Sizing

### Performance and Sizing Data

Attribute	x345/x346
22 No. plans, 1-to-4 digit lengths, 100 entries w/6-digit insert digits	35,300
22 No. plans, 1-to-4 digit lengths, 100 entries w/11-digit insert digits, 20K entries w/3 len insert digits	35,200
22 No. plans, 1-to-5 digit lengths, 100 entries w/11-digit insert digits, 20K entries w/6-digit insert digits	35,200
Rate_area_t	30,000
Home PNP Location and Extension(No bad_alloc exceptions until 300K entries of extension lengths varying from 1-to-4 digits)	300,000
Pickup Groups	10,000
Other	
OAM&P transactions per peak minute	10
OAM&P transactions per average hour	30
Storable CDRs (7 days * 14 hours * 3600 * cps)	25 Million
Provisioned Features	100%
Feature Activations	20%
Contexts	
CTX_SRS_ACARSCAN	16,400
CTX_SRS_CSTA_SM, CTX_SRS_CSTA_SM_2, CTX_SRS_CSTA_SM_3 and CTX_SRS_CSTA_SM_4	4
CTX_SRS_H323_CC and CTX_SRS_H323_CC2	15,000
CTX_SRS_INSVC_RW	20,000
CTX_SRS_MGCP_SM and CTX_SRX_MGCP_SM2	20,001
CTX_SRS_PRMGR and CTX_SRS_PRMGR2	3
CTX_SRS_SMDI	40,000
CTX_SRS_SSAL_CALLDATA	40,000
CTX_SRS_SSAL_CPU_RINGLIST	40,000
CTX_SRS_TTUD1 and CTX_SRS_TTUD2	16
CTX_SRS_UCE_RW	20,000
Recovery (All figures are in seconds)	
Failure of 1 Power Supply	0
Failure of 2 Power Supplies	0

Table 8-7 Database Sizing(Sheet 3 of 4)

<b>Attribute</b>	<b>x345/x346</b>
Failure of 1 Node	6
Single cross-over cable failure	0
Dual cross-over cable failure	0
Single call processing cable failure	0
Single billing cable failure	0
Single management cable failure	0
Disk failure - 1 disk of disk array	0

Table 8-7 Database Sizing(Sheet 4 of 4)

## 8.2.5 Context Sizing

Contexts are blocks of transient memory that are used by applications to store per-call information. The size of contexts is different from application to application and the type of information stored within the context also differs from application to application

[Table 8-8](#) shows the IBM x345/x346 context sizing.

<b>Context Name</b>	<b>Quantity</b>
H323 CC	15,000
IPSEC	32,000
MGCP	1,000
SIP	100,000
UCE RW	20,000

Table 8-8 IBM x345/x346 Context Sizing

**System Performance and Sizing**

*Performance and Sizing Data*



## 9 Statistics, Accounting, and Diagnostics

This chapter describes the statistics, accounting, and diagnostic features for the HiPath 8000.

### 9.1 Statistics and Accounting

To display statistics, use the iNMC or CLI.

#### 9.1.1 HiPath 8000 Level

The HiPath 8000 Softswitch allows you to monitor performance counters and statistics on the following entities:

- Operational Measurements (OM)
- CDR System
- UCE performance data
  - Completed Calls And Aborted Calls Statistics
  - Interworking Calls Statistics
- SIP performance data
  - Messages Sent By Client
  - Messages Received by Client
  - Messages Sent by Server
  - Messages Received by Server
- Message Counters
- Errors In Transaction Portion - Message Type
- Errors In Transaction Portion - General Problem
- Errors In Transaction Portion - Invoke Problem
- Errors In Transaction Portion - Return Result Problem
- Audits & Recovery performance data
- Overload Handling performance data
  - SIP
  - MGSM
- Services performance data

## **Statistics, Accounting, and Diagnostics**

### *Monitoring Support*

- Anonymous Call Rejection
- Call Forwarding
- Calling Identity Delivery
- Call Waiting
- Speed Calling
- Toll-Free
- Screen Line Editing
- Three Way Calling
- Intercom Call
- Voice Mail

## **9.2 Monitoring Support**

### **9.2.1 Operational Measurements**

The Operational Measurements (OM) features enable you to monitor the performance and usage of HiPath 8000 resources, including Network Traffic Management (NTM) Code Controls, and Business Groups. In addition to viewing usage data through the iNMC, this data is stored in OM files on the HiPath 8000.

#### **9.2.1.1 Traffic Measurements**

The HiPath 8000 system provides traffic measurements that are collected and recorded as CSV files by the Operational Measurements Manager (OMM). The files may then be downloaded through FTP (actually Secure FTP) to any Telco platform concerned with the collection of performance data. The files may be transferred in either binary or ASCII format.

There are two types of OM data collected:

- Peg Usage counters — cumulative measurements driven by event occurrences such as successful calls; call failures and any kind of state transition.
- Usage Register counters — cumulative duration of a specified event or condition.

The following counters are required on a per Business Group basis:

- Originating Calls (PUC)
- Terminating Calls (PUC)
- Intragroup Calls (PUC)

- Feature Use (PUC)
- Feature Activation (PUC)
- Feature Deactivation (PUC)
- Dial 8, Dial 9 Calls (PUC)
- Direct Inward Dialing (DID) (PUC)
- Attendant Attempts (PUC)
- Attendant Overflows (PUC)

The following Usage accumulators are needed on a per Business Group basis:

- Intragroup Usage (URC)
- Originating Usage (URC)
- Terminating Usage (URC)

## **9.2.2 Call Trace**

The trace manager runs in an active/standby mode in the cluster and provides a generic API to all call control processes (that is, SMs, UCE, CCM) for call tracing purpose. The API is a shared library that is called (by the process tracing a call) every time a call related message is received or sent for a specific call or a group of calls based on the trace trigger condition. Call tracing is configurable for each of the signaling managers.

## **9.3 Diagnostics Support**

### **9.3.1 Network Diagnostics**

The iNMC and CLI support the Test Line Origination (TLO) feature to run diagnostic tests on network connections. The TLO tool allows you to run test calls. Test calls utilize individual circuit paths and use signaling to test switch connections between the switch and adjoining Class 4/5 switches. After the addressed switch performs the appropriate loopback or tone generation, the switch determines and reports the quality of the voice paths.

**Statistics, Accounting, and Diagnostics**

*Diagnostics Support*

# Index

## A

- AAA manager 2-14
- access control 2-16
- access profiles 6-8
- accountability
  - OAM&P service 4-36
  - security 2-17
- active/active applications 4-16
- address translation and routing
  - call process 4-29
  - features 4-13
- administrator role 6-10
- advanced routing 2-8
- alias translation 4-32
- alternate routes 4-29
- AMA Mediation Server 6-6
- Announcement Creator Service 7-4
- Announcement Management Service 7-4
- API 9-3
- AS 4-5
- associator segment 4-5
- audio codecs 7-15
- authentication
  - OAM&P service 4-36
  - preventive security feature 2-16
  - subscriber feature 2-12

## B

- B2BUA 4-27
- Back to Back User Agent 4-27
- backup and restore 4-37
- base system 3-2
- Basic Operating Principles 5-6
- BHCA 2-16
- billing file format 6-6
- business groups role 6-10
- busy hour call attempt 2-16

## C

- call control 4-17

- call detail records 6-6
  - OAM&P feature 2-11
  - OAM&P service 4-35
  - ticket manager 4-4
  - UCE role 4-6
- call prefixes 4-31
- call processing
  - active applications 4-16
  - applications 4-1
  - engine 4-5
  - feature highlight 2-8
  - feature summary 2-10, 2-10
  - features 4-12
  - HiPath 8000 functions 4-17
  - RTP context manager service support 2-14
  - SLEE 4-10
  - software architecture 4-17
- call resource auditing 4-19
- call trace 9-3
- caller ID blocking 4-18
- calling number display 4-18
- CCM 4-10
- CDRs 6-6
  - OAM&P feature 2-11
  - OAM&P service 4-35
  - ticket manager 4-4
  - UCE role 4-6
- central distributor module 4-5
- certified Ethernet switches 3-8
- Cisco 2621XM router 7-15
- Cisco gateway 2-7
- Cisco PIX 535 7-3
- CLI
  - management facilities feature 2-8
  - OAM&P feature 2-11
  - security features 6-7
- codec 4-33
- ComAssistant 8000 7-10
- command line interface

## Index

- management facilities feature 2-8
- OAM&P feature 2-11
- security feature 6-7
- configuration management 6-4
- connection control manager 4-10
- context manager 4-4
- convergence 1600 SIP proxy 7-17
- CSTA signaling manager 4-8

### D

- data
  - backup 2-17
  - confidentiality 2-17
  - integrity 2-16
- DDR memory 3-2
- diagnostic support 9-3
- digit translation
  - most-matched 4-31
  - support 4-32
- digital signal processing 7-6
- Dispatcher 4-28
- displaying statistics and accounting 9-1
- Documentation Feedback 1-3
- DSP 7-6
- dynamic endpoint registration/unregistration 4-32

### E

- E.164 directory number translation 4-30
- element management
  - features 4-14
  - system 2-7
- element mass provisioning 4-29
- EMS 6-3
- endpoints
  - admission control 4-32
  - POTS 4-20
  - SIP 4-33
  - SIP phones 2-6
- Error Management 7-5
- Ethernet Switch 5-4
  - failover 5-13
- event and alarm manager 4-4
- event handler 6-4
- external CLI scripts 6-7

- external ports 3-4

### F

- Failover
  - ethernet switch 5-13
  - node 5-13
  - processes 5-13
- fault management 6-4
- feedback, documentation 1-3
- firewalls 7-3

### G

- gatekeeper discovery 4-32

### H

- H.323
  - endpoint registration 4-33
  - interface 2-7
- hardware redundancy 2-18
- Harmony 6000 media server
  - description 7-5
  - hardware 7-6
- HG 3550 7-15
- HiPath 8000
  - address translation and routing 4-13
  - base software 4-1
  - base system 3-2
  - call processing 4-12, 4-17
  - call processing applications 4-1
  - configuration management 6-4
  - connection control manager 4-10
  - description 2-2
  - element management features 4-14
  - end point support 4-19
  - extended interface components 7-1
  - external ports 3-4
  - fault management 6-4
  - features 2-8
  - features summary 2-10
  - hardware redundancy 2-18
  - LEDs and switches 3-4
  - local and remote administration 6-5
  - main interface components 7-1
  - management tools 6-2
  - managing 6-4

- network element management system (EMS) 6-3
  - OAM&P 4-14
  - platform 4-11
  - programmability 4-6
  - QoS 2-17
  - QoS control 4-13
  - Resilient Telco Platform 4-2
  - security 2-16
  - service logic execution environment (SLEE) 4-10
  - services framework 4-10
  - signal processing 4-17
  - signaling managers 4-7
  - signaling protocols 4-11
  - softswitch 9-1
  - software components 4-10
  - software redundancy 2-18
  - software upgrades 6-5
  - system scalability 2-16
  - Universal Call Engine (UCE) 4-5
  - HiPath MetaManagement 2-8
  - HiPath QoS 2000 2-17
  - HiPath QoS Manager 2-17
  - HiPath Scurity 2-8
  - hot-swap redundant power 3-6
  - HTTP 2-8
- I**
- IBM 346 technical specifications 3-6
  - IBM x346 servers 3-2
  - inactivity timer 6-8
  - incoming transaction segment 4-5
  - iNMC
    - access profiles 6-8
    - clients per server 6-14
    - element and network management 6-12
    - main screen 6-13
    - network management 6-1
    - node groups 6-8
  - Intel Xeon processors 3-2
  - interchangeable NPA and NXX 4-30
  - interface components 7-1
  - inter-process communication 4-4
- I**
- IPCI 4-4
  - iSMC
    - element management system 2-7
    - OAM&P service 4-35
    - security management 6-10
    - user management 6-9
    - users and roles 6-9
  - iSSC
    - element management system 2-7
    - iSMC security 6-10
    - OAM&P service 4-35
    - subscriber management 6-1, 6-1
  - ITS 4-5, 4-5
- K**
- Kagoor 2-6
  - Kagoor Networks® 7-2
- L**
- L2/L3 ethernet switches 2-6
  - LAN/WAN 2-17
  - layered security 2-17
  - LEDs 3-4
  - Linux SuSe 2-2
  - local administration 6-5
  - Logging 7-5
  - logging function 6-4
- M**
- managing the HiPath 8000 6-4
  - mass provisioning 6-17
  - measurements
    - operational 9-2
    - traffic 9-2
  - Media Gateway Control Protocol 4-20
    - signaling managers 4-9
  - Media Processing Service 7-4
  - media processor card 7-6
  - Media server 2-6
  - memory, DDR 3-2
  - MGCP
    - call waiting 2-13
    - endpoint support 4-20
    - signaling manager 4-9
  - MGCP Service 7-4

## Index

modular UNIX packaging [4-37](#)  
most-matched digit translation [4-31](#)  
MPC [7-6](#)

## N

NAS [7-5](#)  
nature of address [4-30](#)  
NEM [2-14](#)  
Network Elements Management [2-14](#)  
network management center [2-7](#)  
network processor [7-7](#)  
network-attached storage [7-5](#)  
network-based framework [4-10](#)  
NMC [2-7](#)  
NMC-SMX  
    description [6-12](#)  
    structure [6-12](#)  
nodal based service [4-10](#)  
node and communication manager [4-3](#)  
node groups [6-8](#)  
Node Separation [5-4](#)  
non-call processing-based service [4-10](#)  
NormalAdmin [6-9](#)

## O

OAM&P  
    architecture [4-34](#)  
    features [4-14](#)  
    services [4-34](#)  
OAM&P service  
    accountability [4-36](#)  
    authentication [4-36](#)  
    CDRs [4-35](#)  
    rolling upgrade [4-35](#)  
    user authentication [4-36](#)  
ObserverProcess [2-14](#)  
operational measurements [9-2](#)  
OPS [2-18](#)  
optiClient 130 S  
    extended interface component [7-12](#)  
Oracle Parallel Server [2-18](#)  
origin dependent routing  
    alias translation [4-32](#)  
    H.323 endpoint registration [4-33](#)  
    SIP endpoint registration [4-33](#)

OTS [4-5](#)  
outgoing transaction segment [4-5](#)

## P

packetization period [4-33](#)  
POTS  
    endpoint support [4-20](#)  
prefix digit translation [4-31](#)  
private numbering plan [6-17](#)  
Process Configuration [5-8](#)  
    failover [5-13](#)  
RTP  
    alias groups and members [5-10](#)  
    startup groups and dependencies [5-9](#)  
processors, Intel [3-2](#)  
provisioning  
    log [6-10](#)  
    mass provisioning [6-17](#)  
    private numbering plan [6-17](#)  
    rolling upgrades [6-17](#)  
PSTN routing manager [2-14](#)

## Q

QoS [2-17](#)  
QoS control  
    features [4-13](#)  
    MGCP connection [4-33](#)

## R

RAID 1 [3-3](#)  
Real Time Application Framework [7-5](#)  
real-time data management [4-19](#)  
real-time media transaction controllers [2-14](#)  
redundant proxy registration servers [2-14](#)  
remote  
    administration [6-5](#)  
Resilient Telco Platform  
    basic cluster redundancy [2-14](#)  
    middleware [2-8](#)  
    software application [4-2](#)  
resource reservation [4-33](#)  
role  
    RTP middleware [4-3](#)  
    UCE [4-5](#)  
roles



- administrative/maintenance 6-9
- user 4-36
- rolling upgrade
  - OAM&P service 4-35
  - provisioning feature 6-17
- RTP
  - alias groups and members 5-10
  - basic cluster redundancy 2-14
  - context manager service 2-14
  - event manager 6-4
  - middleware 2-8, 2-18
  - middleware role 4-3
  - node manager 2-14, 4-3
  - software application 4-2
  - startup groups and dependencies 5-9
- RTP components
  - context manager 4-4
  - event and alarm manager 4-4
  - inter-process communication 4-4
  - node and communication manager 4-3
  - ticket manager 4-4
  - trace manager 4-4
  - TTUD dispatcher 4-4
- RTP IPC 4-27
- S**
- SCC 7-6
- SDAL/DBAL 4-8
- SDP 4-21
- secure infrastructure for remote access 7-16
- security features
  - CLI 6-7
  - iNMC 6-8
  - iSMC 6-9
  - iSMC security 6-10
- security log 6-10
- security logging 2-17
- security system 2-8
- service control 4-18
- service logic execution environment (see SLEE) 4-10
- service management center 2-7
- services role 6-10
- Session Description Protocol 4-21
- Session Initiation Protocol (see SIP) 4-27
- shelf controller card 7-6
- signaling managers
  - CSTA signaling manager 4-8
  - main tasks 4-7
  - MGCP 4-9
  - SIP 4-10
- signaling protocols 4-26
  - features 4-11
  - SIP 4-27
- simple network management protocol 2-8
- Simple Object Access Protocol 2-8, 6-9
- SIP
  - call examples 4-22
  - endpoint support 4-20
  - implementation 4-27
  - interface 2-7
  - interface block diagram 4-28
  - signaling manager 4-10
  - signaling protocol description 4-27
- SIP Over TCP 4-27
- SIP phones
  - endpoints 2-6
- SIRA 7-16
- SLEE
  - native class services 4-18
  - network-based 4-10
  - nodal-based 4-10
  - non-call processing-based 4-10
- SMC security 6-10
- SNMP 2-8
- SOAP 2-8, 6-9
- sockets 4-27
- software
  - architecture 4-15
  - complex overview 4-2
  - components 4-10
  - features 4-11
  - redundancy 2-18
  - upgrades 6-5
- split brain avoidance 5-4
- subscriber self-care 2-7
- Sun Netra 1400 5-3
- SuperAdmin 6-9

## Index

### SURPASS hiQ 8000

- active/active applications [4-16](#)
  - basic operating principles [5-6](#)
  - call control [4-17](#)
  - OAM&P [4-34](#)
  - password [6-7](#)
  - privileges [6-7](#)
  - system components [5-3](#)
  - user names [6-7](#)
- survivable branch office [7-16, 7-18](#)
- switches [3-4](#)
- system
- management [3-6](#)
  - redundancy [2-8](#)
  - scalability [2-16](#)
- System Architecture
- Ethernet Switch [5-4](#)
  - Sun Netra 1400 [5-3](#)
- System Management [7-5](#)

## T

- ticket manager [4-4](#)
- TLS
- encryption and data integrity [4-21](#)
  - protocol [4-21](#)
  - security feature [6-11](#)
- total telephony feature package [2-8](#)
- trace manager [4-4, 9-3](#)
- traffic measurements [9-2](#)
- Transport Layer Security (see TLS) [4-21](#)
- treatments [7-9](#)
- TTUD dispatcher [4-4](#)

## U

- UCE
- feature segment component [4-18](#)
  - primary components [4-5](#)
  - role [4-5](#)
  - software component [4-5](#)
- UDP/TCP [4-27](#)
- universal call engine (see UCE) [4-5](#)
- usage collection [2-14](#)
- user authorization [4-36](#)
- user management role [6-10](#)

## V

- Vertical Service Codes [4-32](#)
- VLANs [2-17](#)
- VoIP traffic management system [2-6, 7-2](#)
- VSCs [4-32](#)

## W

- web portal [6-10](#)



[www.siemens.com/hipath](http://www.siemens.com/hipath)

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products.

An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

The trademarks used are owned by Siemens AG or their respective owners.

