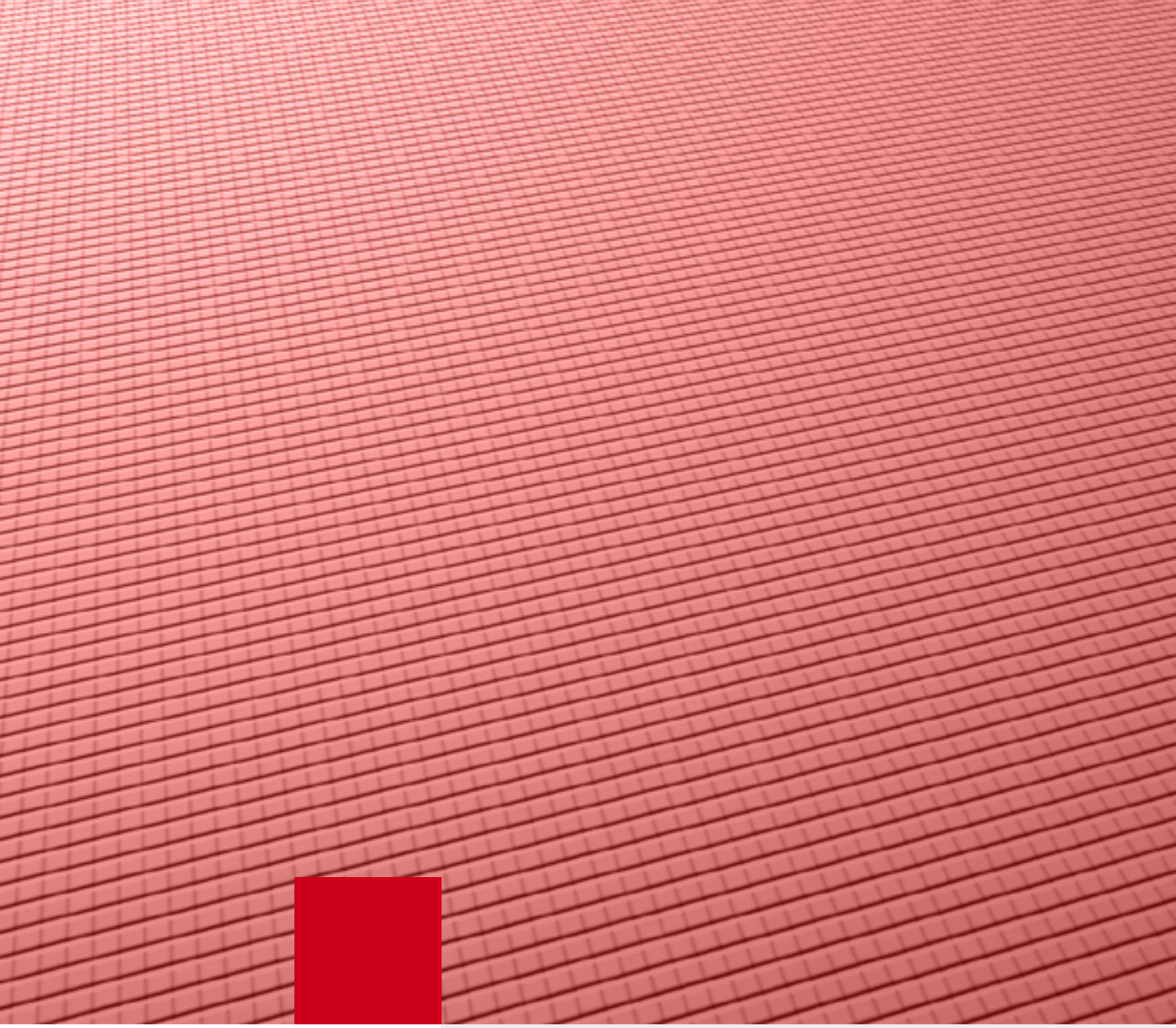

HiPath 8000 Version 2.2

Feature Description Guide

SIEMENS

Global network of innovation

1P A31003-H8022-F100-2-7618

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 Enterprise Communications GmbH & Co. KG 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.

Hofmannstraße 51, D-81359 München, Germany
Reference No.: A31003-H8022-F100-2-7618
Subject to availability. Right of modification reserved.

History of Changes

Version Number	Date	Summary
1	September 2006	Initial release
2	October 2006	Second publication of document. Addition of information for Genesys call center and Agent Console application, and for HiPath ProCenter integration. Miscellaneous corrections.

Contents

1 Important Notices

1.1 About This Book

1.1.1 Audience

This book is intended for those who would like a better understanding of the HiPath 8000 features, including Siemens customers, systems engineers (SEs), and sales representatives.

1.1.2 Prerequisite Knowledge

You should be familiar with basic telecommunications equipment functionality and terminology.

1.1.3 Purpose of This Book

The *HiPath 8000 Feature Description Guide* describes each of the HiPath 8000 system and station features. For most features, the following information is included, as applicable:

- **Definition:** What the feature is
- **Functional Operation**: How the feature works
- **Call Detail Recording (CDR)**: The CDR information that pertains to the use of the feature
- **Traffic Measurement**: The traffic measurements that pertain to the use of the feature
- **Networking:** How the feature operates differently in a HiPath 8000 network, including those networks that use QSIG tunneling to connect with a legacy PBX.
- **Guidelines for Implementation and Use:** How the system may affect or be affected by the feature, along with recommendations for the most efficient use of the feature

This book also provides an overview of the features provided by Siemens session initiation protocol (SIP) endpoints when they are used in a HiPath 8000 environment.

1.1.4 Using This Book

This book contains the following chapters and appendixes:

- This chapter provides information to use this book; it also provides a list of related publications and the procedures to provide feedback about this book.
- Chapter 2, “SIP Endpoint User Features” provides an overview of local user features that reside in Siemens SIP endpoints such as the optiPoint 410 S and optiPoint 420 S; optiClient 130 S; optiPoint WL 2 Professional S; and optiPoint 150 S.

- Chapter 3, “Keyset Telephone User Features” describes features specific to keyset operations. The keyset operations features provide multiple line capability, and other associated functions, for a SIP endpoint configured as a keyset. Keysets are sometimes known as *multiline telephones.*
- Chapter 4, “HiPath 8000-Based Station Call Forwarding User Features” describes the station call forwarding features that reside in the HiPath 8000. These features are accessible via feature access code; the user can also assign a frequently used feature to a feature key or repdial key.
- Chapter 5, “Other User Features” describes other user features that reside in the HiPath 8000. Examples of such features are calling identity delivery and suppression features, abbreviated dialing features, redial and call return features, and display features.
- Chapter 6, “Business Group Features” describes features that are specific to business groups. These features simplify such tasks as dialing plan administration, intragroup communication, and traffic measurements.
- Chapter 7, “Other Group Features” describes the group call pickup feature, which allows users to answer calls on behalf of one another, and the hunt group feature, which permits calls to be routed to an idle line within a group of specified lines.
- Chapter 8, “Emergency Calling Features” describes how the HiPath 8000 uses a Siemens or Cisco gateway, sometimes in conjunction with the Telident station translation system (STS), to provide emergency calling (E911) support. This chapter is applicable to the United States only.
- Chapter 9, “Routing and Translation Features” describes the HiPath 8000 features that provide routing and translation, including public numbering plan compliance and routing that varies depending upon such factors as origin, traffic, and bearer capability.
- Chapter 10, “Call Admission Control Features” describes the HiPath 8000’s integrated call admission control (CAC) feature, which provides for the management of the bandwidth used for the transport of media traffic (such as RTP audio and T.38 fax) through the bottleneck links that may exist in an enterprise network.
- Chapter 11, “PRI Features” describes HiPath 8000 features that support network-side PRI capabilities.
- Chapter 12, “QSIG Tunneling Features” describes SIP-Q, which permits the HiPath 8000 to interwork with another HiPath 8000, the HiPath 4000, or a QSIG PBX connected via the RG 8700 gateway.
- Chapter 13, “CDR Features” describes the CDR features that simplify call tracking and billing for the HiPath 8000.
- Chapter 14, “Security Features” describes the HiPath 8000 features that provide security for various aspects of the system, such as billing records, data files, and administration interfaces.

- Chapter 15, “Serviceability Features” describes the HiPath 8000 features that improve serviceability, such as diagnostics and debug tools, code controls, and administrator controls.
- Chapter 16, “SIP Signaling Features” describes the HiPath 8000 features that support SIP signaling and the interworking with other elements such as application servers, voice conferencing applications, and voice mail systems.
- Chapter 17, “CSTA Support Features” describes how the HiPath 8000 provides a standard European Computer Manufacturers’ Association (ECMA) Computer Supported Telecommunications Applications (CSTA) protocol interface to external CTI applications, which permits applications such as ComAssistant, OpenScape, and HiPath ProCenter to control the HiPath 8000 SIP endpoints. It also describes other HiPath 8000 capabilities relevant to applications that utilize the CSTA interface.
- Chapter 18, “System Functions and Features” describes the HiPath 8000 functions and features that support such tasks as alarm reporting, message waiting indicator control, and recovery handling.
- Appendix A, “Alphabetical Feature Listing” provides a comprehensive, alphabetical list of HiPath 8000 and SIP endpoint features, classified by feature type. It includes a cross-reference to assist in easily locating each feature description in this guide.
- Appendix B, “Feature Access Codes”, lists and describes the default feature access codes for user features that reside in the HiPath 8000.
- Appendix C, “Supported SIP Methods” provides a brief description of the SIP methods that are referenced in several feature descriptions in this book.

This book also contains an index.

1.1.5 Related Information

The following are related publications:

- *HiPath 8000 Backup and Recovery Guide*
- *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 Provisioning Definition Worksheets*
- *HiPath 8000 Data Sheet*
- *HiPath 8000 Delta Specifications for Version 2.2*
- *HiPath Deployment Service Administration Manual*
- *HiPath 8000 E-911 Support and Planning Guide*

- *HiPath 8000 Master Glossary*
- *HiPath 8000 Master Index*
- *HiPath 8000 NetManager iNMC Server Installation, Administration, and Utilities Guide*
- *HiPath 8000 NetManager iSMC Customization Guide*
- *HiPath 8000 NetManager iSSC Installation and Customization Guide*
- *HiPath 8000 Network Planning Guide*
- *HiPath 8000 Overview Guide*
- *HiPath 8000 Security Reference and Planning Guide*
- *HiPath 8000 SOAP/XML Subscriber Provisioning Interface 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 Installation and Upgrades Guide*
- *HiPath 8000 System Planning Guide*
- *HiPath 8000 Third Party Products Reference*
- *HiPath 8000 Traffic Measurements Guide*
- *HiPath 8000 Troubleshooting Guide*
- *HiPath 8000 Assistant API Description*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*
- *HiPath 8000 Assistant Framework, Service Documentation*
- *HiPath ProCenter, V7.0, Hardware Integration Guide*
- *HiPath ProCenter, V7.0, Installation and Maintenance Guide*
- *HiPath ProCenter, V7.0, Manager Guide*
- *HiPath ProCenter, V7.0, Planning and Design Guide*
- *optiClient 130 S, V4.0, Administrator Documentation and Operating Instructions*
- *optiPoint 150 S Administrator Manual*
- *optiPoint 150 S User 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*

1.1.6 Special Notices

If applicable, potentially dangerous situations are noted throughout this guide. The three alert methods are defined below:

DANGER	A danger notice calls attention to conditions that, if not avoided, will result in death or serious injury.
WARNING	A warning notice calls attention to conditions that, if not avoided, could result in death or serious injury.
Caution	A caution notice calls attention to conditions that, if not avoided, may damage or destroy hardware or software.

The symbol that appears with the alert indicates the type of dangerous situation to which the alert calls attention. The symbols are defined below:


Information/ Note


Electrical


Fire


Chemical


General


Weight


Electrostatic

1.2 Documentation Feedback

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

- **Title:** HiPath 8000 V2.2, Feature Description Guide
- **Order Number:** A31003-H8022-F100-2-7618

1.2.1 For U.S. 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.

1.2.2 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.

2 SIP Endpoint User Features

This chapter provides an overview of local user features that reside in the following Siemens SIP endpoints:

- optiPoint 410 S and optiPoint 420 S
- optiClient 130 S
- optiPoint WL 2 Professional S
- optiPoint 150 S

Other SIP telephones used with the HiPath 8000 function differently. Refer to the device's documentation for more information.

- Refer to the following for detailed information about these features:
  - *optiPoint 410/420 Advance S, V6.0, User Manual*
  - *optiPoint 410/420 Advance S, V6.0, Administrator Manual*
  - *optiClient 130 S, V4.0, Administrator Documentation and Operating Instructions*
  - *optiPoint 150 S Administrator Manual*
  - *optiPoint 150 S User Manual*
  - *optiPoint WL 2 Professional S, Operating Manual*
  - *optiPoint WL 2 Professional S, Administration Manual*
  - *HiPath Deployment Service Administration Manual*
- Refer to the following chapters for information about other features accessible to the user:
  - Chapter 3, "Keyset Telephone User Features"
  - Chapter 4, "HiPath 8000-Based Station Call Forwarding User Features"
  - Chapter 5, "Other User Features"

2.1 Endpoint Types Overview

2.1.1 optiPoint 410 S and optiPoint 420 S

The optiPoint 410 S and optiPoint 420 S telephones are modern multifunction SIP telephones. The following are brief descriptions of each:

- The optiPoint 410 S supports 19 function keys, 18 of which are programmable. It provides support for adapters and modules, including the self-labeling key module. Because it is fully compliant with the IEEE 802.3af PoE standard, it does not require an external power supply or midspan power hub.
- The optiPoint 420 S supports 18 function keys, 17 of which are programmable. Like the optiPoint 410 S, it provides support for adapters and modules and is fully compliant with the IEEE 802.3af PoE standard. In addition, it has self-labeling keys as an integral part of the telephone.

2.1.2 optiClient 130 S

The optiClient 130 S is a PC-based multimedia application that permits the user to administer and control voice connections. The optiClient 130 S, V4.0 and later, also supports keyset operations.

2.1.3 optiPoint 150 S

The optiPoint 150 S is a cost-effective entry model for voice over IP telephony. All features are accessed via function keys. It is designed for seamless integration into the HiPath 8000, and provides crucial features such as three-way calling, speakerphone, mute, redial, and simple traversal of UDP over NATs (STUN) protocol. It is simple to operate and easy to administer.

2.1.4 optiPoint WL 2 Professional S

The optiPoint WL 2 Professional S is a single-line WLAN handset. It also provides the following:

- Color display
- Handsfree and vibration ringer
- Web-based device configuration
- Software upgrade and download via PC or deployment service (DLS)
- Dedicated PC software for telephone book transfer and download of ringer tones

2.2 Endpoint Features Summary

Table 2-1 lists the local user features; it also indicates the Siemens SIP endpoints that support each.

- Where applicable, Table 2-1 also includes alternate names for the features.
- Table 2-1includes the keyset operations features described in Chapter 3, “Keyset Telephone User Features”. Depending on the endpoint, some of these features are endpoint-based, HiPath 8000-based, or a combination of the two. Refer to the specific table entries for more information.

Feature	optiPoint 410/420 S	optiClient 130 S	optiPoint 150 S	optiPoint WL 2 Professional S	Comments
Abbreviated dialing	•			•	
Access profiles				•	
Address book		•		•	See also *phone book*.
Advisory tones				•	
Alarm clock				•	
Alternate	•	•	•	•	See also *consultation hold.*
Anniversary				•	
Audible ringing on rollover lines		•			See also Section 3.1, “Audible Ringing on Rollover Lines”, on page 3-2. For optiPoint 410/420 S keyset telephones, this feature is HiPath 8000-based.
Automatic dialing	•	•	•		
Automatic recall on held calls	•	•			See also *call hold.*
Call deflect	•	•	•	•	See also *handover*.
Call forwarding—endpoint-based	•	•	•	•	

Table 2-1 Siemens SIP Endpoint Local Features (Sheet 1 of 7)

Feature	optiPoint 410/420 S	optiClient 130 S	optiPoint 150 S	optiPoint WL 2 Professional S	Comments
Call forwarding return—endpoint-based		•			
Call hold	•	•	•	•	See also *consultation hold*.
Call join	•	•		•	
Call journal/call list/call log	•	•	•	•	
Call refuse/call reject	•			•	
Call waiting (camp-on)	•	•	•	•	
Callback request	•	•		•	See also Section 5.2, “Automatic Callback”, on page 5-3.
Codec selection	•	•	•	•	optiPoint WL 2 Professional S SIP telephones support G.722 wideband codec (7 KHz).
Conference	•	•		•	See also *three-way calling.*
Consultation hold	•	•	•	•	
Contact directory/contact list		•		•	
Context dialing	•	•			
Country and language settings	•	•	•		See also *language settings*.
Dedicated dialing		•			See also *hotline*.
Delayed ringing		•			See also Section 3.2, “Delayed Ringing”, on page 3-3.
Deployment service (DLS)	•	•		•	
Dialing type options	•			•	
Direct station select (DSS) key		•			See also Section 3.3, “Direct Station Select Key”, on page 3-4. For optiPoint 410/420 S keyset telephones, this feature is HiPath 8000-based.
Directories		•		•	See also *address book* and *phone book*.

Table 2-1 Siemens SIP Endpoint Local Features (Sheet 2 of 7)

Feature	optiPoint 410/420 S	optiClient 130 S	optiPoint 150 S	optiPoint WL 2 Professional S	Comments
Directory list				•	
Do not disturb	•	•	•		
Do-not-interrupt dialing	•				
Drop call key		•		•	See also *Stop/Escape key*.
DTMF tone dialing	•	•	•	•	
Dynamic WBM addressing	•				
Easy answer				•	
easyCom communication circle		•			
Echo cancellation	•	•		•	
Elapsed time display	•	•	•	•	
Extended keypad		•			
Function key programming	•	•		•	
Handover		•		•	The optiPoint WL 2 Professional S supports handover between different access points.
Handset PIN				•	
Handsfree operation	•	•		•	
Headset support	•	•		•	
Hold, call	•	•	•	•	See *call hold.*
Hold, consultation	•	•	•	•	See *consultation hold.*
Hot keypad dialing	•				
Hotline	•	•			Sometimes known as *dedicated dialing.*
Hunt group support	•	•			See Chapter 7, “Other Group Features”.
Instant messaging with HiPath 8000		•			
IP Unity access	•			•	

Table 2-1 Siemens SIP Endpoint Local Features (Sheet 3 of 7)

Feature	optiPoint 410/420 S	optiClient 130 S	optiPoint 150 S	optiPoint WL 2 Professional S	Comments
Jitter buffer control	•	•		•	The optiPoint WL 2 Professional S supports adaptive jitter buffer control.
Join	•			•	See *call join.*
Keypad lock				•	
Keyset operation modes		•			See also Section 3.4, “Keyset Operation Modes”, on page 3-5. For optiPoint 410/ 420 S keyset telephones, this feature is HiPath 8000-based.
Keyset operation support	•	•			See Chapter 3, “Keyset Telephone User Features”.
Language settings			•	•	See also *country and language settings.*
Line focus	•				See also Section 3.5, “Line Focus”, on page 3-8.
Line key operation modes	•	•			See also Section 3.6, “Line Key Operation Modes”, on page 3-8.
Line reservation	•				See also Section 3.7, “Line Reservation”, on page 3-9.
LDAP access		•	•	•	
Local conference	•	•	•	•	Also known as *three-way calling.*
Locking	•				See also *phone lock*.
Mailbox	•			•	See also Section 18.9, “Message Waiting Indicator”, on page 18-3.
Manual hold		•			See also Section 3.8, “Manual Hold”, on page 3-10. For optiPoint 410/420 S keyset telephones, this feature is HiPath 8000-based.
Missed calls list	•	•	•	•	See also *call log*.
Mobility	•				

Table 2-1 Siemens SIP Endpoint Local Features (Sheet 4 of 7)

Feature	optiPoint 410/420 S	optiClient 130 S	optiPoint 150 S	optiPoint WL 2 Professional S	Comments
Multiline appearance	•	•			See also Section 3.9, “Multiline Appearance”, on page 3-11. For optiPoint 410/420 S keyset telephones, this feature requires configuration in the endpoint and in the HiPath 8000.
Multiline origination and transfer	•	•			See also Section 3.10, “Multiline Origination and Transfer”, on page 3-13.
Multiline preference	•	•			See also Section 3.11, “Multiline Preference”, on page 3-14.
Music on hold—endpoint-based	•	•		•	
Mute	•	•	•	•	
Night mode				•	
Notebook/notepad	•	•			
Onhook dialing	•	•	•	•	
Open listening	•	•	•	•	
optiGuide	•		•		
Outbound proxy support	•	•	•	•	
Outlook integration		•		•	
Phantom lines		•			See also Section 3.12, “Phantom Lines”, on page 3-15. For optiPoint 410/420 S keyset telephones, this feature is HiPath 8000-based.
Phone book			•	•	See also *address book* and *directories*.
Phone lock	•				
Pickup group support	•	•			See Chapter 7, “Other Group Features”.
Preview key	•	•			See also Section 3.13, “Preview”, on page 3-16.
Recall	•				See also *automatic recall on held calls.*

Table 2-1 Siemens SIP Endpoint Local Features (Sheet 5 of 7)

Feature	optiPoint 410/420 S	optiClient 130 S	optiPoint 150 S	optiPoint WL 2 Professional S	Comments
Redial	•		•	•	
Registration by name or number		•		•	
Repeat dialing	•	•		•	See also *call log*.
Repertory dialing	•	•			
Repertory dialing—temporarily shifted keys		•			
Ring tone, variable	•	•	•	•	See also *ringer tones*.
Ringer cutoff	•	•	•	•	
Ringer tones				•	See also *ring tone, variable*.
Room character configuration	•	•			
ScreenSaver manager		•			
Second call	•	•		•	See also *call waiting (camp-on).*
Selected dialing	•				
Session time support	•	•		•	
Setup	•			•	
Silence suppression	•	•	•	•	
SIP Stimulus and SIP Functional modules		•			
Speakerphone		•		•	
Speed dial	•			•	
Stop/Escape key	•			•	See also *drop call key.*
Third-party call control	•	•			
Three-way calling	•	•	•	•	Also known as *local conference.*
Time display	•	•		•	See also *elapsed time display.*
Toggle/connect			•	•	
Tones and cadences	•	•		•	See *ring tone, variable.*

Table 2-1 Siemens SIP Endpoint Local Features (Sheet 6 of 7)

Feature	optiPoint 410/420 S	optiClient 130 S	optiPoint 150 S	optiPoint WL 2 Professional S	Comments
Transfer, blind	•	•	•	•	See also Section 5.28, “Transfer”, on page 5-32.
Transfer, unscreened	•	•	•	•	See also Section 5.28, “Transfer”, on page 5-32.
Transfer, with third-party consultation	•	•	•	•	See also Section 5.28, “Transfer”, on page 5-32.
USB support		•		•	A standard memory stick can be used to back up and restore personal data.
Vibration alert				•	
Video camera support		•			
Video viewer		•			
VIP calls				•	
Visual indicators for line and feature key status	•	•			See also Section 3.14, “Visual Indicators for Line and Feature Key Status”, on page 3-17.
VLAN ID via DHCP	•		•	•	
Voice dialing				•	
Volume control	•	•	•	•	
Warmline	•				
Web-based management tool	•		•	•	
Web browser window		•			
Xpressions access	•			•	

Table 2-1 Siemens SIP Endpoint Local Features (Sheet 7 of 7)

3 Keyset Telephone User Features

This chapter describes features specific to keyset operations. A *keyset telephone* is configured with a *primary line* (also known as a *prime line*), which is the main DN of a keyset telephone associated with the device. A keyset telephone can also have additional secondary and phantom line appearances, both of which are defined in this chapter.

Any of the following SIP endpoints can be configured as keysets:

- optiPoint 410 S and optiPoint 420 S
- optiClient 130 S, V4.0 and later

The keyset operations features provide multiple line capability, and other associated functions, for a SIP telephone configured as a keyset. Keysets are sometimes known as *multiline telephones.*

Refer to the following for information about administration practices associated with these functions and features:

- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*

Refer to the *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide* for more information about configuration of executive-assistant arrangements.

Refer to the following for more information to operate these features:

- *optiPoint 410/420 Advance S, V6.0, User Manual*
- *optiClient 130 S, V4.0, Administrator Documentation and Operating Instructions*

3.1 Audible Ringing on Rollover Lines

3.1.1 Definition

The audible ringing on rollover lines feature permits lines to audibly signal new incoming calls while the user is active on the keyset. This feature is also known as *rollover ringing*.

3.1.2 Functional Operation

For the optiClient 130 S, rollover ringing is configured in the endpoint. Refer to the *optiClient 130 S, V4.0, Administrator Documentation and Operating Instructions* for more information.

For optiPoint 410/420 S keyset telephones, the system administrator specifies the following:

- Whether the ringer option is enabled. Rollover ringing only applies to lines that have this option enabled—that is, rollover ringing only takes place is the applicable line otherwise rings when it is idle.
- One of the following rollover ring options for each keyset:
  - No ring when active on the telephone
  - Alert ring when active on the telephone
  - Alert beep when active on the telephone
  - Standard ring when active on the telephone

  The selected option applies to all line appearances on the keyset. The user controls the volume of the rollover ring.

The rollover ring option is used by the telephone when any line appearance other than the one in use is in the ringing state. When the telephone is idle, normal ringing is applied.

If the user at an idle telephone answers one incoming call on a line appearance while other lines are still ringing, the ringing changes from normal ringing to rollover ringing. Likewise, if the user releases a call and returns the phone to idle while rollover ringing is active, it changes to normal ringing.

3.1.3 Guidelines for Implementation and Use

- **optiPoint 410/420 S keyset telephone**: If the loudspeaker is in use:
  - Alert ring reverts to alert beep. If the user is in open listening mode, the beep is applied through the handset; otherwise the beep is applied through the loudspeaker.
  - Standard ring reverts to no ring.
- Rollover ring is not applied:
  - For lines that are set for alerting only. These lines do not ring even if the phone is idle.
  - When the telephone's ringer is turned off. Refer to the applicable user manual.

3.2 Delayed Ringing

3.2.1 Definition

The delayed ringing feature provides the capability to provision each keyset line key with an option to delay audible ringing when a call is presented to the line; the associated incoming call is not affected. An immediate ring option provides the capability to temporarily overrides delayed ringing for all lines on the endpoint configured for ringing.

This feature is particularly useful for executive-assistant arrangements because it allows the assistant to answer calls for the executive's secondary line appearance before the executive hears the line ringing.

- Refer to Section 3.9, "Multiline Appearance", on page 3-11 for information about ringing options for each line.
- Refer to Section 3.14, "Visual Indicators for Line and Feature Key Status", on page 3-17 for more information about line key status indicators.

3.2.2 Functional Operation

Depending on the endpoint, either the endpoint administrator or user:

- Assigns delayed ringing to a line appearance and defines the duration of the delay before audible alerting.
  - **optiPoint 410/420 S keyset telephones:** The default is 0 seconds (such that the feature is not active); the upper limit is approximately one hour.
  - **optiClient 130 S**: The delay is fixed at 5 seconds.

  Refer to the applicable user manual for more information.

- **optiPoint 410/420 S keyset telephones:** Assigns the Immediate Ring feature key to the device.

When a call is presented to a line provisioned for delayed ringing, the associated line key LED flashes to indicate that the call is present. Upon timeout of the delay ring timer, the device begins to audibly alert (ring), and the associated incoming call display is presented. For the optiClient 130 S, the display is *not* delayed.

To override delayed ringing, the user can also activate and deactivate immediate ringing by pressing the Immediate Ring key. The key's associated LED lights to indicate when it is active, and `Immediate Ring Activated` or `Immediate Ring Deactivated` appears in the display as applicable.

3.3 Direct Station Select Key

3.3.1 Definition

The direct station select (DSS) key feature is available for optiPoint 410/420 S keyset telephones. It provides a user access to multiple functions for a given internal DN by using a single key (*DSS key*) with associated status indication. The DSS key gives status of a DN, makes a call to the DN, and answers a call on behalf of the associated DSS DN.

Up to 10 DSS keys can be assigned to a given DN. Up to nine DSS keys can be assigned to a single device.

3.3.2 Functional Operation

For the optiClient 130 S, DSS keys are configured in the endpoint. Refer to the *optiClient 130 S, V4.0, Administrator Documentation and Operating Instructions* for more information.

For optiPoint 410/420 S keyset telephones, the system administrator programs DSS destinations. Users cannot program them locally at their telephones because the administrator must create a line key to allow DSS operation.

The telephone does not audibly alert; instead, the DSS LED provides the following displays:

- **Off**: The DSS line is idle.
- **On**: The DSS line has a call in progress or on hold.
- **Flashing**: The line is ringing.

The DSS LED reflects the status of the line (DN) programmed for the DSS key, *not* the status of the user associated with the prime DN device.

The user presses the DSS key to call the party associated with the key.

A blinking DSS key indicates an incoming call for another user with the same DSS key appearance. When the user presses the key, the call is forwarded to the prime line, and the user is connected to the call. The keyset rejects the attempt to pickup if the prime line is remotely busy.

3.3.3 Networking

DSS key operation does not function across a network.

3.3.4 Guidelines for Implementation and Use

The DSS feature can be used on a keyset telephone that has its prime line configured as part of a hunt group. Refer to Section 7.2, “Hunt Group”, on page 7-3.

3.4 Keyset Operation Modes

3.4.1 Definition

The keyset operation modes feature permits the system administrator to specify whether a keyset telephone uses the data of the primary line or the data of the line in use for call origination and features. For optiPoint 410/420 S keyset telephones, this feature is controlled via the HiPath 8000; for the optiClient 130 S, this feature is controlled via the endpoint.

These designations are useful for executive and assistant arrangements. For example, if an assistant places calls on behalf of an executive, the assistant’s telephone can have a line appearance of the executive. If marked for *line-based operation* as described in Section 3.4.2.2, “Line-Based Operation”, on page 3-7, the assistant can easily place such calls, and the executive can subsequently retrieve them when the assistant successfully reaches the person the executive seeks.

3.4.2 Functional Operation

For the optiClient 130 S, keyset operation modes are configured in the endpoint. Refer to the *optiClient 130 S, V4.0, Administrator Documentation and Operating Instructions* for more information.

For optiPoint 410/420 S keyset telephones, keyset operation modes are usually evaluated during the provisioning of the HiPath 8000 environment and are applicable to all line types, including phantom lines.

For each line of each keyset, the system administrator configures the keyset operation mode as follows:

- **Device-based operation:** This mode is the default. It uses the data of the primary line for call origination and features.
- **Line-based operation:** This mode uses the data of the line currently in use for call origination and features.

For call termination, the calling party is sent displayable identification information based on the line or device involved in terminating the call.

When a specific device answers a call, the identification might differ from the identification provided when the call was alerting all the devices sharing the applicable line.

3.4.2.1 Device-Based Operation

When the keyset user originates a call, the configured data of the primary line (its configured name and DN) is referenced in caller and called ID services. When the user originates a call, the following takes place:

- **If the call is originated on the primary line:** Services provisioned on the primary DN are initiated if they do not require a feature access code to operate. Some examples are transfer, CSTA support, and calling name.
- **If the call is originated on a secondary line:** Services provisioned on the primary DN are initiated if they do not require a feature access code to operate. Additionally, a subset of services provisioned on the secondary DN are initiated. These services are line-based and do require a feature access code to operate—for example, CSTA support.

The following HiPath 8000 features always use the primary line's configured data regardless of the keyset operation mode:

- **Called party name and number upon alerting:** Refer to Section 5.4, “Caller Identity Service”, on page 5-4.

- **HiPath 8000-based station speed calling:** Refer to Section 5.25, “Station Speed Calling—HiPath 8000-Based”, on page 5-29.

The following HiPath 8000 features use the primary line's configured data if the telephone is configured for device-based operation:

- **Calling party name and number upon alerting or answer:** Refer to Section 5.4, “Caller Identity Service”, on page 5-4.
- **Called/connected party name and number upon answer:** Refer to Section 5.4, “Caller Identity Service”, on page 5-4
- **Call transfer if provisioned on the primary line that originates the operation:** Refer to Section 5.28, “Transfer”, on page 5-32.

3.4.2.2 Line-Based Operation

When the keyset user originates a call, the configured data of the selected line (the primary or secondary DN’s name and number) is referenced in caller and called ID services. When the user originates a call with a secondary line, all services configured to be provisioned on the DN of the secondary line are initiated if they do not require a feature access code to operate.

In addition to ringing and incoming call termination, the following HiPath 8000 features always operate with the selected line regardless of the keyset operation mode:

- **Immediate recall from consultation hold:** Refer to the applicable user manual.
- **Manual hold, including recall:** Refer to Section 3.8, “Manual Hold”, on page 3-10.
- **Station call forwarding—all calls:** Refer to Section 4.1, “Call Forwarding, Station—All Calls”, on page 4-2.
- **Customer-originated trace:** Refer to Section 5.12, “Customer-Originated Trace”, on page 5-13.
- **Toll and call restrictions**: Refer to Section 5.27, “Toll and Call Restrictions”, on page 5-31.
- **Hunt group:** Refer to Section 7.2, “Hunt Group”, on page 7-3.
- **CSTA**: Refer to Section 17.1, “CSTA Protocol Interface”, on page 17-2.

The following HiPath 8000 features operate with the selected line only if the telephone is configured for line-based operation:

- **Calling party name and number upon alerting or answer:** Refer to Section 5.4, “Caller Identity Service”, on page 5-4.
- **Called/connected party name and number upon answer:** Refer to Section 5.4, “Caller Identity Service”, on page 5-4.

- **Call transfer if provisioned on the line that originates the operation:** Refer to Section 5.28, “Transfer”, on page 5-32.

3.4.3 CDR

When a keyset user initiates a call from a line configured for line-based operation, the HiPath 8000 records the line used and the device from where the call was initiated.

3.5 Line Focus

The line focus feature ensures that the optiPoint 410/420 S display contains the appropriate information, depending on the keyset line currently in use. This feature is controlled via the endpoint.

A keyset line has the *focus* when the display contains information pertaining to it. When a call is connected, that line has the focus. When the call clears, focus is applied to the next suitable line. When a line is alerting, focus is determined by terminating line preferences. Refer to Section 3.11, “Multiline Preference”, on page 3-14 for more information.

Call handling actions (such as placing calls on manual hold) also impact focus. If there is no suitable line, no line has the focus, and the display returns to idle mode.

The menu and function key actions apply to the line with the focus. However, in the case of a pop-up display, any functions that impact the audio path (such as hookswitch or loudspeaker actions) still apply to the currently active line.

When a line key has the focus, its associated LED flutters. Refer to Section 3.14, “Visual Indicators for Line and Feature Key Status”, on page 3-17 for more information.

This feature is not applicable to the optiClient 130 S because the user can:

- Display the state of any line at any time
- Display the state of all lines simultaneously

Refer to the *optiClient 130 S, V4.0, Administrator Documentation and Operating Instructions* for more information.

3.6 Line Key Operation Modes

3.6.1 Definition

The line key operation modes feature allows a keyset user to automatically place an active line on manual hold. Refer to Section 3.8, “Manual Hold”, on page 3-10.

The optiPoint 410/420 S keyset telephones also support a configurable option to either place the call on manual hold or to release it when the user is active on one line and selects the same line or a different line.

This feature is controlled via the endpoint.

3.6.2 Functional Operation

A keyset user can automatically hold the call of the active line as follows:

- **Active line key**: When the user presses the line key for the active line, the call is automatically placed on manual hold. The telephone can become idle or can start ringing if another line was alerting at the time the line was placed on hold.

  Similarly, if the user selects an alerting line while active on another line, the active line's call is placed on manual hold.

- **Inactive line key:** When the user presses the line key of an inactive line, the active line call is automatically placed on manual hold and the user is connected to the previously inactive line.

For an optiPoint 410/420 S keyset telephone, the telephone can instead be configured to release the call when another line is selected. The default setting is to place the call on manual hold.

3.6.3 CDR

Based on system configuration upon retrieval of a call, the billing for the remainder of the call is assigned to the primary line of the station answering the recall.

3.7 Line Reservation

3.7.1 Definition

The line reservation feature is available for optiPoint 410/420 S keyset telephones. It permits a keyset user to reserve a line when dialing a destination or selecting a line, so that:

- Incoming calls cannot interfere with outgoing call initiation.
- Two keysets with the same line appearance cannot use the same line and attempt to dial simultaneously.

3.7.2 Functional Operation

The keyset telephone automatically reserves a line whenever the user is being prompted for a destination address and hears dial tone. The line key LED indicates this reserved state. One line can be reserved at a time on a given keyset.

The keyset cancels the reservation after a preconfigured period determined by the reservation timer. The server also runs a timer so it can force the line to be released if reserved for an excessively long period. Alternatively, the server may permit the administrator to cancel a reservation.

3.8 Manual Hold

3.8.1 Definition

The manual hold feature allows a keyset user to place the call on the active line in a waiting position. The keyset user can then go onhook without losing the call, and can place or answer another calls on a different line key. Refer also to Section 3.6, “Line Key Operation Modes”, on page 3-8.

The held call can be retrieved by other keysets sharing the line appearance, assuming they support the required manual hold signaling. A hold ringback timer ensures that the caller is not left on hold indefinitely.

Siemens SIP endpoints support the SIP signaling event package that supports this feature. Other SIP telephones that do not support this package cannot signal a call on manual hold. As a result, the call is treated as a consultation hold, which requires that the same station user retrieve the call from consultation hold.

A digital feature telephone (DFT), which is a telephone with no line keys, does not have access to the manual hold feature. Holding of a connection is via the call hold feature. Refer to the applicable user manual.

3.8.2 Functional Operation

Depending on the configuration of an optiPoint 410 S or optiPoint 420 S keyset telephone, pressing the line key can release a call instead of placing it on manual hold. Refer to Section 3.6, “Line Key Operation Modes”, on page 3-8.

A keyset user can press the line key, press the Hold key, or use the display of the active line to place that call on manual hold. After doing so:

- The line key LED shows the hold status on all keysets with that line appearance.

- The user can hang up and originate or answer a call on another line on that keyset.
- Any user with that line appearance can press the line key and retrieve the held call.
- A hold ringback timer is started. If the timer expires, the held call is presented as an alerting call to all keysets sharing that line. Each line has its own configurable timer.

When a call is retrieved from hold, the parties receive the following displays:

- The retrieving party's display contains the name and number of the retrieved party if it is available for presentation.
- The retrieved party's display contains the name and number of the retrieving party if it is available for presentation.

Manual hold is available for simple two-party calls, but not for consultations or conferences.

3.9 Multiline Appearance

3.9.1 Definition

The multiline appearance feature allows for multiple lines to be assigned to a keyset and for a line to be assigned to multiple keysets. This feature is particularly useful for executive-assistant arrangements.

For optiPoint 410/420 S keyset telephones, this feature requires configuration in the HiPath 8000 and in the endpoint; for the optiClient 130 S, this feature is controlled via the endpoint.

Each keyset is assigned a primary line, also known as the *prime line*, and can be assigned up to a total of 10 lines. The primary line is the DN for that keyset. The primary line and each secondary or phantom line are assigned to separate line keys. A keyset *cannot* have a line appearance of a DFT.

- **Private**: A line (primary or phantom) that appears on only one keyset.

A *phantom line* is a line that is not assigned as a primary line on any device. See Section 3.12, "Phantom Lines", on page 3-15 for more information.

- **Shared**: A line (secondary or phantom) that is shared between keysets.

A *secondary line* is a shared appearance of a primary line on a keyset, other than the keyset that is configured with the prime line.

3.9.2 Functional Operation

For the optiClient 130 S, multiline appearance is configured in the endpoint. Refer to the *optiClient 130 S, V4.0, Administrator Documentation and Operating Instructions* for more information.

For optiPoint 410/420 S keyset telephones, the system administrator can assign one of the following ring preferences to each line appearance:

- **Ring**: The line always audibly alerts when an incoming call is presented and calling party information appears on the display.
- **No ring:** The associated line key LED indicates an incoming call, but no audible alerting occurs and no calling party information appears on the display.
- **Delay ring:** The line audibly alerts after a configured delay and calling party information appears on the display. Refer to Section 3.2, “Delayed Ringing”, on page 3-3.

Calls are directed as follows:

- Calls to the primary line of a keyset are simultaneously directed to all other keysets that have that line configured as a secondary line.
- Calls to a phantom line are simultaneously directed to all other keysets that have that line configured as a shared phantom line.

The user can press the line key associated with a line at any keyset to originate, answer, hold, and retrieve calls. The LED for each line key indicates the status of the associated DN and the action of the telephone when a line key is pressed.

3.9.3 Networking

All line appearances must reside on the same switch and within the same IP addressing domain.

3.9.4 CDR

The HiPath 8000 records the device and line used.

3.10 Multiline Origination and Transfer

3.10.1 Definition

The multiline origination and transfer feature provides the capability to:

- Originate or answer calls at any line appearance at any keyset
- Transfer calls via consultation transfer
- Transfer calls via manual hold

This feature is controlled via the endpoint.

3.10.2 Functional Operation

A keyset user can originate and answer calls manually and automatically. To originate calls:

- A user can manually select a line by pressing a line key before going off-hook, pressing the speaker key, or using onhook dialing to originate a call.
- A line may be automatically selected if the idle line preference is active at the time the user goes off-hook, presses the speaker key, or uses onhook dialing to originate a call.

To answer calls:

- A user can manually select a line by pressing a line key before gong off-hook, or by pressing the speaker key, to answer a call.
- A line may be automatically selected if the ringing line preference is active at the time the user goes off-hook, or presses the speaker key, to answer a call.

A keyset user can use the transfer capabilities associated with this feature as follows:

- **Call transfer via consultation transfer:** Transfer can be accomplished by placing the call on consultation hold and consulting with a second keyset using the display. The user can then transfer the held party by going onhook after the consulted party answers.

  Refer to Section 5.28, “Transfer”, on page 5-32 for more information about transfers with third-party consultation.

- **Call transfer via manual hold:** Transfer can be accomplished by placing the call on manual hold and selecting a different line and consulting with a second keyset (having the same line appearance of the held line). The second party can then retrieve the call from manual hold if no restrictions exist.

  Refer to Section 3.8, “Manual Hold”, on page 3-10 for more information.

3.11 Multiline Preference

3.11.1 Definition

The multiline preference feature:

- Allows a keyset to automatically select which line it uses when the user originates or answers a call.
- Lets a user override the automatic selection of a line and manually select the line to use.

This feature is controlled via the endpoint.

3.11.2 Functional Operation

The multiline preferences for terminating calls are as follows:

- **Ringing line preference:** The line in the alerting or audible ringing state is automatically selected when the user goes offhook. In the case of multiple lines alerting or ringing the lines are selected on the one that has been alerting the longest. When a terminating call exists, the terminating line preference takes priority over originating line preference.
- **Ringing line preference with preference for prime line:** The line in the alerting or audible ringing state is automatically selected when the user goes offhook. However, if the prime line is alerting, it is given priority.
- **Incoming line preference:** The earliest line to start audible ringing is selected, or else the earliest alerting (ringing suppression ignored) line is selected.
- **Incoming line preference with preference for prime line:** The earliest line to start audible ringing is selected, or else the earliest alerting (ringing suppression ignored) line is selected. However, if the prime line is alerting, it is given priority.
- **No preference:** The user manually selects a line by pressing its line key before going offhook, or by pressing the speaker key, to answer a call. Manual line selection overrides automatic line preferences.

The multiline preferences for originating calls are as follows:

- **Idle line preference:** This is the default. The line preference order, or *rank*, is used to select the line. The highest ranked idle line is selected.
- **Prime line preference:** The prime line is selected.
- **Last line preference:** The last line used (originating or terminating) is selected.
- **No preference:** The user manually selects a line by pressing its line key before going offhook, or by pressing the speaker key, to originate a call. Manual line selection overrides automatic line preferences.

Automatic line selection occurs whenever an outgoing call commences and a line has not been pre-selected. Automatic line selection also occurs when a line needs to be reserved for dialling and a line as not been pre-selected— for example, when entering a digit via the keypad while on-hook and idle.

Ringing line preference is the default.

3.11.3 Guidelines for Implementation and Use

If an optiPoint 410/420 S keyset telephone is configured for both hot keypad dialing and no originating line preference, the user receives the following notifications:

- An audible beep
- A display message that prompts the user to select a line before dialing begins

Refer to the *optiPoint 410/420 Advance S, V6.0, User Manual* for more information about hot keypad dialing.

3.12 Phantom Lines

3.12.1 Definition

A phantom line is identical to a normal line in all respects, except that a phantom line is not assigned to any device as a primary line. This line type can appear as a private line on one keyset or as a shared secondary line on two or more keysets. For optiPoint 410/420 S keyset telephones, this feature is controlled via the HiPath 8000; for the optiClient 130 S, this feature is controlled via the endpoint.

Phantom lines are particularly useful as rollover lines. For example, sales representatives can have the system administrator configure the primary line to roll over to a phantom line. This configuration is beneficial because when the representative speaks to the second party, there is great flexibility in holding, transferring, or redirecting the call.

3.12.2 Functional Operation

The function of a phantom line is identical to a normal line in all respects. Its DN can be called, and the line can be answered, held, used to originate calls, and in all other operations used in the same manner as other line types.

3.12.3 CDR

The HiPath 8000 records the device and line used.

3.13 Preview

3.13.1 Definition

The preview feature permits a keyset user to view display information associated with certain lines without answering the call or retrieving it from hold.

This feature is useful to anyone who handles a number of simultaneous calls because it provides the ability to make an intelligent choice of which calls to answer first and to identify high-priority callers.

This feature is controlled via the endpoint.

3.13.2 Functional Operation

The endpoint administrator:

- Assigns the Preview feature key to the device.
- Defines the value of the preview timer, which determines how long the preview information appears on the display. The possible time interval is from 2 to 60 seconds, with a default of 8 seconds.

Previewing can take place while the user is active on a call or while the keyset is idle. To activate preview mode, the user presses the Preview key. After it is active, the user can press any line key to view caller information associated with the line—for example:

- Alerting lines
- The currently connected party, regardless of whether the call was incoming or outgoing
- Parties on manual hold or recalling from hold

The type of preview information provided depends on how the HiPath 8000 administrator provisions the line's ring preference. Refer also to Section 3.2, "Delayed Ringing", on page 3-3 and Section 3.9, "Multiline Appearance", on page 3-11.

- **Immediate or delayed ring:** Calling identity information and LED indication is provided.
- **No ring:** LED indication is provided.

The information remains on the display for the interval specified by the preview timer.

To deactivate preview mode, the user can do either of the following:

- Press the Preview key again.
- Become active in a call. For example:
  - Press the key associated with the line currently being previewed.

– Go onhook or offhook as appropriate.

– Answer a ringing call.

3.14 Visual Indicators for Line and Feature Key Status

3.14.1 Definition

The visual indicator features allow the keyset user to view the various states (for example, ringing, hold, consult) of a line via its associated LED and to view the various states of a feature key (for example, call pickup group) via its associated LED. This feature is controlled via the endpoint.

If the telephone is not an optiPoint 410/420 S or optiClient 130 S, the user cannot see the status of shared lines other than new alerting calls.

3.14.2 Functional Operation

Each line key (primary, secondary, phantom) on a keyset has a corresponding visual indicator (LED) to indicate the status of that line. Table 3-1 on page 3-18 lists and describes the line status LED indicators.

The optiClient 130 S also provides an interface which displays the state of all lines via graphical icons. Refer to the *optiClient 130 S, V4.0, Administrator Documentation and Operating Instructions* for more information.

Line Status	Line Type	LED State	Flash Rate	Comments
Idle	Primary or secondary	Off	n/a	
Offhook/dial/ busy	Primary	Flutter -or- On	50 ms on, 50 ms off	This LED state is applicable to the line with the focus (refer to Section 3.5, “Line Focus”, on page 3-8.
	Secondary	On	n/a	This indication is given on other appearances of the active line.
Ringing/ alerting	Primary or secondary	Flash	500 ms on, 500 ms off	
Manual hold	Primary or secondary	Wink	450 ms on, 50 ms off	
Consultation hold	Primary	Flutter -or- On	50 ms on, 50 ms off	• This LED state is applicable to the line with the focus (refer to Section 3.5, “Line Focus”, on page 3-8). • The LED changes only at the holding telephone; there is no change for shared views of the same line.
	Secondary	On	n/a	This indication is given on other appearances of the active line.
Station call forwarding—all calls	Primary or secondary	Blink	50 ms on, 450 ms off	This indication is given when the line becomes idle.

Table 3-1 Line Status LED Indicators

Feature keys also have LEDs associated with them to indicate, where applicable, that the feature is active.

4 HiPath 8000-Based Station Call Forwarding User Features

This chapter describes the station call forwarding features that reside in the HiPath 8000. These features are accessible via feature access code; the user can also assign a frequently-used feature to a feature key or repdial key.

Siemens SIP endpoints also have local call forwarding features. Refer to the applicable user manual for information about those features.

Refer to the following for information about administration practices associated with these functions and features:

- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*

Refer to the following for more information to operate these features:

- *optiPoint 410/420 Advance S, V6.0, User Manual*
- *optiClient 130 S, V4.0, Administrator Documentation and Operating Instructions*
- *optiPoint 150 S User Manual*
- *optiPoint WL 2 Professional S, Operating Manual*

4.1 Call Forwarding, Station—All Calls

Siemens SIP endpoints also provide the capability to locally configure and control unconditional call forwarding. However:

- **It is strongly recommended that the endpoint-based call forwarding features not be used simultaneously with other station call forwarding features that reside in the HiPath 8000.**
- It is preferable to use the endpoint-based call forwarding features if the user requires greater control of call forwarding.

4.1.1 Definition

The HiPath 8000-based station call forwarding—all calls feature, sometimes known as *call forwarding variable* or *call forwarding unconditional*, provides the capability to redirect calls intended for the subscriber to another destination. The subscriber activates and deactivates the feature and specifies the forwarding destination.

This feature is also available on a usage-sensitive basis, and is sometimes known as *usage-sensitive call forwarding variable*. Although it is technically a separate feature, it operates in the same manner as station call forwarding—all calls. The only difference is the manner in which it is billed.

This feature can be provisioned at the business group level with a denied option at the subscriber level.

- The remote activation call forwarding (RACF) feature provides the subscriber the capability to manage the station call forwarding—all calls from a locations other than the subscriber's station. Refer to Section 4.7, "Call Forwarding, Station—Remote Activation", on page 4-9.
- Call forwarding—return is an inherent capability of station call forwarding—all calls; it allows the forwarded-to station to call the forwarding station and override (ignore) the forwarding. Refer to Section 4.9, "Call Forwarding—Return", on page 4-10.
- The time-of-day forwarding feature can provide a scheduling capability in conjunction with this feature. Refer to Section 4.11, "Call Forwarding, Station—Time-of-Day", on page 4-11.
- The station call forwarding—voice mail (CFVM) feature provides message waiting indication for this feature. Refer to Section 4.11, "Call Forwarding, Station—Time-of-Day", on page 4-11.

4.1.2 Functional Operation

The subscriber activates the station call forwarding—all calls feature as follows:

1. The subscriber goes off-hook, receives a dial tone, and enters *72. The subscriber hears a recall dial tone.
2. The subscriber dials the DN of the remote station to which calls are to be forwarded. Depending on the system configuration, the HiPath 8000 might provide a confirmation tone at this point to acknowledge receiving the dialed sequence.
3. If the subscriber has the courtesy call option, the system automatically places a call to the forwarding destination. Refer to Section 4.3, “Call Forwarding, Station—Courtesy Call”, on page 4-5.

When a subscriber has the station call forwarding—all calls feature activated and receives a call, a reminder ring (approximately 0.5 seconds long) indicates that a call was received and forwarded. The subscriber cannot answer calls while the feature is active, but can originate calls as usual.

The following are additional notifications for optiPoint 410 S or optiPoint 420 S keyset telephones:

- The message `Calls forwarded` appears on the display.
- If configured to do so, the associated line key LED winks. Refer also to Section 3.14, “Visual Indicators for Line and Feature Key Status”, on page 3-17.

Table 4-1 lists and describes the displays associated with this feature for the calling party, forwarding party, and forwarded-to party.

Forwarding Status	Calling Party (Party A) Display	Forwarding Party (Party B) Display	Forwarded-To Party (Party C) Display
Party A calls party B; reminder ring provided to party B	Party B’s name and number	Party A’s name and number	—
Call forwarded to party C; party C is ringing	Party C’s name and number	—	Party A’s name and number
Party C answers	Party C’s name and number	—	Party A’s name and number

Table 4-1 Station Call Forwarding—All Calls: Associated Displays

To deactivate the station call forwarding—all calls feature, the subscriber goes off-hook, receives dial tone, and dials *73. The HiPath 8000 provides a confirmation tone to acknowledge the deactivation, and then provides dial tone.

4.2 Call Forwarding, Station—Busy Line

Siemens SIP endpoints also provide the capability to locally configure and control call forwarding on busy. However:

- **It is strongly recommended that the endpoint-based call forwarding features *not* be used simultaneously with other station call forwarding features that reside in the HiPath 8000.**
- It is preferable to use the endpoint-based call forwarding features if the user requires greater control of call forwarding.

4.2.1 Definition

The HiPath 8000-based station call forwarding—busy line (CFBL) feature, sometimes known as *call forwarding busy*, provides the capability to redirect calls intended for the subscriber to another destination when the subscriber's station is in use. The subscriber activates and deactivates the feature, and specifies the forwarding destination.

This feature can be provisioned at the business group level with a denied option at the subscriber level.

- The system administrator can also configure the station CFBL feature such that when the subscriber activates it, calls automatically route to a fixed destination. Refer to Section 4.6, "Call Forwarding, Station—Fixed", on page 4-8.
- Call forwarding—return is an inherent capability of station CFBL; it allows the forwarded-to station to call the forwarding station and override (ignore) the forwarding. Refer to Section 4.9, "Call Forwarding—Return", on page 4-10.
- The time-of-day forwarding feature can provide a scheduling capability in conjunction with this feature. Refer to Section 4.11, "Call Forwarding, Station—Time-of-Day", on page 4-11.
- The station call forwarding—voice mail (CFVM) feature provides message waiting indication for this feature. Refer to Section 4.12, "Call Forwarding, Station—Voice Mail", on page 4-13.

4.2.2 Functional Operation

The subscriber activates the station CFBL feature as follows:

1. The subscriber goes off-hook, receives a dial tone, and enters *90. The subscriber hears a recall dial tone.
2. The subscriber dials the DN of the remote station to which calls are to be forwarded. Depending on the system configuration, the HiPath 8000 might provide a confirmation tone at this point to acknowledge receiving the dialed sequence.
3. If the subscriber has the courtesy call option, the system automatically places a call to the forwarding destination. Refer to Section 4.3, “Call Forwarding, Station—Courtesy Call”, on page 4-5.

When a caller dials the DN of a station that has the station CFBL feature active, the HiPath 8000 determine if the station is in use. If the station is in use, the HiPath 8000 routes the call to the forwarding destination. Otherwise, the subscriber is alerted to the incoming call in the usual manner.

To deactivates the station CFBL feature, the subscriber goes off-hook, receives dial tone, and dials *91. The HiPath 8000 provides a confirmation tone to acknowledge the deactivation, and then provides dial tone.

4.3 Call Forwarding, Station—Courtesy Call

4.3.1 Definition

The station call forwarding—courtesy call feature provides the capability to place a call to the specified forwarding destination when the subscriber activates any of the following features:

- Station call forwarding—all calls
- Station CFBL
- Station CFDA

A courtesy call is *not* provided when these call forwarding features are invoked due to time-of-day forwarding. Refer to Section 4.11, “Call Forwarding, Station—Time-of-Day”, on page 4-11.

4.3.2 Functional Operation

The system administrator determines if the courtesy call option is active for each subscriber.

After a subscriber dials the DN of the forwarding destination, one of the following events take place:

- **If the remote station is idle:** The HiPath 8000 rings it. When the remote station answers, a conversation path is established between the subscriber and the remote station so the forwarded-to party can be alerted that calls will be forwarded to his or her number.
- **If the remote station does not answer or is busy:** The subscriber is notified that the activation attempt failed.The subscriber can activate the feature by repeating the activation procedure within a 2-minute time period that starts after the subscriber hangs up. If this is done, the subscriber hears a confirmation tone followed by dial tone. No attempt is made to alert the remote station on the second activation. If the second request is made after the 2-minute timeout period, it is processed as a new request.

4.4 Call Forwarding, Station—Don't Answer

Siemens SIP endpoints also provide the capability to locally configure and control call forwarding on no answer. However:

- **It is strongly recommended that the endpoint-based call forwarding features *not* be used simultaneously with other station call forwarding features that reside in the HiPath 8000.**
- It is preferable to use the endpoint-based call forwarding features if the user requires greater control of call forwarding.

4.4.1 Definition

The HiPath 8000-based station call forwarding don't answer (CFDA) feature, sometimes known as *call forwarding no reply*, provides the capability to redirect calls intended for the subscriber to another destination if the call is not answered after a preset number of rings. The subscriber activates and deactivates the feature and specifies the forwarding destination.

This feature can be provisioned at the business group level with a denied option at the subscriber level.

- If a subscriber is not currently registered, calls to that subscriber are diverted to the station CFDA forward-to DN.
- The system administrator can also configure the station CFDA feature such that when the subscriber activates it, calls automatically route to a fixed destination. Refer to Section 4.6, "Call Forwarding, Station—Fixed", on page 4-8.
- Call forwarding—return is an inherent capability of station CFDA; it allows the forwarded-to station to call the forwarding station and override (ignore) the forwarding. Refer to Section 4.9, "Call Forwarding—Return", on page 4-10.
- The time-of-day forwarding feature can provide a scheduling capability in conjunction with this feature. Refer to Section 4.11, "Call Forwarding, Station—Time-of-Day", on page 4-11.
- The station call forwarding—voice mail (CFVM) feature provides message waiting indication for this feature. Refer to Section 4.12, "Call Forwarding, Station—Voice Mail", on page 4-13.

4.4.2 Functional Operation

The system administrator defines the value for the number of rings before forwarding takes place.

The subscriber activates the station CFDA feature as follows:

1. The subscriber goes off-hook, receives a dial tone, and enters *92. The subscriber hears a recall dial tone.
2. The subscriber dials the DN of the remote station to which calls are to be forwarded. Depending on the system configuration, the HiPath 8000 might provide a confirmation tone at this point to acknowledge receiving the dialed sequence.
3. If the subscriber has the courtesy call option, the system automatically places a call to the forwarding destination. Refer to Section 4.3, "Call Forwarding, Station—Courtesy Call", on page 4-5.

When a caller dials the DN of a station that has the station CFDA feature active, the subscriber is alerted to the incoming call in the usual manner. If the call is not answered after a preset number of rings, the HiPath 8000 routes the call to the forwarding destination.

Table 4-2 lists and describes the displays associated with this feature for the calling party, forwarding party, and forwarded-to party.

Forwarding Status	Calling Party (Party A) Display	Forwarding Party (Party B) Display	Forwarded-To Party (Party C) Display
Party A calls party B; party B is ringing	Party B's name and number	Party A's name and number	—
CFDA timeout expires on party B; party C is ringing	Party C's name and number	—	Party A's name and number
Party C answers	Party C's name and number	—	Party A's name and number

Table 4-2 Station CFDA—Associated Displays

To deactivates the station CFDA feature, the subscriber goes off-hook, receives dial tone, and dials *93. The HiPath 8000 provides a confirmation tone to acknowledge the deactivation, and then provides dial tone.

4.5 Call Forwarding, Station—Enhanced

Refer to Section 4.11, "Call Forwarding, Station—Time-of-Day", on page 4-11.

4.6 Call Forwarding, Station—Fixed

Siemens SIP endpoints also provide the capability to locally configure a fixed forwarding destination. However:

- **It is strongly recommended that the endpoint-based call forwarding features *not* be used simultaneously with other station call forwarding features that reside in the HiPath 8000.**
- It is preferable to use the endpoint-based call forwarding features if the user requires greater control of call forwarding.

4.6.1 Definition

The HiPath 8000-based station call forwarding—fixed feature provides the capability to redirect calls intended for the subscriber to a fixed destination. The subscriber activates and deactivates the feature; however, the system administrator configures the forwarding destination.

This capability is available for the station CFBL and station CFDA features. Refer to Section 4.2, “Call Forwarding, Station—Busy Line”, on page 4-4 and Section 4.4, “Call Forwarding, Station—Don’t Answer”, on page 4-6.

4.6.2 Functional Operation

The system administrator defines station call forwarding—fixed functionality by configuring the station CFBL and station CFDA features such that the subscriber is not permitted to modify the forwarding destination.

The subscriber activates and deactivates the station CFBL and station CFDA features in the usual manner. However, after the access code is entered, the HiPath 8000 does not permit the subscriber to specify a forwarding destination.

4.7 Call Forwarding, Station—Remote Activation

4.7.1 Definition

The station remote activation call forwarding (RACF) feature, sometimes known as *call forwarding remote activation*, is an optional capability of the station call forwarding—all calls feature. It provides the subscriber the capability to activate, deactivate, and change the redirect number for station call forwarding—all calls from a locations other than the subscriber’s station. This capability permits the subscriber to manage station call forwarding options and change forwarding destinations from home or from another work location.

To subscribe to this feature, the subscriber must also have the station call forwarding—all calls feature. Refer to Section 4.1, “Call Forwarding, Station—All Calls”, on page 4-2.

4.7.2 Functional Operation

The subscriber accesses the station RACF feature as follows:

1. The subscriber dials the RACF DN as configured by the HiPath 8000 administrator.
2. The HiPath 8000 prompts the subscriber to enter the subscriber’s home DN, followed by a prompt to enter the subscriber’s PIN.
3. After the HiPath 8000 verifies the home DN and PIN, it prompts the subscriber to enter the option associated with the action to be performed.

4.8 Call Forwarding, Station—Remote Call Forwarding

4.8.1 Definition

The HiPath 8000-based station remote call forwarding (RCF) feature provides the capability to redirect calls intended for subscriber to a fixed destination. This feature is similar to station call forwarding—all calls, with the following exceptions:

- No physical telephone is associated with the base DN. Refer to Section 9.10, “Virtual DN”, on page 9-8 for more information.
- A specified number of simultaneous calls can be forwarded to the remote station from the RCF base DN.

The calling party receives no indication that the call terminates at a remote location.

4.8.2 Functional Operation

The system administrator configures the station RCF feature by specifying the following:

- The RCF DN that serves as the forwarding destination.

  The RCF DN does not originate, and all calls to the DN are permanently forwarded through the direct distance dialing (DDD) network to the remote location.

- The maximum simultaneous calls allowed for forwarding. If reception of more than one simultaneous call is desired, the forwarded-to DN associated with the RCF DN can be a member of a hunt group. Although the HiPath 8000 does not require that this be the case, doing so permits the forwarded-to party to receive and process simultaneous calls. Refer to Section 7.2, “Hunt Group”, on page 7-3.

  Call forwarding takes place regardless of the status of the forwarded-to party. If all lines are busy, the calling party might hear busy tone or can alternately be routed to the voice mailbox associated with the DN.

4.9 Call Forwarding—Return

Call forwarding—return is an inherent capability of the following HiPath 8000-based station call forwarding features:

- Station call forwarding—all calls
- Station CFBL
- Station CFDA
- Station CFVM

- Selective call forwarding
- Time-of-day station call forwarding

It allows the forwarded-to station to call the forwarding station and override (ignore) the forwarding. Therefore, the forwarded-to user can call the party that has forwarding active towards them. This occurs even when calling party information is not delivered to the subscriber.

This feature is particularly useful in executive-assistant arrangements, because it allows the assistant to call the executive even when the executive's telephone is forwarded to the assistant.

The optiClient 130 S provides endpoint-based call forwarding—return. However, this feature does *not* operate in the same manner as the HiPath 8000-based feature. For example, endpoint-based call forwarding—return requires calling party information in order to properly function.

Refer to the *optiClient 130 S, V4.0, Administrator Documentation and Operating Instructions* for more information.

4.10 Call Forwarding, Station—Selective

Refer to Section 5.20, "Selective Call Forwarding", on page 5-19.

4.11 Call Forwarding, Station—Time-of-Day

4.11.1 Definition

The HiPath 8000-based time-of-day station call forwarding feature, sometimes known as *call forwarding enhanced* and *enhanced call forwarding (ECF)*, provides a scheduling capability for the basic station call forwarding services of the station call forwarding—all calls, station CFBL, and station CFDA features. It can also be used with the selective call forwarding feature in some circumstances.

Important Note

Time-of-day forwarding is a separate feature; the user is *not* required to subscribe to station call forwarding—all calls, station CFBL, or station CFDA in order to use time-of-day forwarding.

Call forwarding—return is an inherent capability of time-of-day forwarding; it allows the forwarded-to station to call the forwarding station and override (ignore) the forwarding. Refer to Section 4.9, “Call Forwarding—Return”, on page 4-10.

4.11.2 Functional Operation

The subscriber uses the GUI provided by the *i*SSC to define the schedules, activate and deactivate the feature, and specify the forwarding destination. The following can be specified:

- Whether the feature is active
- Maximum number of seconds to ring before forwarding the call (0 - 60)
- A screen list of up to 16 numbers. Based on a value on each time interval, this list:
  - Is ignored
  - Contains the numbers which will be allowed to be forwarded
  - Contains the numbers which will not be allowed to be forwarded
- A time-of-day schedule that provides the details of when time-of-day forwarding applies, the type of forwarding, and the forward-to DN. There can be up to 49 entries (a maximum of seven per day). Each entry has the following information:
  - The day of the week and the start and end times that the forwarding will be done. The schedule entries cannot overlap.
  - Forward-to DN to be routed to when forwarding. Note that this can be an extension if the DN is within a business group.
  - The type of station call forwarding to be done, either call forwarding—all calls, CFBL, CFDA, or a combination of CFBL and CFDA
  - Whether to forward all calls, only those contained in the screen list, or only those *not* contained in the screen list

When a caller dials the DN of a station that has call forwarding—time-of-day active, the HiPath 8000 handles the call in a manner similar to how it handles forwarded calls that do not have a schedule associated with them. Refer to the following:

- Section 4.1, “Call Forwarding, Station—All Calls”, on page 4-2
- Section 4.2, “Call Forwarding, Station—Busy Line”, on page 4-4
- Section 4.4, “Call Forwarding, Station—Don’t Answer”, on page 4-6

Note that the user's dialing characteristics, rather than the caller's, are used when forwarding the call. When forwarding the call, no splash ring is provided.

Because a telephone user interface for administering the feature is not provided, a courtesy call is *not* provided when calls are forwarded due to time-of-day forwarding.

4.12 Call Forwarding, Station—Voice Mail

4.12.1 Definition

The station call forwarding—voice mail (CFVM) feature ensures that message waiting indication (MWI) is automatically delivered to the SIP endpoint when a new voice mail message is present.

CFVM can be used independently, or it can be used in conjunction with station call forwarding—all calls, station CFBL, and station CFDA.

- When it is used independently, all unanswered or busy-forwarded calls route to voice mail, and the user receives MWI.
- When it is used in conjunction with other station call forwarding features, it does the following:
  - It ensures that the user receives MWI when calls are forwarded to voice mail.
  - It permits different forwarding to be assigned to different scenarios, and for the user to receive MWI for the calls that are routed to voice mail.

    This capability is useful, for example, if a user wants unanswered calls to route to an assistant, and busy-forwarded calls to route to voice mail.

- Although the system administrator can define separate forwarding targets for busy-forwarded and unanswered calls independently of the CFVM feature, the user does *not* receive MWI unless CFVM is subscribed to.
- Call forwarding—return is an inherent capability of station CFVM; it allows the forwarded-to station to call the forwarding station and override (ignore) the forwarding. Refer to Section 4.9, “Call Forwarding—Return”, on page 4-10.

4.12.2 Functional Operation

The system administrator sets the RTP parameter Srx/Main/CFVMCompatibility to specify if station CFBL, station CFDA, or both can be assigned to a subscriber at the same time CFVM is subscribed, as follows:

- **Station CFBL**:
  - When set to True, CFBL and CFVM can be assigned to the same subscriber. When both are assigned and active, CFBL takes precedence in a busy-line situation.
  - When set to False, CFBL and CFVM cannot be assigned to the same subscriber.
- **Station CFDA**:
  - When set to True, CFDA and CFVM can be assigned to the same subscriber. When both are assigned and active, CFDA takes precedence in a no-answer situation because the no-answer timer for the CFVM feature does not start.
  - When set to False, CFDA and CFVM cannot be assigned to the same subscriber.

The system administrator can also specify the conditions under which a received MWI indication from the VMS is considered valid. Based on the status of the subscriber's CFVM feature:

- **If it is active:** An MWI indication can be accepted and processed for a voice mail subscriber.
- **If it not active:** The acceptance of an MWI indication for a voice mail subscriber is based on the setting of the RTP parameter Srx/Main/MwiOnVMInactive:
  - When set to True, an MWI indication is accepted and processed.
  - When set to False, an MWI indication is ignored.

4.13 CDR

When a call is forwarded, CDRs are generated as follows:

- One *standard CDR* for the call leg that takes place between the original calling party and the final forwarded-to (connected) party. This CDR type is generated for all calls.
- One *call forwarding CDR* for each call leg created when the original call is forwarded. Because the HiPath 8000 permits up to five forwards per call, up to five of these CDRs can be generated.

For example, assume that party A calls party B. Party B forwards to party C; party C then forwards to party D. In this scenario:

- A standard CDR is generated for the A-to-D call.

- Individual call forwarding CDRs are generated for the B-to-C and C-to-D call legs.

4.14 Guidelines for Implementation and Use

The following are the forwarding target requirements:

- The number must be a routable destination in the private network or in the PSTN—for example, it cannot be a feature access code.
- The number must be compatible with any toll and call restrictions in effect for the subscriber.

5 Other User Features

This chapter describes other user features that reside in the HiPath 8000. Examples of such features are calling identity delivery and suppression features, abbreviated dialing features, redial and call return features, and display features.

Refer to the following for information about administration practices associated with these functions and features:

- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*

Refer to the following for more information to operate these features:

- *optiPoint 410/420 Advance S, V6.0, User Manual*
- *optiClient 130 S, V4.0, Administrator Documentation and Operating Instructions*
- *optiPoint 150 S User Manual*
- *optiPoint WL 2 Professional S, Operating Manual*

5.1 Anonymous Call Rejection

5.1.1 Definition

The anonymous call rejection feature, sometimes known as *anonymous caller reject*, provides subscribers the capability to reject calls from parties who have a privacy feature active (such as caller ID blocking) that prevents the delivery of the calling number to the called party.

5.1.2 Functional Operation

If the system administrator assigns the anonymous call rejection feature to the subscriber as usage-sensitive, the subscriber can activate or deactivate the feature.

To activate the anonymous call rejection feature, the subscriber goes off-hook, receives a dial tone, and enters *77. The HiPath 8000 provides a confirmation tone or announcement to acknowledge the activation.

When anonymous call rejection is activated, the HiPath 8000 checks incoming calls to determine if the presentation of the calling party's DN is allowed. This check is performed regardless of whether the subscriber's extension is offhook or idle.

- **If presentation is allowed or if the presentation status is unavailable:** The HiPath 8000 completes the call.

  Screening of calls, however, may depend on the precedence of other features that a called party has active on the line.

- **If presentation is restricted:** The HiPath 8000 does not complete the call and the subscriber does not receive alerting for the call. Instead, the caller hears a denial announcement that informs the calling party that the system cannot accept the call unless the calling party information is made public. If the calling party does not hang up within 10 to 12 seconds of completion of the announcement, the system automatically disconnects the call.

To deactivate the anonymous call rejection feature, the subscriber goes off-hook, receives a dial tone, and enters *87. The HiPath 8000 provides a confirmation tone or announcement to acknowledge the deactivation.

5.1.3 Traffic Measurements

The following anonymous call rejection traffic measurements are maintained on a per-SPCS basis:

- Number of feature activations
- Number of feature deactivations
- Overflow counts for the number of unsuccessful feature activation attempts because there were no available SPCS resources
- Overflow counts for the number of unsuccessful feature deactivation attempts because there were no available SPCS resources
- Number of calls routed to the anonymous call rejection denial announcement

The following maintenance measurements can be kept hourly on a per-SPCS basis. They can be available on demand by local and remote maintenance as well as regular maintenance reports:

- Number of incoming calls with restricted presentation status that were provided with standard error treatment because the anonymous call rejection denial announcement facilities were not available

- Number of activations that were provided with a confirmation tone because the confirmation announcement facilities were not available
- Number of deactivations that were provided with a confirmation tone because the confirmation announcement facilities were not available

5.1.4 CDR

Call detail recording (CDR) is provided on a usage-sensitive basis.

CDRs are generated once daily, at the client-scheduled record generation time, for each line with anonymous call rejection. This includes the count of calls and denial treatment since the last record generation.

5.2 Automatic Callback

5.2.1 Definition

The automatic callback feature, sometimes known as *auto callback* or *call completion on busy subscriber/no reply (CCBS/NR)*, permits a calling party to activate an automatic callback if the called station:

- Is busy for any reason, including conference, forwarding, and DND status.
- Is not answering an alerting call.

The optiPoint 410/420 S and optiClient 130 S support this feature.

The called party can be another subscriber within the same HiPath 8000 or a user located in a legacy PBX in the network. In the latter case, automatic callback is interworked on the HiPath 8000 with the QSIG CCBS/NR service signaled over the SIP-Q interface.

Siemens SIP endpoints also have local features that simplify redialing of calls. Refer to the applicable user manual for information about those features.

5.2.2 Functional Operation

The system administrator can allow or disallow the monitoring of busy or no-reply conditions for subscribers served by the HiPath 8000.

To activate the automatic callback feature, the subscriber must make a call and either hear busy tone or receive no answer. The subscriber then goes onhook, goes offhook again, and enters *66. The user can also enter *66 upon hearing the busy tone. In either instance, the HiPath 8000 provides a confirmation tone or announcement to acknowledge that it received the callback request.

After the feature is activated, the following events take place:

- **If the called party was busy:** The system automatically redials the last number dialed. If the called party is now idle, the call is offered. Otherwise, monitoring begins and the calling party hears a confirmation tone or sees a display. The called party has no notification of the callback request.

  As soon as the called party goes onhook, the calling party is notified of the called party's availability and is recalled. When the calling party answers, a new call to the original destination is automatically dialed.

- **If the called party did not answer the alerting call:** The called party becomes available for callback after initiating some activity on the device, then transitioning to idle state. At that point, the system automatically redials the number.

When parties A and B have successfully activated callback against each other (for example, party A to B, then party B to A), only one callback execution occurs when both parties become idle.

To cancel all callback requests, the calling party enters #66*. The HiPath 8000 provides a confirmation tone or announcement to acknowledge that it received the cancellation request.

Some SIP endpoints support the activation and deactivation of automatic callback via the Optiguide display instead of using an access code. Refer to the applicable user manual for more information.

5.3 Automatic Recall

Refer to Section 5.17, “Return Call”, on page 5-16.

5.4 Caller Identity Service

5.4.1 Definition

The caller identity service is a collection of features to allow the subscriber to be presented with caller identification information of the intragroup call partner. The information is updated as the call progresses to connection.

This feature provides the following functionality in conjunction with the calling number delivery and calling name delivery features, including the blocking features:

- Calling party number display
- Calling party name display
- Called party number display
- Alerting party number display
- Alerting party name display
- Automatic display suppression (on/off) of number for calling, alerting, and connected party
- Automatic display suppression (on/off) of name for calling, alerting, and connected party
- Display suppression (on/off) of number per call for calling party
- Display suppression (on/off) of name per call for calling party

The feature utilizes a private extension header within SIP provisional and final responses to convey the called or connected party identity (number and name, if provided).

When calling, called, and connected parties appear, the number displayed appears in the preferred format of the number that can be used to call back the calling party—for example, the shortest possible dialable number, the national number, or the international number.

Refer also to the following:

- Section 5.5, “Calling Identity Delivery and Suppression”
- Section 5.7, “Calling Name Delivery Blocking”
- Section 5.9, “Calling Number Delivery Blocking”
- Section 5.12, “Customer-Originated Trace”

Refer to the individual feature descriptions for specific information about associated displays.

5.4.2 Networking

- The number, name, and presentation indicators for network parties are obtained from the data stored in the UCE context.
- SIP-Q sends the number, name, and presentation indicators for network parties.
- The calling party ID and called party ID features reside in and operate locally to the HiPath 8000. Therefore, it can coexist and has no impact in a networked HiPath 8000 environment.

- CorNet-NQ/QSIG interworking provides support for calling (alerting/connected) party display at the calling party.
- Refer to Section 12.7.2, “Caller Identity Service”, on page 12-6 for information about the interworking that takes place for this feature between the HiPath 8000 and a legacy PBX.

5.5 Calling Identity Delivery and Suppression

5.5.1 Definition

The calling identity delivery and suppression (CIDS) feature provides subscribers the capability to deliver or suppress their calling identity parameters (name and number).

This feature can be provisioned at the business group level with a denied option at the subscriber level. Counters are provided for feature activation attempts.

5.5.2 Functional Operation

The system administrator specifies a subscriber’s *permanent presentation status*. This parameter represents the default status for presentation or suppression of the subscriber’s calling identity information. The system administrator also specifies whether the subscriber can access the CIDS feature to ignore the permanent presentation status on a per-call basis.

The subscriber accesses the CIDS feature as follows:

- **To deliver calling identity parameters:** The subscriber goes off-hook, receives a dial tone, and enters *64. After hearing a recall dial tone, the subscriber can then dial the call. The subscriber’s name and number appear on the called party’s display.

  If the subscriber enters this code, but the DN is configured to permanently block calling identity information, the subscriber hears an announcement indicating the line is permanently marked anonymous and cannot be changed.

- **To suppress calling identity parameters:** The subscriber goes off-hook, receives a dial tone, and enters *45. After hearing a recall dial tone, the subscriber can then dial the call. `Private/Anonymous` appears on the called party’s display instead of the subscriber’s name and number.

  If the subscriber enters this code, but the DN is configured to permanently deliver calling identity information, the subscriber hears an announcement indicating the line is permanently marked public and cannot be changed.

The subscriber can also enter either access code while a call is in progress.

Siemens SIP telephones also allow dialing of all digits (enbloc dialing). The subscriber enters the correct access code and DN as one digit sequence, rather than pausing for recall dial tone after entering the access code.

If the caller activates CIDS, the HiPath 8000 does not retrieve the permanent presentation status of the caller's DN permanent presentation status. Instead, it delivers or suppresses the calling identity information according to the CIDS access code the subscriber entered.

5.5.3 Networking

- The presentation indicators for network parties are obtained from the data stored in the UCE context.
- SIP-Q sends the presentation indicators for network parties.

5.6 Calling Name Delivery

5.6.1 Definition

The calling name delivery (CNAM) feature, sometimes known as *name delivery,* provides the terminating party with the possibility of receiving the name of the originating party. The calling party information is obtained from a local database and a host-delivered calling name.

5.6.2 Functional Operation

The system administrator determines the access codes associated with the CNAM feature.

When subscribers receive a call from another SIP endpoint, whether it be within the business group or outside the business group, the CNAM feature assignment has no effect because SIP endpoints always deliver the calling name, assuming that it is available and public.

However, the CNAM feature is required in order to receive calling name information for calls received from other endpoint types (such as ISUP or MGCP). This feature assignment permits the CNAM database lookup to occur for the incoming call.

The system administrator can assign the CNAM feature to the subscriber as usage-sensitive, which permits the subscriber to use an access code to activate or deactivate the feature.

If the subscriber is also assigned the calling number delivery (CND) feature, the access code activates and deactivates both features. Refer to Section 5.8, "Calling Number Delivery", on page 5-9.

5.6.3 Networking

- The presentation indicators for network parties are obtained from the data stored in the UCE context.
- SIP-Q sends the presentation indicators for network parties.

5.7 Calling Name Delivery Blocking

5.7.1 Definition

The calling name delivery blocking (CNAB) feature, sometimes known as *outgoing name delivery block*, provides subscribers the capability to change the presentation status of their name when making a call.

This feature can be provisioned at the business group level with a denied option at the subscriber level. Counters are provided for feature activation attempts.

5.7.2 Functional Operation

The system administrator specifies a subscriber's permanent presentation status, sometimes known as *outgoing caller ID presentation status (name)*. This parameter represents the default status for presentation or suppression of the subscriber's calling name. The system administrator also specifies whether the subscriber can access the CNAB feature to change the presentation status on a per-call basis.

To activate the CNAB feature, the subscriber goes off-hook, receives a dial tone, and enters *68. The HiPath 8000 provides a confirmation tone, followed by dial tone. The user then dials the intended called party's DN to complete the call.

If the subscriber enters this code, but is not permitted to change the presentation status, the subscriber hears a denial announcement indicating the line's presentation status cannot be change.

When the CNAB feature is activated, the HiPath 8000 toggles the subscriber's permanent presentation status as follows:

- **If the permanent presentation status is public:** `Private/Anonymous` appears on the called party's display.
- **If the permanent presentation status is private:** The subscriber's number appears on the called party's display.

After the call is ended, the subscriber's permanent presentation status is restored to its original setting.

5.8 Calling Number Delivery

5.8.1 Definition

The calling number delivery (CND) feature provides the terminating party with the possibility of receiving the number of the originating party. The calling party information is obtained from the system database.

The number displayed appears in the preferred format of the number that can be used to call back the calling party—for example, the shortest possible dialable number, the national number, or the international number.

5.8.2 Functional Operation

The system administrator determines the access codes associated with the CND feature.

When subscribers receive a call from another SIP endpoint, whether it be within the business group or outside the business group, the CND feature assignment has no effect because SIP endpoints always deliver the calling number, assuming that it is available and public.

However, the CND feature is required in order to receive calling number information for calls received from other endpoint types (such as ISUP or MGCP). This feature assignment permits the CND database lookup to occur for the incoming call.

All subscribers are pre-assigned with this feature. The system administrator can assign the CND feature to the subscriber as usage-sensitive, which permits the subscriber to use an access code to activate or deactivate the feature.

If the subscriber is also assigned the CNAM feature, the access code activates and deactivates both features. Refer to Section 5.6, “Calling Name Delivery”, on page 5-7.

5.8.3 Networking

- The presentation indicators for network parties are obtained from the data stored in the UCE context.
- SIP-Q sends the presentation indicators for network parties.

5.9 Calling Number Delivery Blocking

5.9.1 Definition

The calling number delivery blocking (CNDB) feature, sometimes known as *outgoing number delivery block*, provides subscribers the capability to change the presentation status of their number when making a call.

This feature can be provisioned at the business group level with a denied option at the subscriber level. Counters are provided for feature activation attempts.

5.9.2 Functional Operation

The system administrator specifies a subscriber's *permanent presentation status,* sometimes known as *outgoing caller ID presentation status plus (number)*. This parameter represents the default status for presentation or suppression of the subscriber's calling number. The system administrator also specifies whether the subscriber can access the CNDB feature to change the presentation status on a per-call basis

To activate the CNDB feature, the subscriber goes off-hook, receives a dial tone, and enters *67. The HiPath 8000 provides a confirmation tone, followed by dial tone. The user then dials the intended called party's DN to complete the call.

If the subscriber enters this code, but is not permitted to change the presentation status, the subscriber hears a denial announcement indicating the line's presentation status cannot be change.

When the CNDB feature is activated, the HiPath 8000 toggles the subscriber's permanent presentation status as follows:

- If the permanent presentation status is public, `Private/Anonymous` appears on the called party's display.
- If the permanent presentation status is private, the subscriber's number appears on the called party's display.

After the call is ended, the subscriber's permanent presentation status is restored to its original setting.

5.10 Click to Answer

The click-to-answer feature provides the capability for a SIP endpoint to use a command of the Genesys Agent Console application to answer a SIP call when it is presented. As a result of the command, an answer event is generated and is passed via the HiPath 8000.

This feature is applicable to a subscriber who is also a call center agent on the Genesys call center and can control calls presented through the console application. The application lets the subscriber answer calls, make calls, transfer calls, and perform other useful functions.

Refer also to Section 16.7, “Interworking with Genesys Call Center”, on page 16-6.

The associated SIP endpoint must be an optiPoint 410/420 S DFT; this functionality is not applicable to keyset telephones.

5.11 Conference, Station-Controlled

5.11.1 Definition

The station-controlled conference feature, also known as *station-controlled large conference*, provides subscribers the capability to establish a conference call with up to 48 participants on an ad-hoc (on-demand) basis. Conference participants can be members of the same business group, another business group, or in the public network.

This feature can be provisioned at the business group level with a denied option at the subscriber level.

Siemens SIP endpoints also support a local three-way calling feature, which permits conferences of up to three participants. Refer to the applicable user manual for information about this feature.

5.11.2 Functional Operation

The system administrator determines the access code used to delete the last joined party.

Station-controlled conference participants can be classified as follows:

- **Conference-aware or conference-unaware**
  - A *conference-aware* participant knows that the current call is a conference. A conference-aware participant may be an active or passive participant, as described below.

  - A *conference-unaware* participant does *not* know that the current call is a conference; it is a simple point-to-point call. Conference-unaware participants are always passive participants as well.

- **Active or passive**
  - An *active* participant has the ability to invoke advanced functionality associated with the conference feature—for example, initially creating a conference and adding parties to it. Active participants are always conference-aware, must be associated with the same business group as the creator of the conference, and must be subscribed to the conference feature.
  - A *passive* participant can converse with other parties to the conference, but cannot invoke any advanced functionality associated with the feature. Passive participants can be either conference-aware or -unaware. Members of other business groups and those who participate via the public network are always passive participants.

To create a conference, the user first creates two calls (a held call and a consultation call), then presses the Conference key. This user is conference-aware and an active participant. Depending on the additional features assigned to other participants, others can subsequently:

- Transfer calls.
- Hold calls. Conference-aware participants can also avoid putting music into the conference.
- Alternate between held and active calls.
- **If the participant is conference-aware and active:**
  - Add another party to the conference. Refer to the applicable user manual for more information.
  - Remove the last joined party by dialing the delete-last-joined-party (DLJP) feature access code.

This function is generally used when a user has mistakenly added an unwanted or unavailable party into conference. It eliminates the need to disconnect and reconnect all conference participants in order to remove the one unwanted party.

5.11.3 Networking

Refer to Section 12.7.5, “Three-Way Calling and Voice Conferencing”, on page 12-7 for information about the interworking that takes place for this feature between the HiPath 8000 and a legacy PBX.

5.12 Customer-Originated Trace

5.12.1 Definition

The customer-originated trace feature (sometimes known as *malicious call trace*) provides subscribers the capability to generate an automatic trace of the last call received. Subscribers typically use this feature in response to malicious, harassing, or nuisance calls, in order to provide a trace over time of such activity.

A classmark at the subscriber level is required for access to this feature.

5.12.2 Functional Operation

Depending on whether the system administrator defines the trace as a one- or a two-step activation procedure, the subscriber activates this feature as follows:

- **One-step procedure**: Immediately after hanging up on a call, the subscriber goes off-hook, receives a dial tone, and enters *57. The trace is immediately initiated.
- **Two-step procedure**: After entering *57 as described above, the HiPath 8000 prompts the subscriber to dial 1 to initiate the trace. Before doing so, the subscriber can cancel the trace by going onhook.

After the trace is complete, the collected information is written to a file accessible to the system administrator.

5.13 Feature Status Notification

Feature status notification provides the capability to send the status of message waiting indication. Refer also to Section 18.9, “Message Waiting Indicator”, on page 18-3.

This status is sent when:

- There is a change to MWI status.
- When the SIP CPE/subscriber newly registers. Registration related to refresh of the SIP dialog does not cause the sending of the MWI feature status.

5.14 Hot Desking

5.14.1 Definition

The hot desking feature provides subscribers the capability to log on to and use a telephone in another office, or at another position in the same office. The telephone in the other office or position (the *remote office telephone*) then has all of the same HiPath 8000-provided features and capabilities as the telephone in the subscriber's usual office or position (the *home office telephone*). This feature is also known as *hoteling*.

The mobility feature permits the telephone-based features of the optiPoint 410 S or optiPoint 420 S to transfer to another *guest telephone*. Refer to the *optiPoint 410/420 Advance S, V6.0, User Manual*.

5.14.2 Functional Operation

The system administrator determines the access codes associated with the hot desking feature.

To activate the hot desking feature at the remote office telephone, the subscriber goes offhook, enters the hot desking feature access code, the DN of the home office telephone, and the hot desking PIN.

To deactivate the hot desking feature:

- **At the remote office telephone where the subscriber is currently logged on**: The subscriber goes offhook and enters the hot desking feature access code.
- **At any other remote office telephone:** The subscriber goes offhook, enters the hot desking feature access code, the DN of the home office telephone, and the hot desking PIN.

For optiPoint 410 S or optiPoint 420 S users, the administrator can assign a function key to the hot desking feature. If such a key is present, the display prompts the user to enter the DN of the home office telephone and the hot desking PIN after the user presses the Hot Desking key. The telephone additionally provides the following status indications:

- The LED associated with hot desking lights when the feature is activated.
- The display provides the home DN.

Regardless of the telephone type, the remote office telephone's message waiting indicator provides the status of the home DN's mailbox upon logon. After logging off, the message waiting indicator is restored to show the status of the remote office telephone, rather than that of the home DN's mailbox.

5.14.3 Guidelines for Implementation and Use

- To operate, hot desking must be assigned to both the home office telephone and on the remote office telephone.
- Telephone-based features are not transferred from the home office telephone to the remote office telephone. Refer to the applicable user manual for information about transfer of telephone-based features via the mobility feature.
- The remote office telephone and the home office telephone must be hosted by the same HiPath 8000, both must be SIP telephones, and both must be in the same business group.
- The home office telephone can be a keyset, but the remote office telephone cannot.
- If a user logs on to a remote office telephone:
  - Outgoing calls can still be placed from the home office telephone.
  - Incoming calls are routed to the remote office telephone.

5.15 Last Number Redial

Refer to Section 5.2, "Automatic Callback", on page 5-3.

5.16 Music On Hold—HiPath 8000-Based

5.16.1 Definition

The HiPath 8000-based music on hold feature provides the capability for callers to hear music when they are placed on hold. The feature can be directly assigned to an individual user, or it can be included in a feature profile assigned to the user. For a hunt group, the user is the hunt group pilot DN. Refer also to Section 7.2, "Hunt Group", on page 7-3 and Section 15.8, "Feature Profiles", on page 15-5 for more information.

When provisioned, music is provided for all instances when a subscriber places a caller on hold. This includes consultation hold, call hold, manual hold, and CSTA-initiated hold.

If it is active, this feature takes precedence over the endpoint-based music on features.

5.16.2 Functional Operation

The system administrator specifies the music to provide by using the intercept name associated with the music. This music can be identical for every instance in which a subscriber is placed on hold. Optionally, the administrator can specify different music to be provided for:

- Each feature profile, in which case all users assigned that feature profile provide the same music to their callers (when applicable)
- Each pilot DN, in which case all calls to the associated hunt group hear the same music (when applicable)
- Each individual line

The availability of this feature is based on the services assigned to the party initiating the hold. When this feature is invoked, the following takes place:

1. The entity (endpoint, trunk, gateway) that is to hear the music is connected to the media server that provides the music. This media server can be the same one that provides other announcements, or it can be a separate server.
2. Because music is treated as an announcement, a standard announcement connection is established between the receiving entity and the media server.
3. The system passes the announcement ID for the music source and the endpoint information to the media server.
4. The media server plays the music until the caller is retrieved from hold.

5.16.3 Guidelines for Implementation and Use

- The customer is responsible for creating and provisioning the .wav files associated with the music on hold intercept. The .wav files are stored on the media server.
- The music on hold can be chained in a sequence of one or more files and played in a loop.

5.17 Return Call

5.17.1 Definition

The return call feature, sometimes known as *automatic recall* or *auto recall*, provides subscribers the capability to perform an activation procedure that automatically sets up a call to the last incoming number. The subscriber need not know the telephone number of the last incoming call; however, the HiPath 8000 can be configured to announce the number during the activation procedure.

This feature is applicable to E.164 numbers in the system dial plan. Refer also to Section 9.3, “E.164 Compliance”, on page 9-2.

Siemens SIP endpoints also have local features that simplify returning of calls. Refer to the applicable user manual for information about those features.

5.17.2 Functional Operation

The system administrator can allow the subscriber to recall callers who have their calling identity suppressed. The administrator can also limit recalls to intraswitch calls (calls between business group members) only.

To activate the return call feature, the subscriber goes off-hook, receives a dial tone, and enters *69.

If the call setup is attempted and the user is busy, the HiPath 8000 monitors the busy/idle status of both lines and initiates a callback when the users are found idle.

A return call request is denied if the called line has station call forwarding—all calls active. Application of special ringing to the subscriber's line is directed to the activating station only, regardless of whether station call forwarding—all calls has been activated for the calling party.

5.18 Screen List Editing

The screen list editing feature provides the capability to use the telephone user interface to create and modify lists associated with the features described in the following sections:

- Section 5.19, "Selective Call Acceptance", on page 5-17
- Section 5.20, "Selective Call Forwarding", on page 5-19
- Section 5.21, "Selective Call Rejection", on page 5-21
- Section 5.22, "Serial Ringing", on page 5-22
- Section 5.23, "Simultaneous Ringing", on page 5-25

5.19 Selective Call Acceptance

5.19.1 Definition

The selective call acceptance feature, sometimes known as *selective caller accept*, provides the capability to build a list of numbers (known as a *screen list*) from which the subscriber wants to accept incoming calls.

This feature can be provisioned at the business group level with a denied option at the subscriber level.

5.19.2 Functional Operation

The selective call acceptance screen list is a set of numbers, each of which can be up to 15 digits long, for which calls should be connected to the subscriber. The screen list can contain up to 32 entries.

To activate the selective call acceptance feature, the subscriber goes off-hook, receives a dial tone, and enters *27. When a caller's number matches a number on the acceptance list, the call is completed. When the caller's number is not on the acceptance list, one of the following occurs:

- The caller hears an announcement that indicates the subscriber does not accepting calls from this number.
- The call is forwarded to a remote DN.

To deactivate the selective call acceptance feature, the subscriber goes off-hook, receives a dial tone, and enters *28.

If selective call acceptance is active, but the screen list is empty, all calls will be rejected.

5.19.3 Traffic Measurements

Table 5-1 on page 5-18 lists and describes the traffic measurements associated with the selective call acceptance feature.

Peg Counter	Description
SCA Access Code Attempted	The number of hourly peg counts and usage counts with a usage-scan rate of 1 per 10 seconds for screen list editing and for attempts to invoke control procedures as a result of dialing the selective call acceptance feature access code. These counts are available per hour on an individual SPCS basis.
SCA Unaccepted Calls	The number of hourly peg counts of unaccepted calls. These counts are available per hour on an individual SPCS basis.
SCA Validation	The number of hourly peg counts of all calls checked against the screen list of a subscriber with selective call acceptance active. These counts are available per hour on an individual SPCS basis.
SCA Customer Denied Resource Unavailable	The number of overflow counts for the number of subscribers denied access to selective call acceptance because of unavailable resources. These counts are available on an individual SPCS basis.
SCA Treatment Denied Resource Unavailable	The number of overflow counts for the number of unaccepted calls. These counts are available on an individual SPCS basis.

Table 5-1 Selective Call Acceptance Feature—Traffic Measurements (Sheet 1 of 2)

Peg Counter	Description
SCA Attempt Denied Resource Unavailable	The number of overflow counts for the SPCS and/or any circuits used to provide selective call acceptance control procedures. These counts are available on an individual SPCS basis.

Table 5-1 Selective Call Acceptance Feature—Traffic Measurements (Sheet 2 of 2)

5.19.4 CDR

CDRs are provided on a usage-sensitive basis.

CDRs are generated once daily, at the client-scheduled record generation time, for each line with selective call acceptance. This includes the count of calls and denial treatment since the last record generation. The following are the CDRs associated with this feature:

- Selective call acceptance activation
- Selective call acceptance deactivation
- Selective call acceptance screen list created
- Selective call acceptance screen list edited
- Selective call acceptance screen list deleted

5.20 Selective Call Forwarding

5.20.1 Definition

The selective call forwarding feature, sometimes known as *call forwarding selective*, provides the capability to build a list of numbers (a *screen list*) which the subscriber wants to automatically forward to another destination.

This feature can be provisioned at the business group level with a denied option at the subscriber level.

- Call forwarding—return is an inherent capability of selective call forwarding; it allows the forwarded-to station to call the forwarding station and override (ignore) the forwarding. Refer to Section 4.9, “Call Forwarding—Return”, on page 4-10.
- In some instances, the time-of-day forwarding feature provides a scheduling capability in conjunction with this feature. Refer to Section 4.11, “Call Forwarding, Station—Time-of-Day”, on page 4-11.

5.20.2 Functional Operation

The selective call forwarding screen list is a set of numbers, each of which can be up to 15 digits long, for which calls should be forwarded to a remote station. Business group extensions can also appear on the screen list. The screen list can contain up to 32 entries.

To activate the selective call forwarding feature, the subscriber goes off-hook, receives a dial tone, and enters *63. When a caller's number matches a number on the forwarding list, the call is forwarded to the redirect number. This can be another telephone, another subscriber, voice mail, or an announcement. When the caller's number is not on the forwarding list, the call is completed as usual.

To deactivate the selective call forwarding feature, the subscriber goes off-hook, receives a dial tone, and enters *83.

Selective call forwarding is independent of other call forwarding features such as station call forwarding—all calls, station CFDA, and station CFBL. The system administrator can designate a separate remote DN for each feature: one for selective call forwarding, one for station call forwarding—all calls, and so on. Calls from DNs that cannot be determined, or are not on the list, can be forwarded to the remote station designated for the second call forwarding service.

5.20.3 Guidelines for Implementation and Use

5.20.3.1 Forwarding Target Requirements

The following are the forwarding target requirements:

- The number must translate to a routable destination—for example, it cannot be a feature access code.
- The number must be compatible with any toll and call restrictions in effect for the subscriber.

5.20.3.2 Real-Time and Memory Considerations

The following are the real-time considerations for the selective call forwarding feature:

- Screen list match processing time
- Feature interaction consideration time
- The time involved in the specific implementation of the feature—for example, forwarding the call, connecting the party to a rejection announcement, and obtaining name information from the service control point (SCP).

It is assumed that each subscriber has one screen list per specific feature.

5.21 Selective Call Rejection

5.21.1 Definition

The selective call rejection feature, sometimes known as *selective caller reject*, provides the capability to build a list of numbers (known as a *screen list*) from which the subscriber does not want to accept incoming calls.

This feature can be provisioned at the business group level with a denied option at the subscriber level.

5.21.2 Functional Operation

The selective call rejection screen list is a set of DNs, each of which can be up to 15 digits long, for which calls should be rejected. The screen list can contain up to 32 entries.

When a caller's number does not match a number on the rejection list, the call is completed. When the caller's number matches a number on the rejection list, the caller hears an announcement that indicates the subscriber does not accept calls from the number.

The subscriber initiates procedures for activating, deactivating, modifying or obtaining a status report for selective call rejection by going offhook, receiving dial tone, and dialing the correct feature access code. The default access codes are *60 to activate the feature, and *80 to deactivate the feature.

The system provides announcements to guide the subscriber through the selective call rejection procedures.

As long as the calling DN is on the station's screen list, routing to a rejection announcement takes place regardless of whether the station is busy or idle. The subscriber does not receive any announcement when a call has been rejected.

5.21.3 Traffic Measurements

Table 5-2 lists and describes the traffic measurements associated with the selective call rejection feature.

Peg Counter	Description
SCR Attempt	The hourly peg counts and usage counts with a usage scan rate of 1 per 10 seconds for selective call rejection screen editing and for attempts to invoke control procedures as a result of dialing the selective call rejection access code.

Table 5-2 Selective Call Rejection Feature—Traffic Measurements (Sheet 1 of 2)

Peg Counter	Description
SCR Call To Denial Announcement	The hourly peg counts of rejected calls.
SCR All Calls Screened	The hourly peg counts of all calls screened for a subscriber with selective call rejection active.
SCR Customer Denied Resource Unavailable	The overflow counts for the number of customers denied access to selective call rejection because of unavailable system resources.
SCR Denied Announcement Unavailable	The overflow counts for the number of rejected calls because of denied access to selective call rejection.
SCR Access Denied Resource Unavailable	The overflow counts for the system and/or any circuits used to provide selective call rejection control procedures.

Table 5-2 Selective Call Rejection Feature—Traffic Measurements (Sheet 2 of 2)

5.21.4 CDR

CDRs are provided on a usage-sensitive basis.

CDRs are generated once daily, at the client-scheduled record generation time, for each line with ACR. This includes the count of calls and denial treatment since the last record generation. The following are the CDRs maintained for this feature:

- SCR activation
- SCR deactivation
- SCR screen list editing
- SCR screen list created
- SCR screen list deleted

5.22 Serial Ringing

5.22.1 Definition

The serial ringing feature provides subscribers the capability to be sequentially rung at a series of locations. This is especially useful for those whose job duties require them to be in or around many different work areas throughout the day.

This feature optionally includes the ability for the caller to instantly transfer to the caller's voice mailbox, rather than waiting for the call to progress through all locations to do so.

The simultaneous ringing feature is similar to this feature, but it rings several locations at the same time. Refer to Section 5.23, “Simultaneous Ringing”, on page 5-25.

5.22.2 Functional Operation

The system administrator determines the access codes associated with the serial ringing feature.

The system administrator assigns the simultaneous ringing feature to a subscriber, then associates it with one of the user’s DNs, referred to as the *main DN.*

After this step, either the subscriber or the system administrator creates a screen list, known as a *serial ringing list,* that contains up to six DNs. These DNs represent the additional locations that ring when an incoming call arrives at the main DN, and the sequence in which they are rung. Each DN can contain up to 15 digits.

To perform this task, the subscriber goes offhook, receives a dial tone, and enters the correct access code. The subscriber hears an announcement that provides the feature name, its current status (active or inactive), and the number of DNs currently on the list. The HiPath 8000 then prompts the user to specify one of the following actions to perform:

- Activate or deactivate the feature
- Hear the DNs that are currently on the list
- Add or delete DNs to and from the list

The subscriber can also use the *i*SSC to perform this task. By doing so, the user can also:

- Change the ring duration default (18 seconds) for the main DN and for each DN on the serial ringing list to a value between 1 and 120 seconds
- Activate and deactivate individual serial ringing list entries

To activate the serial ringing feature, the subscriber can:

- Select the option to activate the feature while in the list editing mode.
- Use the *i*SSC.
- Enter the correct access code. The HiPath 8000 provides a confirmation tone or announcement to acknowledge the activation. If the subscriber’s serial ringing list is empty, the HiPath 8000 prompts the subscriber to enter DNs into the list. As soon as a valid DN is entered, the feature is activated.

After the feature is activated, incoming calls cause the main DN to ring. If it is not answered in the configured ring duration interval, the next destination DN is rung for its configured ring duration interval. The first DN to answer is connected.

The HiPath 8000 uses the subscriber's dialing characteristics, rather than the caller's, when it sets up calls to the numbers in the serial ringing list.

If there is no answer after all destination DNs are rung, the call is then routed to one of the following:

- The user's station CFDA destination (if defined)
- An intercept announcement

If there is no answer at a given destination DN, the HiPath 8000 can optionally provide an intercept announcement before attempting the next number in the list. The options are as follows:

- An announcement that keeps the caller apprised of the call's progress—for example, "Trying to reach the user at a different number."
- An announcement that provides the above information, and also gives the option for the caller to press a digit to be instantly routed to the called party's voice mailbox.

To deactivate the serial ringing feature, the subscriber can:

- Select the option to deactivate the feature while in the list editing mode.
- Use the *i*SSC.
- Enter the correct access code. The HiPath 8000 provides a confirmation tone or announcement to acknowledge the deactivation.

5.22.3 CDR

- A record is created for the original call to the main number. In this CDR, the caller's number is the "A" number and the main DN is the "B" number.
- Up to six CDRs are created, one for each of the other calls that are set up. In these CDRs, the caller's DN is the calling party number, the DN being called is the "B" DN, and the main DN is the "charge-to" DN. This is done to assure that the feature owner is made responsible for any charges associated with these six calls.

5.23 Simultaneous Ringing

5.23.1 Definition

The simultaneous ringing feature provides subscribers the capability to be simultaneously rung at multiple locations. This is especially useful for those whose job duties require them to be in or around many different work areas throughout the day.

The serial ringing feature is similar to this feature, but it rings one location at a time. Refer to Section 5.22, “Serial Ringing”, on page 5-22.

5.23.2 Functional Operation

The system administrator determines the access codes associated with the simultaneous ringing feature.

The system administrator assigns the simultaneous ringing feature to a subscriber, then associates it with one of the user’s DNs, referred to as the *main DN.*

After this step, either the subscriber or the system administrator creates a screen list, known as a *simultaneous ringing list,* that contains up to six DNs. These DNs represent the additional locations that ring when an incoming call arrives at the main DN. Each DN can contain up to 15 digits.

To perform this task, the subscriber goes offhook, receives a dial tone, and enters the correct access code. The subscriber hears an announcement that provides the feature name, its current status (active or inactive), and the number of DNs currently on the list. The HiPath 8000 then prompts the user to specify one of the following actions to perform:

- Activate or deactivate the feature
- Hear the DNs that are currently on the list
- Add or delete DNs to and from the list

Depending on configuration, the subscriber can also manage the simultaneous ringing list as follows:

- If the remote feature access (RFA) option is active, the subscriber can manage the list from any telephone, not just from the home DN.

  After dialing the RFA DN as configured by the HiPath 8000 administrator, the HiPath 8000 prompts the subscriber to enter the subscriber's home DN, followed by a prompt to enter the subscriber's PIN. After the HiPath 8000 verifies the home DN and PIN, it prompts the subscriber to enter the option associated with the action to be performed.

- The subscriber can use the *i*SSC.

To activate the simultaneous ringing feature, the subscriber can:

- Select the option to activate the feature while in the list editing mode, either while at the home DN or while invoking the RFA option.
- Use the *i*SSC.
- Enter the correct access code. The HiPath 8000 provides a confirmation tone or announcement to acknowledge the activation. If the subscriber's simultaneous ringing list is empty, the HiPath 8000 prompts the subscriber to enter DNs into the list. As soon as a valid DN is entered, the feature is activated.

After the feature is activated, incoming calls cause the main DN and each destination DN to ring. The first DN to answer is connected. If the call is forwarded to another DN, such as voice mail, it rings until answered.

The HiPath 8000 uses the subscriber's dialing characteristics, rather than the caller's, when it sets up calls to the numbers in the simultaneous ringing list.

To deactivate the simultaneous ringing feature, the subscriber can:

- Select the option to deactivate the feature while in the list editing mode.
- Use the *i*SSC.
- Enter the correct access code. The HiPath 8000 provides a confirmation tone or announcement to acknowledge the deactivation.

The user can also access the simultaneous ringing feature remotely as follows:

1. The user dials the remote activation DN associated with the feature.
2. When the HiPath 8000 detects a call to the remote activation DN, it connects the caller to the media server. The media server prompts the caller to enter the correct home DN and PIN.

3. The user dials the correct home DN (main number) followed by the correct PIN. The media server collects these digits and passes them to the HiPath 8000.
4. The HiPath 8000 confirms the PIN and provides a confirmation tone or announcement to the user.
5. The user has the same access to the feature as if it was accessed from the home DN. However, local (non-PSTN extensions) must be prefixed with the digits 02. For example, if the local extension is 1020, the user must enter `021020` for the change to take effect.

5.23.3 CDR

- A record is created for the original call to the main number. In this CDR, the caller's number is the "A" number and the main DN is the "B" number.
- Up to six CDRs are created, one for each of the other calls that are set up. In these CDRs, the caller's DN is the calling party number, the DN being called is the "B" DN, and the main DN is the "charge-to" DN. This is done to assure that the feature owner is made responsible for any charges associated with these six calls.

5.24 Station Dialing

5.24.1 Definition

The station dialing features permit a user to invoke offhook dialing or context dialing to access the following features and destinations:

- Another station
- Public network (external) destination
- Control digits (to control a voice mail system or IVR device)

The following are the types of station dialing:

- **Offhook dialing** lets the user lift the handset, obtain dial tone, and enter keypad digits. The digits are automatically processed without the need for an interdigit timeout or user intervention. The user always has access to offhook dialing during the initial dial state.
- **Context dialing** lets the user enter and modify the digits before the HiPath 8000 processes the digits. By using context dialing, the subscriber can enter digit sequences such as:
  - An access code
  - An access code + DN

5.24.2 Functional Operation

The user can dial in the following ways:

- **Offhook dialing:** The user lifts the handset and hears dial tone (or obtains dial tone in a different manner) and enters keypad digits. The digits are automatically processed, without the need for inter-digit timeout or user intervention.
- **Context dialing:** The user enters and modifies digits before the HiPath 8000 processes those digits. The user begins dialing from the keypad. Upon completing the access code or destination to dial, the telephone sends the digits to the HiPath 8000 when one of the following occurs:
  - The user selects `Dial?` to complete dialing and send the information to the HiPath 8000 (i.e., enbloc-dialing mode).
  - The user waits for the inter-digit timeout to elapse.

Depending on the type of station dialing used, the telephone functions differently. For example, if the user wants to make a public network call to a 7-digit destination:

- **Offhook dialing:**
  1. The user dials the PSTN access code.
  2. The user continues to enter each of the seven digits.
  3. After each digit, the telephone compares the digits entered to the entries configured in its internal dialing plan to determine if a complete dialing sequence is present.
  4. When the telephone determines that a complete dialing sequence is present, it sends the access code and the 7-digit number to the HiPath 8000 in a single message, known as an *INVITE message*.
  5. The HiPath 8000 analyzes the INVITE message, recognizes the PSTN access code, and accepts the additional digits as the public network destination.
- **Context dialing:**
  1. The user dials the PSTN access code + 7-digit number.
  2. The user selects `Dial?` or waits for the inter-digit timeout to elapse.
  3. The telephone sends the digits to the HiPath 8000.
  4. The HiPath 8000 receives the access code and the 7-digit number in a single INVITE message.
  5. The HiPath 8000 analyzes the digits it received and recognizes the initial digit as the PSTN access code.
  6. The HiPath 8000 determines if it has additional digits to analyze.

In this example, there are additional digits present, so the HiPath 8000 accepts these as the public network destination.

Therefore, the HiPath 8000 must always assume that context dialing is being used, and must always look for the additional digit.

5.25 Station Speed Calling—HiPath 8000-Based

5.25.1 Definition

The HiPath 8000-based station speed calling feature, sometimes known as *speed dial*, provides the capability to place frequently dialed numbers in a centralized speed calling list.

This feature can be provisioned at the business group level with a denied option at the subscriber level.

Siemens SIP endpoints also have local features that simplify the dialing of frequently-used numbers. Refer to the applicable user manual for information about those features.

The following are the types of station speed calling:

- **One-digit station speed calling:** This feature allows a subscriber to place calls to a repertory of frequently called numbers by dialing a 1-digit speed calling code. Eight numbers can be placed in the list. The system administrator sets up and maintains the list.
- **Two-digit station speed calling:** This feature allows a subscriber to place calls to a repertory of 30 frequently called numbers by dialing a 2-digit speed calling code. The system administrator sets up and maintains the list.

Each of the speed calling lists can be provided to a subscriber as follows:

- A *private list* is used by one subscriber, who can modify any entry.
- A *shared list* is owned by one subscriber, but can be used by many subscribers. Only the owner can modify the list entries.

A subscriber can have both a one-digit and a two-digit list. They can both be private, both be shared, or one can be private with the other one shared.

5.25.2 Functional Operation

If the subscriber has the ability to create speed calling entries, the subscriber goes off-hook, receives a dial tone, and enters the following:

- **1-digit speed calling entry:** *74, followed by the number (2 through 9) to associate with the entry, and the number to store for the entry

- **2-digit speed calling entry:** *75, followed by the number (20 through 49) to associate with the entry, and the number to store for the entry

To dial a speed calling list entry, the subscriber goes off-hook, receives a dial tone, and enters the number associated with the entry—for example, to dial entry 23, the subscriber enters the digits 23. After entry, if the subscriber does not select `Dial?,` the number is automatically dialed after a 4-second timeout expires.

5.25.3 Guidelines for Implementation and Use

- Stations with speed calling should be given standard originating treatment up to the point where the first digit is collected.

  For stations with 1-digit speed calling: 4-second nominal timing (3 to 5 seconds is acceptable, 4 seconds is preferred) should be initiated when the first dialed digit received is one of the digits 2 through 9. If the first dialed digit is one of the digits 2 through 9, is followed by the user selecting `Dial?` or by a 4-second timeout, and the subscriber has access to the feature, the call completes to the corresponding address in the speed calling list.

  For stations with 2-digit speed calling: 4-second timing should be initiated when the second dialed digit is received, provided that the first digit dialed is one of the digits 2 through 4. If the second digit collected is one of the digits 0 through 9; the first digit was 2, 3, or 4; and the subscriber has access to the feature, the system determines if this digit is followed by the user selecting `Dial?` or by a 4-second timeout. If so, the call completes to the corresponding address in the speed calling list.

- Speed calling can be used any time dialing is appropriate; however, the speed calling entry must supply all dialing information, including applicable access codes.

- The HiPath 8000 can provide each subscriber a shared list and an individual list. In this instance, one list must be a 1-digit list and the other a 2-digit list. In the case of shared lists, only one subscriber can make changes to the list.

5.26 Teleworking

The teleworking feature provides a solution that permits HiPath 8000 users who work remotely to have access to the telephone features they can access while at their primary office locations.

optiClient 130 S users need only have a VPN connection in order to invoke the teleworking feature. Contact your Siemens representative about the availability of teleworking solutions applicable to other SIP endpoints. Refer to the *HiPath 8000 Overview Guide* for detailed information about the software that permits teleworking for HiPath 8000 users.

5.27 Toll and Call Restrictions

5.27.1 Definition

The toll and call restrictions feature provides destination limitations on calls originated at designated stations and private facilities.

The associated subfeatures can be assigned to any subscriber or private facility with call-origination capability, unless otherwise restricted by an assigned feature.

5.27.2 Functional Operation

The system administrator can assign restrictions for the following types of calls originating from a business group:

- Direct-dialed international calls (011+)
- Direct-dialed calls (1+)
- Operator-assisted international calls (01+)
- Operator-assisted calls (0+)
- Operator-request calls (0-; i.e., 0 followed by # or 4-second timeout)
- Local directory assistance calls (411)
- Long distance directory assistance calls (555)

Additionally, the system administrator can store up to 10 entries in a block list. These entries can be DNs or partial DNs—for example, area codes. Block lists can be specified on a per-subscriber basis, a per-business group basis, or per-private facility basis.

When the HiPath 8000 detects that a restricted station or private facility is attempting to originate a call, it determines if the dialed digits represent a permitted destination.

- **If the dialed digits are permitted:** The call proceeds normally.
- **If the dialed digits are prohibited:** The system routes the call to an announcement or to reorder tone. The treatment can be assigned on a per-subscriber or per-group basis.

5.27.3 Guidelines for Implementation and Use

- The screening is based on the North American numbering plan (NANP). These features do not screen calls made using other dialing plans (such as extension dialing and business group dialing plans).

  Refer to the following for more information about these features:

  – Section 6.7, “Business Group Dialing Plan”, on page 6-5

  – Section 6.14, “Extension Dialing”, on page 6-11

  – Section 9.7, “North American Numbering Plan Compliance”, on page 9-3

- The dialed digits screening is independent of prefixes or access codes dialed by the caller (such as, 10XXX or the PSTN access code).

5.28 Transfer

5.28.1 Definition

The call transfer features permit a business group member to redirect an established call to another member of the same business group. The interaction between the system and the third party is similar to that during three-way calling, except that when a party with the feature hangs up, the incoming or outgoing call is transferred to the third party. The system disconnects all parties when a transfer is attempted to a party outside the business group.

The following transfer features are supported:

- The *blind transfer* feature permits a transfer without consultation to another party.
- The *unscreened transfer* feature permits the user to perform a call transfer prior to the transferred-to destination answering the call. The transfer request is completed during ringing or call waiting (camp-on).

  Unlike blind transfer, the user has some control over the attempted transfer. Upon the user hearing ringback tone and seeing a display, the user can complete the transfer before the destination answers.

- The *transfer with third-party consultation* feature permits a screened transfer. After speaking with the transfer-to party, the user can transfer the first party to the transfer destination.

The transfer security feature ensures that unsuccessfully transferred calls are recalled to the transferring party. Refer to Section 5.29, “Transfer Security”, on page 5-36.

5.28.2 Functional Operation

The transfer features are implemented between the SIP endpoint and the HiPath 8000, as follows:

- The request and type of transfer is controlled by the telephone.
- The processing and checking (for example, for transfer restrictions) is controlled by the HiPath 8000.

The user transfers calls as follows:

- **Blind transfer:** While a call is in progress, the user selects `Blind Transfer?` from the optiGuide display and presses the ✔ key to confirm the selection. The optiGuide display then prompts the user to dial the transfer destination. After the user dials the destination and presses the ✔ key, `Transferring`, then `Call Transferred` appears on the display.
- **Unscreened Transfer:** While a call is in progress, the user selects `Consult/Transfer?` from the optiGuide display and presses the ✔ key to confirm the selection. The optiGuide display then prompts the user to dial the transfer destination. After the user dials the destination and presses the ✔ key, `Complete Transfer?` appears on the display. The user waits until hearing ringback tone and seeing a display, then presses the ✔ key.
- **Transfer with third-party consultation:** While a call is in progress, the user selects `Consult/Transfer?` from the optiGuide display and presses the ✔ key to place the first party on consultation hold. The user can now dial and connect to the transfer-to party and announce the pending transfer. After the transferred-to party answers, the user presses the ✔ key in response to the `Complete Transfer?` prompt.

The user accesses the optiGuide's Configuration menu to specify whether each transfer feature is active for the specific telephone. The user can also use the Setup/Function Keys menu to assign each transfer feature to an unassigned function key. After the feature key is assigned, it activates the feature and permits the user to enter a transfer destination.

Table 5-3 lists and describes the displays associated with blind transfers for the transferring party, transferred party, and transferred-to party.

Transfer Status	Transferring Party (Party A) Display	Transferred Party (Party B) Display	Transferred-To Party (Party C) Display
Party A calls party B, party B answers -or- Party B calls party A, party A answers	Party B's name and number	Party A's name and number	—

Table 5-3 Blind Transfer—Associated Displays (Sheet 1 of 2)

Transfer Status	Transferring Party (Party A) Display	Transferred Party (Party B) Display	Transferred-To Party (Party C) Display
Party A puts party B on consultation hold by selecting `Blind Transfer`	—	Party A's name and number; see note 1	—
Party A performs a blind transfer to party C, party C is ringing	—	Party C's name and number	Party B's name and number
Party C answers	—	Party C's name and number	Party B's name and number
1. Party B may or may not receive `Held` display, but does hear music.			

Table 5-3 Blind Transfer—Associated Displays (Sheet 2 of 2)

Table 5-4 lists and describes the displays associated with unscreened transfers for the transferring party, transferred party, and transferred-to party.

Transfer Status	Transferring Party (Party A) Display	Transferred Party (Party B) Display	Transferred-To Party (Party C) Display
Party A calls party B, party B answers -or- Party B calls party A, party A answers	Party B's name and number	Party A's name and number	—
Party A puts party B on consultation hold by selecting `Consult/ Transfer`	—	Party A's name and number; see note 1	—
Party A calls party C, party C is ringing	Party C's name and number	Party A's name and number	Party A's name and number
A transfers party B to party C	—	Party C's name and number	Party B's name and number
Party C answers	—	Party C's name and number	—
1. Party B may or may not receive `Held` display, but does hear music.			

Table 5-4 Unscreened Transfer—Associated Displays

Table 5-5 lists and describes the displays associated with transfers with third-party consultation for the transferring party, transferred party, and transferred-to party.

Transfer Status	Transferring Party (Party A) Display	Transferred Party (Party B) Display	Transferred-To Party (Party C) Display
Party A calls party B, party B answers -or- Party B calls party A, party A answers	Party B's name and number	Party A's name and number	—
Party A puts party B on consultation hold by selecting `Consult/ Transfer`	—	Party A's name and number; see note 1	—
Party A calls party C, party C is ringing	Party C's name and number	Party A's name and number; see note 2	Party A's name and number
Party C answers	Party C's name and number	Party A's name and number; see note 2	Party A's name and number
A alternates between party B and party C (optional)	Party B's name and number	Party A's name and number	Party A's name and number; see note 2
Party A transfers party B to party C	—	Party C's name and number	Party B's name and number
1. Party B may or may not receive the `Held` display, but does hear music. 2. Depending on the endpoint and software release, party B or C might also receive `Held` display.			

Table 5-5 Transfer with Third-Party Consultation—Associated Displays

5.28.3 Guidelines for Implementation and Use

To enable transfer on SIP endpoints, transfer must be configured at the business group or feature profile level, and assigned to the business group.

5.29 Transfer Security

5.29.1 Definition

The transfer security feature provides the capability to ensure that:

- A transferred party is not left ringing for too long at another internal user's endpoint
- A user does not transfer a party to an invalid destination

This feature can also provides an intercept to a provisioned destination if a call transfer recall occurs and the transferring party is busy and cannot be camped onto.

This feature is applicable to station-to-station calls transferred via an unscreened or blind transfer. It is *not* applicable to screened transfers or to calls transferred outside of the business group.

5.29.2 Functional Operation

The user can activate the transfer security feature for internal calls only, external calls only, or both.

The transferring party receives immediate recall, and the transferred-to party is released, in the following instances:

- Incomplete or invalid dialing
- Attempt to transfer to a party that goes on hook prior to transfer
- Provisioned restrictions on the user attempting the transfer, the party being transferred, or the transferred-to party. (Immediate Recall)

The transferring party receives delayed recall, and the transferred-to party is released, if there is no answer at the transferred-to party.

A configured recall busy destination is used to redirect the transferred party to an alternate destination if the transferring user is busy upon recall, and cannot accept a camp-on. In addition, intercept treatment occurs if the transfer security recall goes unanswered for a provisioned intercept time.

The following timers start when a call is transferred:

- The transfer security timer, which determines the time interval before delayed recall occurs
- The intercept treatment timer, which determines the time interval before the transferred party receives intercept treatment

The system administrator specifies the values associated with both timers.

5.29.3 CDR

For complex call scenarios—for example, when a call is transferred with consultation—a thread identifier correlates the CDRs associated with each leg of the call. Refer to Section 13.2, “Call Detail Record Generation”, on page 13-1.

6 Business Group Features

This chapter describes features that are specific to business groups. These features simplify such tasks as dialing plan administration, intragroup communication, and traffic measurements.

Refer to the following for information about administration practices associated with these functions and features:

- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*

6.1 Attendant Answering Position

6.1.1 Definition

The attendant answering position (AAP) feature provides support for a SIP-based AAP using a DFT, keyset telephone, or a soft client. The AAP functionality includes night service (automatic and manual control) to route calls to predefined night stations or other answering device— for example, to voice messaging, to an automated attendant application, or to a night bell device.

Refer also to Section 7.5, “Hunt Group—Night Service”, on page 7-6.

6.1.2 Functional Operation

The system administrator identifies a hunt group as an attendant answering group. The administrator also specifies values for the following capabilities available to all hunt groups:

- **Time-in-queue threshold value:** Refer to Section 7.2, “Hunt Group”, on page 7-3.
- **Night service DN:** Refer to Section 7.5, “Hunt Group—Night Service”, on page 7-6.
- **An automatic make busy on no answer advance:** Refer to Section 7.6, “Hunt Group—No Answer Advance”, on page 7-7.

AAPs are devices that, through the use of hunt groups, the business’s main DN, or by dialing 0, provide a termination point for:

- Incoming calls to the business
- Incoming calls to an operator within the business
- Personal calls to the AAP user

AAPs have the capability to:

- Act as a night service destination and to manually activate night service for the business
- Extend calls to other destination within the private network or external destinations
- Camp on to busy stations
- Be recalled
- Access external trunk resources
- Prevent calls made or extended within the private network from being transferred, held, or overridden with the exception of Inter-AAP calls
- Simultaneously handle multiple call presentation—for example, to the business and operator lines
- Trace malicious calls
- Provide through-connect and trunk-to-trunk connections
- Perform inter-AAP call transfers
- Display the name and number related to incoming business calls

One or more AAPs may be provisioned per business group.

6.2 Business Group Access Codes

The business group access codes feature allows the assignment of feature access codes, network access codes, and attendant access codes to be separately administrable for each business group.

6.3 Business Group Account Codes

6.3.1 Definition

The business group account codes feature lets the subscriber add a number into the CDR record for allocation of charges on billable calls (incoming or outgoing). For example, a lawyer can charge a client for long-distance calls in addition to the time spent on the call.

6.3.2 Functional Operation

The system administrator specifies the number of digits of the account code. It can be from 2 to 14 digits long; its length is the same for all stations in a business group.

To enter the account code, the subscriber enters a specified activation code followed by the account code, either before or after the called number is dialed.

The user can also include the account code as part of a speed dialing entry.

6.4 Business Group Authorization Codes

6.4.1 Definition

The business group authorization codes feature provides the capability to control access to calls to parties outside the business group.

6.4.2 Functional Operation

The system administrator specifies the number of digits of the account code. It can be from 2 to 14 digits long; its length is the same for all stations in a business group. Up to 100,000 authorization codes are supported, with up to 50,000 per business group.

To access this feature, the subscriber dials the public network access code (usually 9), followed by the destination digits. The system then prompts the subscriber to enter the authorization code. After the subscriber does so, one of the following events takes place:

- **If the authorization code is valid:** The call completes normally.

- **If the authorization code is invalid:** The system prompts the subscriber to re-enter the authorization code. If the second entry is also invalid, the call is given intercept treatment.

6.5 Business Group Billing

The business group billing feature supports the Message Detail Recording - Regional Accounting Office (MDR-RAO) per *GR-610 Message Detail Recording (MDR)* (FSD 02-02-1110). This capability can be turned on or off on a per-business group basis.

When the feature is enabled, CDR provides the following data for calls from and to the business group as applicable:

- Customer identification
- Originating or terminating facility type
- Originating or terminating facility identification
- Call completion code
- Business feature code
- Automatic route selection (ARS) or automatic alternate routing (AAR) pattern group
- Facility restriction level (FRL)
- End of dialing or digit reception time
- Queue elapsed time
- Access code
- Authorization code
- Account code
- Dialed digits

Refer to Chapter 13, “CDR Features” and to the *HiPath 8000 Call Detail Recording (CDR) Reference Guide* for more information.

6.6 Business Group Department Names

The business group department names feature permits a business group subscriber to be associated with a specific department. The department name can be delivered as an alternative to the calling or connected party name. The CDR record provides the department name.

Up to 50 department names are supported for each business group.

6.7 Business Group Dialing Plan

6.7.1 Definition

The business group dialing plan provides virtual private branch exchange (PBX) service via the HiPath 8000 and appears to be a standalone entity within which the business group-specific dialing plan is in force. To reach lines outside of the business group, the caller usually dials an access code.

Each business group can support multiple dialing plans, which permits multiple sites to have their own distinct dialing plans, yet maintain access to intra-business group feature functionality. There is also one system (default) dialing plan that can be used for common public dial plan access.

Every subscriber has a directory number (DN), which can be a public direct inward dialing (DID) DN or a pseudo public DN. If a subscriber has a pseudo public DN, the DN is of the same length as a public DN but cannot be dialed from the public network. In addition to a public DN, a subscriber may also have a private number—for example, an extension number and a fully-qualified private number.

DNs are sometimes known as *business group lines (BGLs).*

A fully-qualified private number is a digit string up to 20 digits long. It does not necessarily have a relation to the E.164 DN of the subscriber. The number is in the form of LOC+extension, where LOC is the location code and can be further broken down into the following levels:

- **L0:** Level 0 or subscriber location code. L0 is 0-4 digits in length.
- **L1:** Level 1 or national location code. L1 is 0-6 digits in length. L1 cannot be administered without L0.
- **L2:** Level 2 or International location code. L2 is 0-4 digits in length. L2 cannot be administered without L1.

All three levels are optional.

The extension number within a single location uniquely identifies the subscriber. L0 digits can overlap with the extension digits, for example, 923-5505 where 923 is the L0 code and 3-5505 is the extension.

The business group dialing plan also specifies the access codes listed in Table 6-1 on page 6-6.

- The customer can use * and # as the first (and perhaps only) digit of any of the access codes.
- If needed, the customer can specify a code from 1 to 5 digits for use as an equivalent to *.
- * code conflicts are resolved by use of critical inter-digit timing or use of # as an end-of-dialing indicator.

Access Code Type	Number of Digits	Description
Attendant	1 to 5	Connects a HiPath 8000 user to the attendant. Many times, it is defined as the digit 0.
PSTN	1 to 5	Connects a HiPath 8000 user to the public network. Many times, it is defined as the digit 9. Also known as *off-net call prefix* and *off-net access code*.
Private facility	1 to 5	Gives access to private facilities—for example, tie trunks. For example, all codes of the form 1XX could be reserved for private-facility access.
Private network	1 to 6	Gives access to private networks. For example, dialing the digit 8 could lead to connection to a private network. Also known as *on-net call prefix* and *on-net access code*.

Table 6-1 Access Codes Defined in Business Group Dialing Plan

6.7.2 Functional Operation

All SIP telephones within a business group register with their fully-qualified private number or with their public DN, whether it be DID or pseudo.

Subscribers in a business group are reachable by dialing:

- Fully-qualified private number
- DID number: Refer to Section 6.11, “Direct Inward Dialing”, on page 6-9.
- Extension number: Refer to Section 6.14, “Extension Dialing”, on page 6-11.

A business group dialing plan allows:

- Extension dialing
- Fully-qualified private number dialing
  - L0-extension: if L0 is administered in the private numbering plan

  - L1-L0-extension: if L1 is administered in the private numbering plan
  - L2-L1-L0-extension: if L2 is administered in the private numbering plan
- On-net dialing: On-net access code (HiPath on-net barrier code) is dialed before the fully qualified private number.
  - <On-net access code>-L0-extension: if L0 is administered in the private numbering plan
  - <On-net access code>-L1-L0-extension: if L1 is administered in the private numbering plan
  - <On-net access code>-L2-L1-L0-extension: if L2 is administered in the private numbering plan

In each type of dialing plan, the calling and called private numbers can be within the same LOC or different LOCs.

6.7.3 Guidelines for Implementation and Use

- If a telephone is provisioned with the fully-qualified private number, it is assumed that the fully-qualified private number is unique within the domain of the host HiPath 8000.
- Outside callers from the public network can only reach subscribers with pseudo DNs by dialing the main DN of the business group and then being transferred. Outside callers cannot reach subscribers by dialing the pseudo DN.

6.8 Business Group Main Number

The business group main number feature provides for a published directory number for each business group. The attendant can answer this number or it can be assigned as the first number in a business group range (*extension range*). The main number can be also be a pseudo number, and not assigned to a dedicated line. It can be mapped to any extension in the business group, such as the attendant's assigned line.

6.9 Business Group Traffic Measurements

6.9.1 Definition

The business group traffic measurements feature provides counts of several types of HiPath 8000 activity on a per-business group basis. The business group administrator can use these measurements to monitor the company's calling patterns and usage at a high level, or can analyze them in greater detail if desired.

The basic traffic tool is another performance monitoring tool used to view snapshots of the traffic for incoming SIP calls to the HiPath 8000. Refer to Section 15.3, “Basic Traffic Tool”, on page 15-3.

6.9.2 Functional Operation

The system administrator can activate or deactivate this feature for the business group.

The business group measurement data is delivered to the *i*SMC or HiPath 8000 Assistant. The business group administrator can access the measurements and monitor the company’s calling patterns by simply performing a visual inspection of the reported data. However, some administrators may want to perform additional analysis of this data to determine:

- The average time an employee spends on the telephone
- The percentage of calls placed outside the business group
- The business group calling features that are under- or overused

6.9.3 Measurement Types

Table 6-2 lists and describes the traffic measurements available for each business group.

Measurement	Description
Originating calls	The number of call origination attempts that resulted in the system’s receipt of at least 1 digit. Calls that do not normally result in digits being dialed (hotline, warm line) are included upon determination of the destination. The count is kept on a business group basis. For SIP endpoints using enbloc delivery of the dialed digits, the count is pegged for any call reaching the incoming transaction segment (ITS) of the universal call engine (UCE).
Terminating calls	The number of incoming calls intended to complete within the system, including intrasystem calls. The count is made upon the system's recognition of the destination. The count is kept on a per business group basis.
Intragroup calls	The number of group originating calls intended to complete within the group. The count is made upon the system's recognition of destination. This count is pegged if the originating business group and the terminating business group are the same.
Intragroup usage	Traffic usage generated by intragroup calls. The measurement collection software accumulates usage for calls with the same originating and terminating business group.

Table 6-2 Business Group Traffic Measurements(Sheet 1 of 2)

Measurement	Description
Originating usage	Traffic usage generated by originating calls measured at a single, common point in the system network. The measurement collection software scans all calls in the system every 100 ms. It counts the number of calls originated from the business group. The resulting count represents the usage for that period (i.e., count x 100ms = usage).
Terminating usage	Traffic usage generated by terminating calls measured at a single, common point in the system network. The measurement collection software scans all calls in the system every 100 ms. It counts the number of calls terminated to each business group. The resulting count represents the usage for that period (i.e., count x 100ms = usage).
Feature use	The number of times the system's treatment of a call is affected by feature treatment. The count is incremented each time a feature-related function is performed in lieu of, or in addition to, a normal call processing function.
Feature activation	The number of times the system responds to requests to allow a feature's function. This count is best exemplified by existing station call forwarding—all calls activation counts.
Feature deactivation	The number of times the system responds to requests to deny or end a feature's function.
Dial 8, dial 9 calls	A separate count of the number of originating Dial 8 and Dial 9 attempts that occur within the system. For example, *Dial 9* generally indicates public network calls and *dial 8* indicates private network calls.
DID calls	The number of terminating calls to the business group that originated in the public network. DID calls are recognized by the absence of an originating business group.
Circuit attendant loop	Event counts and overflow measurements on circuit attendant loops. This is the number of calls to the attendant and overflows.

Table 6-2 Business Group Traffic Measurements(Sheet 2 of 2)

6.10 Business Group Web Portal

The business group web portal feature provides web portals for the management of features at the business group level.

6.11 Direct Inward Dialing

The direct inward dialing (DID) feature allows an external caller to dial a national or international number and connect directly to a HiPath8000 subscriber.

6.12 Direct Outward Dialing

6.12.1 Definition

The direct outward dialing (DOD) feature allows subscribers to have direct outward dialing access to the PSTN. This access is usually signaled using a 1- to 5-digit PSTN access code that is defined in the business group dialing plan. Refer to Section 6.7, “Business Group Dialing Plan”, on page 6-5.

The use of the PSTN access code ensures no conflicts with the extension-dialing pattern.

6.12.2 Functional Operation

When the user enters the PSTN access code, the HiPath 8000 recognizes the digit sequence and permits the user to dial the external number. After the user finishes dialing, the HiPath 8000 completes the call in the usual manner.

A HiPath 8000 user can also dial the access code and outside number in one sequence. In this case, the HiPath 8000 strips the access code from the dialed number and replaces the called party number with the remaining digits. Refer to Section 5.24, “Station Dialing”, on page 5-27.

6.13 Distinctive Ringing

6.13.1 Definition

The distinctive ringing feature provides the ability for users of the following SIP endpoints to hear different ringing indications for internal and external calls:

- optiPoint 410 S and optiPoint 420 S
- optiClient 130 S

This permits the user to distinguish internal and external calls based on the melody defined in the endpoint.

When the distinctive ringing feature is active for a business group, a different internal ringing pattern (known as *Bellcore-dr1*) is sent to the telephone for calls received from users within the business group.

The business group administrator controls internal ringing for the entire business group. If this capability is not provisioned, the internal ringing pattern sent to the telephone is the same as the pattern defined for external calls (known as *Bellcore-dr2*).

The actual alert indication strings (Bellcore-dr1 and Bellcore-dr2) must be defined in the telephone's alert indication section. If the strings are not defined in the telephone, the telephone rings with a default cadence for all calls, regardless of whether they are internal or external.

6.14 Extension Dialing

6.14.1 Definition

The extension dialing feature allows a subscriber in a business group to dial other subscribers in the same business group by dialing an abbreviated number that is synonymous with the extension number. Extension dialing is also known as *station-to-station dialing.*

Although this feature is sometimes known as *intercom dialing*, it does *not* provide a speakerphone-like capability.

6.14.2 Functional Operation

Extension dialing permits the dialing of intragroup calls on a 1- to 7-digit basis. Per-group traffic measurements of all extension-call attempts and durations are available. Refer to Section 6.9, “Business Group Traffic Measurements”, on page 6-7.

An extension-dialed call is an intragroup call dialed using a digit sequence assigned to extension dialing. When a digit sequence assigned to extension dialing is entered at a station, the HiPath 8000 can convert extension to the directory number of the called station. After the HiPath 8000 determines the DN of the called station, it completes the call in the normal manner.

6.14.3 Guidelines for Implementation and Use

The extension dialing feature is assigned to the business group as a whole; after it is assigned, all stations within the business group have the feature.

Any of the fully or semi-restricted limitations and restrictions of the group or station also apply to calls dialed by extension. Refer to Section 6.17, “Station Restrictions”, on page 6-12.

6.15 Group-Level Feature Administration

The group-level feature administration feature provides the capability to assign subscriber features to the business group as a whole. It also provides an override capability at the subscriber level to deny the feature. The subscriber-level assignments have priority over the group-level assignments.

6.16 Multiple Language Announcements

The multiple language announcements feature provides the capability to assign different languages to each subscriber, incoming trunk group, endpoint, and PRI.

Siemens SIP endpoints also have local features that provide the capability to define the language for menu prompts. Refer to the applicable user manual for information about those features.

When the IP Unity media server is used, the following languages are available by default:

- English
- German
- Swedish

The following additional languages can be added by way of a project-specific request:

- Spanish
- French
- Russian
- Japanese
- Chinese (Mandarin)

Contact your Siemens representative for information about the languages supported by the Convedia server and the integrated media server.

The media server used for the announcements must be provisioned with separate files for each announcement and language.

6.17 Station Restrictions

6.17.1 Definition

The station restrictions feature, sometimes known as *line restriction*, lets the system administrator restrict the calls permitted to and from a given station. *Originating line restrictions* refers to restrictions on calls placed from a station; *terminating line restrictions* refers to restrictions on calls being terminated to a station.

The system administrator can assign this feature to the entire business group or to individual users.

6.17.2 Functional Operation

The HiPath 8000 checks station restrictions before completing calls and performing call transfers. If a call is found to be in violation of configured restriction levels, the system routes the call to error treatment and subsequently releases it.

Because station restriction is not a visible subscriber service, it does not increment a visible usage counter.

6.17.2.1 Semi-Restricted Lines

Calls originated at a semi-restricted line and directed to a line outside of its business group and/ or calls directed to a a semi-restricted line from a line outside of its business group are routed to error treatment (usually reorder tone or special intercept announcement).

Semi-restricted lines have indirect access to and from lines outside the business group for the following types of calls (provided that the appropriate features are available):

- Calls from outside the business group and forwarded to the semi-restricted line by a non-restricted DN
- Calls from outside the business group and transferred to the semi-restricted line by a non-restricted DN
- Calls from outside the business group and picked up at the semi-restricted line
- Calls from a semi-restricted line to an non-restricted business group and forwarded to an outside line.
- Calls from a semi-restricted line to a non-restricted DN and transferred at the DN outside the business group.

The administrator can assign a semi-restricted line to a DN on an originating basis, on a terminating basis, or both.

6.17.2.2 Fully-Restricted Lines

A fully-restricted line has all of the attributes of an semi-restricted line. In addition, calls directed to a fully-restricted line from the business group attendant, as well as calls originated at a fully-restricted line and directed to the business group attendant, are routed to error treatment (reorder tone or special intercept announcement). A fully-restricted line does not have indirect access of any sort to or from lines outside the business group; this should include multiply-forwarded calls.

The administrator can assign a fully-restricted line to a DN on an originating basis, on a terminating basis, or both.

6.17.2.3 Fully-Restricted Lines with Attendant Access

A fully-restricted line with attendant access can access the attendant for information and to requests transfers to another DN within the business group. The HiPath 8000 does not permit the attendant to transfer a DN with this restriction to points outside of the business group, as well as attempts by the attendant to transfer calls from outside the business group to a DN with this restriction.

All other characteristics of fully-restricted lines are also present.

The administrator can assign a fully-restricted line with attendant access to a DN on an originating basis, on a terminating basis, or both.

6.17.3 Networking

The station restrictions feature does not function across nodes in a network.

6.17.4 Guidelines for Implementation and Use

The station restrictions feature is explicitly assigned to a business group or DN. For this reason, there is no performance impact on non-business group related calls. For business group related calls, reference to restrictions are to shared memory only, thereby minimizing performance impact.

6.18 Voice VPN

The voice VPN feature permits the use of on-net routing to establish a communication path between subscribers of a business group, even if these subscribers are in different locations.

The private dialing plan allows the integration of subscribers hosted in either traditional PBXs or public switches as part of the business group by establishing a number in the private dialing plan that translates into a route to the PSTN switch or PBX. This capability allows access to these subscribers by dialing the private number (extension number) designated by the private dialing plan, instead of dialing the public directory number. This is a one-way capability in that the PSTN switch or PBX user has no ability to dial the private dialing plan themselves.

7 Other Group Features

This chapter describes the group call pickup feature, which allows users to answer calls on behalf of one another, and the hunt group feature, which permits calls to be routed to an idle line within a group of specified lines.

Refer to the following for information about administration practices associated with these functions and features:

- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*

Refer to the following for more information to operate these features:

- *optiPoint 410/420 Advance S, V6.0, User Manual*
- *optiClient 130 S, V4.0, Administrator Documentation and Operating Instructions*
- *optiPoint 150 S User Manual*
- *optiPoint WL 2 Professional S, Operating Manual*

7.1 Call Pickup—Group

7.1.1 Definition

The group call pickup feature permits stations to be combined into *pickup groups*. Pickup groups permit a member to answer a call on behalf of another member of the group.

A pickup group can consist of a combination of different user endpoint types, such as digital feature telephones (DFTs) or keyset telephones. A call to any member in the group can be picked up at any other station in the group.

The HiPath 8000 supports up to 10,000 pickup groups. Each pickup group can contain up to 500 stations. A station (DN) can be a member of one pickup group.

7.1.2 Functional Operation

The system administrator creates the pickup group. Every business group can be configured with its own feature access code, or the default value **3 can be used.

During an incoming call to a pickup group member, the following notifications take place:

- **For the called station:** The called party hears ringing.

  For other pickup group members: `Pickup Call?` appears on each member's display.

- If a GROUP PICKUP LED is configured, it flashes.
- If the calling party information is available, it appears on the display of all pickup group members who are idle or have no pending incoming calls. If a pickup group member receives an incoming call, the incoming call information replaces the pickup group call information.

A group member picks up a ringing or alerting call of another station by pressing the Group Pickup key, using the optiGuide display, or by dialing **3. If a line appearance key and the Group Pickup key are both flashing, the member can press either key to answer the call.

When two or more members in the group are ringing, calls are answered in order of arrival; therefore, the call ringing the longest is automatically picked up first.

If there are no alerting calls for the group, and a pickup is attempted, the member who attempts the pickup receives an error indication. This indication might be an interrupted dial tone, a message on the display, or an error tone.

Important Note

If one or more phantom lines are in a pickup group:

- At least one member of the group must be a prime line; the phantom line must be assigned to a line key of this prime line terminal.
- With multiple line appearances of one phantom line on several keysets, the prime lines of these keysets must be in the same pickup group to be able to answer pickup group calls on these phantom lines.

7.1.3 Networking

- A pickup group cannot exist across the network.
- Refer to Section 12.7.1, “Call Pickup—Group”, on page 12-6 for more information about the interworking that takes place for this feature between the HiPath 8000 and a legacy PBX.

7.1.4 Guidelines for Implementation and Use

The following are the guidelines associated with the group call pickup feature:

- The system administrator must configure each pickup group member's SIP terminal number and service ID to be equal to the group member's DN.

Important Note

If the pickup group member is not configured in this manner, the feature does *not* function properly.

- Every possible calling party's area code and office code combination must be defined in the default numbering plan.
- For each group, up to eight ringing lines are queued for pickup. If a ninth call rings, it cannot be picked up even if other calls leave the queue or it later becomes the only ringing line in the pickup group.
- To pick calls from the PSTN for members within the pickup group, the system administrator must assign the member the classmark for call pickup external.
- Although CSTA does not support call pickup, the user can use the associated feature access code to invoke the feature.

7.2 Hunt Group

7.2.1 Definition

The hunt group feature, sometimes known as *multiline hunt group (MLHG)*, permits calls to be routed to an idle member of a group of stations, known as a *hunt group.* Hunt groups provide a simple mechanism for distributing calls among a group of stations.

The HiPath 8000 supports hunt groups that can be accessed through a pilot station number *(pilot hunt group*) or through a call number of a controlling station (*master hunt group*).

With a pilot hunt group, dialing the pilot number (station) for a group provides access to the pilot group. Calls are not distributed to the pilot station; this number is used only as an access number to the hunt group.

With a master hunt group, dialing the master number (station) for a group provides access to the master hunt group. Calls are distributed to the master station; the master station also has access to certain features that control the hunt group, such as station call forwarding.

The HiPath 8000 supports up to 25,000 hunt groups. Each hunt group can contain up to 2000 stations. A station (DN) can be a member of multiple hunt groups. Although each station has its own DN, the system administrator can designate it as non-external.

7.2.2 Functional Operation

A call is placed to a hunt group by dialing the pilot number. The hunting sequence may be as follows:

- **Circular hunting with memory:** An incoming call causes the HiPath 8000 to progressively search for an idle station within the hunt group, starting with station position stored when the previous call to the hunt group was made.

  When a line is selected to complete a call to the group, the line that is one past it in the group is marked to become the starting point for the hunt on the next call to the hunt group. For example, if the last line in the group was chosen for the previous call, this is the first line in the group for the next call.

- **Linear hunting:** An incoming call causes the HiPath 8000 to progressively search for an idle station within that hunt group. The hunting sequence starts with the first member and ends with the last member in the group, completing the call to the first idle station encountered.

- **Manual hunting:** The HiPath 8000 does not perform the distribution of call to agents, and all incoming calls are queued. For the distribution to work, the hunt group should also be marked for CSTA, which allows an external application to be notified of calls going into the queue, and to subsequently retrieve (reroute) those calls.

HiPath ProCenter Enterprise uses manual hunting to distribute calls to agents. Refer to Section 16.4, “Integration with HiPath ProCenter”, on page 16-3 for more information.

A hunt group is busy when one of the following conditions are present:

- It is in night service. Refer to Section 7.5, “Hunt Group—Night Service”, on page 7-6.
- There are no idle members in the group to present the call to, and there are no idle positions in the queue.

When a hunt group line becomes idle, each group it belongs to must be searched to determine if there are any calls queued that can be processed by that line. The sequence to search the queues is based on the priority of the queues for that member, with the lower-numbered priorities checked before a higher-numbered priority queue. Queues with the same priority can be checked in any sequence.

Upon determining busy, the sequence of treatment is as follows:

1. If the group is in night service, the call is routed to the night service DN. Refer to Section 7.5, “Hunt Group—Night Service”, on page 7-6.
2. Otherwise, if there is an associated queue with idle positions in the queue, queuing will be performed. Refer to Section 7.8, “Hunt Group—Queuing”, on page 7-8.

3. Otherwise, if CFBL is active on the group via the pilot DN, the call is forwarded. Refer to Section 4.2, “Call Forwarding, Station—Busy Line”, on page 4-4.
4. Otherwise, if an Overflow DN is present, the call is routed to it. Refer to Section 7.7, “Hunt Group—Overflow”, on page 7-7.
5. Otherwise, busy tone is given. This is the default.

Blocking status of the hunt group and its members is determined as follows:

- **If the pilot DN of the hunt group is dialed:** The blocking status of the pilot DN is checked, not those of individual members. If the pilot DN is blocked, hunting does not occur. If it is not blocked, normal hunting occurs.
- **If a member's DN is dialed directly:** The blocking status of the member’s is checked.

The hunt group—queuing feature provides an enhancement to the basic hunt group overflow on busy treatment. Refer to Section 7.8, “Hunt Group—Queuing”, on page 7-8.

7.2.3 Networking

- All members of a hunt group must reside in the same system.
- Calls delivered to members of pilot hunt groups cannot overflow or forward to a remotely located voice mail system.
- Calls originated by a hunt group member can route over a network interface.
- Calls arriving over a network interface can route to a hunt group interface.

Refer to Section 12.7.3, “Hunt Group”, on page 12-6 for more information about the interworking that takes place for this feature between the HiPath 8000 and a legacy PBX.

7.3 Hunt Group—Make Busy

7.3.1 Definition

The make busy feature permits a station to appear busy to incoming calls that hunt to the line. Calls to a line’s non-hunt DN are still permitted, as are call originations.

7.3.2 Functional Operation

To activate the make busy feature, the subscriber goes off-hook, receives a dial tone, and either enters the correct access code or presses the Hunt Make Busy key. The HiPath 8000 provides a confirmation tone, followed by dial tone.

To deactivate the make busy feature, the subscriber goes off-hook, receives a dial tone, and either enters he correct access code or presses the Hunt Make Busy key again.

When a hunt group member change the make-busy status, the member hears an announcement that indicates whether the service is active.

7.4 Hunt Group—Music On Hold

Refer to Section 5.16, “Music On Hold—HiPath 8000-Based”, on page 5-15.

7.5 Hunt Group—Night Service

7.5.1 Definition

The night service feature permits alternate routing of inbound calls to attendants or operators to devices such as the following when no AAP or attendant console application is available to take the call:

- Night agent telephone
- Automated attendant application
- Voice messaging server

Night service is supported for incoming calls to a business and for incoming calls to a business group attendant or attendant groups.

Refer also to Section 6.1, “Attendant Answering Position”, on page 6-1.

7.5.2 Functional Operation

The hunt group administrator specifies the night service DN.

The feature can be activated by either or both of the following methods:

- **Automatic activation:** This takes place when all members of the hunt group are in hunt—make busy state. Refer to Section 7.3, “Hunt Group—Make Busy”, on page 7-5.
- **Manual activation:** This takes place when a hunt group member activates the feature.

Calls received while a business is in night service can be routed to one or more preconfigured night answer destinations regardless of device type. For example:

- Announcement service

- Automated attendant application
- Night bell destination
- Another hunt group monitored and serviced by other routing applications—for example, an attendant or help desk application
- Intercept treatment

Night answering positions have the capability to:

- Extend calls to other destinations within the private network or to external destinations
- Camp on to busy stations
- Be recalled
- Access external trunk resources

The following are other characteristics associated with this feature:

- Authorized users can pick up calls alerting at night service destinations.
- Although calls alerting at night answer destinations are not prioritized by the HiPath 8000, prioritization may occur within applications monitoring night calls queued at hunt groups.

7.6 Hunt Group—No Answer Advance

The no answer advance feature can optionally be assigned to each hunt group's pilot DN. When a hunted-to station does not answer, this feature causes a resumption of the hunt from the non-answering station's position following the defined hunt sequence for the group.

This treatment can occur multiple times during the same termination attempt. Each time a call hunts to an idle line, the no answer advance timer is set, which permits the feature operation to occur upon a subsequent no-answer.

When the no answer advance feature is assigned, Auto Make Busy is allowed as an option. When it is assigned, a non-answering line subscribed to the hunt make busy feature is automatically marked Hunt Make Busy.

Refer also to Section 7.3, "Hunt Group—Make Busy", on page 7-5 for more information.

7.7 Hunt Group—Overflow

The hunt group—overflow feature permits an overflow DN to be assigned to the pilot DN. By doing so, it modifies the treatment of busy handling within the group by providing a fixed destination for routing the call.

7.8 Hunt Group—Queuing

7.8.1 Definition

Queuing provides an enhancement to the basic hunt group overflow on busy treatment, modifying both the determination and handling of busy conditions for the group. Refer to Section 7.2.2, “Functional Operation”, on page 7-4 for details about how busy conditions are determined, along with the sequence of treatment upon determining busy.

Each hunt group can optionally have an associated overflow queue to which calls are routed prior to the normal hunt group overflow DN. Queued calls are distributed to the next available line in the hunt group as it becomes available (on a first-in, first-out basis).

If the optional Maximum Time in Queue is not specified, a call remains in queue until either the caller abandons or a hunt group member becomes idle and the call is distributed. If it is specified, a call remains in the queue only for that maximum duration. The sequence of treatment upon exceeding that duration in queue is as follows:

1. If there is an overflow DN, the call is routed to it. Refer to Section 7.7, “Hunt Group—Overflow”, on page 7-7.
2. Otherwise, if there is a night service DN, the call is routed to it. Refer to Section 7.5, “Hunt Group—Night Service”, on page 7-6.
3. Otherwise, busy tone is given.

7.8.2 Functional Operation

The administrator can specify the following for each hunt group queue:

- Maximum number of callers that can be simultaneously queued (up to 511)
- Audible treatment heard by a caller while in queue (for example, customizable sequences of ringing, music, announcements, or combinations of these items). A media server is required to provide the audible treatment.
- Maximum time in queue threshold (0 [unlimited time] up to 43,200 seconds [12 hours]). This value is optional.

7.9 Hunt Group—Stop Hunt

7.9.1 Definition

The stop hunt feature provides the ability to terminate all hunting within the group when encountered on a member of the hunt group. It is checked during the hunt before moving to the next line in the hunt sequence. Calls to a line's private DN are still permitted, as are call originations.

7.9.2 Functional Operation

To activate the stop hunt feature, the subscriber goes off-hook, receives a dial tone, and enters #*93 or presses the Stop Hunt key.

To deactivate the stop hunt feature, the subscriber goes off-hook, receives a dial tone, and enters #*92 or presses the Stop Hunt key again.

7.10 Hunt Group—Traffic Measurements

7.10.1 Definition

The hunt group traffic measurements feature provides counts of hunt group and queuing activity on a per-hunt group basis. The hunt group administrator can use these measurements to monitor the company's calling patterns and usage at a high level, or can analyze them in greater detail if desired.

The basic traffic tool is another performance monitoring tool used to view snapshots of the traffic for incoming SIP calls to the HiPath 8000. Refer to Section 15.3, "Basic Traffic Tool", on page 15-3.

7.10.2 Functional Operation

The hunt group administrator specifies whether to maintain traffic statistics for a particular hunt group and the interval in which to collect them.

The hunt group measurement data is delivered to the *i*SMC or HiPath 8000 Assistant. The hunt group administrator can access the group's measurements and monitor the group by periodically performing a visual inspection of the reported data. However, some administrators may want to perform additional analysis of this data to determine:

- The average time a hunt group member spends on outgoing calls
- The number of calls that are not initially able to be connected to a hunt group member, and instead are overflowed or queued
- The number of calls that are unable to queue for a hunt group member because the queue is full
- The number of callers who hang up before speaking to a hunt group member

7.10.3 Measurement Types

Table 7-1 lists and describes the traffic measurements available for each hunt group.

Measurement	Description
Incoming calls	The number of incoming calls that attempt to terminate to the hunt group.
Outgoing calls	The number of outgoing calls originated by hunt group members.
Overflow calls	The number of incoming calls that are initially unable to connect to a hunt group member because no hunt group member is available.
Total usage	The total usage (in seconds) for calls incoming to and outgoing from the hunt group. For incoming calls, the usage measurement begins when the call is answered by a hunt group member. For outgoing calls, the usage measurement begins when the called party answers the call.
Queue attempts	When a queue is associated with the hunt group, the number of attempts to place a call in queue. It records both successful and unsuccessful attempts.
Queue usage	When a queue is associated with the hunt group, the total usage (in seconds) for all calls in queue.
Queue overflow	When a queue is associated with the hunt group, the number of attempts queue a call that failed because the queue was full.
Queue abandons	When a queue is associated with the hunt group, the number of queued calls abandoned by the originator before being connected to a hunt group member.

Table 7-1 Hunt Group Traffic Measurements

8 Emergency Calling Features

This chapter describes how the HiPath 8000 uses a Siemens or Cisco gateway, sometimes in conjunction with the Telident station translation system (STS), to provide emergency calling (E911) support. This chapter is applicable to the United States only.

Refer to the *HiPath 8000 E-911 Support and Planning Guide* for more information about this feature.

Refer to the following for information about administration and operational practices associated with this feature:

- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*

Contact your Siemens representative about the HiPath 4000 and third-party publications that pertain to this feature.

8.1 Definition

The emergency calling (E911) feature provides the capability to provide a caller's physical location and calling party number (CPN) to a public safety answering point (PSAP) dispatcher when a caller dials 911 to report an emergency.

This feature is targeted to United States customers located in states with regulatory requirements for E911. It may also be used in other countries that have regulatory requirements pertaining to emergency calling service from an enterprise system.

The HiPath 8000 uses one of the following configurations to provide this capability:

– Siemens HiPath 4000 in conjunction with a Telident STS

– Siemens RG 8700 (which permits the networking of a HiPath 4000 or non-Siemens QSIG PBX) in conjunction with CAMA trunks

– Cisco gateway in conjunction with a Telident STS

Although the Telident STS is not required for emergency calling in configurations that use the RG 8700, the enterprise can choose to incorporate one into its system for other purposes.

For simplicity, the remainder of this chapter uses the term *Siemens gateway* to refer to the HiPath 4000 and RG 8700, except where operation differs among the products.

Contact your Siemens representative about the use of other vendors' products with the HiPath 8000 for emergency calling.

8.2 Configuration Options

To provide emergency calling, an administrable local identification number (LIN) is required for each subscriber in the business group. A centralized automatic message accounting (CAMA) interface to the PSAP is also required.

When the HiPath 4000 or Cisco gateway is present, the following are the options to meet these requirements:

- **The HiPath 8000 is used to administer the LINs, and the Telident STS provides the CAMA interface.**

  To use this option, the administrator assigns the LINs and their associated routing in the HiPath 8000.

- **The Telident STS is used to administer the LINs; it also provides the CAMA interface.**

  This option might be more practical for an enterprise that already owns this equipment and already has its emergency database created.

When the Telident STS is not used, the LINs must be administered in the HiPath 8000 and sent to the gateways.

8.3 Functional Operation

A HiPath 8000 user has an emergency to report, dials the emergency number and expects to be connected to an emergency call center.

The call is handled according to the customer's preference and in compliance with applicable regulatory requirements. The options are as follows:

- The caller is connected directly to a PSAP's emergency services operator. In this scenario, the PSAP needs to know the location of the calling party to reach this location. Depending on how the LIN is administered:

– The HiPath 8000 sends the LIN to a gateway with a Telident STS or CAMA trunk.

  or

– The Telident STS associates the calling party number sent by the HiPath 8000 to the associated LIN in its database.

Depending on the gateway used:

– **HiPath 4000 or Cisco gateway**: The Telident STS sends the LIN to the PSAP using a CAMA trunk.

– **RG 8700 gateway**: The gateway sends the LIN to the PSAP using a CAMA trunk.

Based on the LIN or CPN, the PSAP dispatcher can obtain information such as the caller's address from the automatic location identification (ALI) database.

The information provided is not necessarily the user's information; it is the information associated with the device (telephone) used to make the emergency call.

- The caller is connected to an on-site emergency services operator. A subsequent emergency call from the operator routes to a local CO. Although third-party equipment can be used in this scenario, it is not necessary.

The following sections indicate the differences in operation, depending on the gateway used.

8.3.1 HiPath 4000 Gateway

The information flow from the HiPath 8000, to the Siemens gateway, and ultimately to the Telident STS, depends on the following:

- **If the LIN is administered in the HiPath 8000**: The HiPath 8000 sends the LIN to the Siemens gateway, which in turn sends it to the Telident STS.
- **If the LIN is administered in the Telident STS:** The HiPath 8000 sends the CPN to the Siemens gateway. Depending on the Siemens gateway operating mode, it sends either the associated LIN or the CPN to the Telident STS.

  In this scenario, the Siemens gateway operating mode determines if additional conversion or prefixing is required before the CPN is passed on to the Telident STS.

When the HiPath 4000 gateway is used:

1. The HiPath 8000 signals the user's calling party information to the Siemens gateway, as follows:

   - **If the LIN is administered in the HiPath 8000**: The HiPath 8000 sends the user's LIN.
   - **If the LIN is administered in the Telident STS**: The administrator configures the HiPath 8000 to send the CPN, which is the user's fully-qualified private number. If the user has a DID number, it is also sent as an additional party number (APN) operation.

   The signaling is performed in accordance with the CorNet-NQ protocol. The HiPath 8000 uses the SIP-Q tunnel to the HiPath 4000.

2. **If the HiPath 8000 sends the LIN to the Siemens gateway**: The Siemens gateway passes on the LIN to the Telident STS.

3. **If the HiPath 8000 sends the CPN to the Siemens gateway:** Depending on the operating mode of the Siemens gateway, one of the following takes place:

   - **If the Siemens gateway sends the LIN to the Telident STS:** If necessary, the Siemens gateway adds leading zeroes to the public network number via an outdial rule, to ensure that the number is 10 digits long. If no CorNet-NQ APN operation was received, the Siemens gateway outpulses the systemwide emergency number with the correct number of digits the Telident STS requires.
   - **If the Siemens gateway sends the CPN to the Telident STS:** The Siemens gateway converts the public network number via an outdial rule, to the length indicated by a Siemens gateway administrative parameter.

4. The Siemens gateway uses DTMF E&M trunks to route the call and signal the LIN or the public network number, as appropriate, to the Telident STS.

5. **If the Siemens gateway sends the LIN to the Telident STS:** The Telident STS converts the LIN to the 10-digit NANP CAMA MF format.

   If the Siemens gateway sends the CPN to the Telident STS: The Telident STS matches the public network number with the LIN in its database.

6. The Telident STS uses a CAMA trunk to transmit the LIN or CPN to the local PSAP.

8.3.2 RG 8700 Gateway

When the RG 8700 gateway is used:

1. The HiPath 8000 signals the user's calling party information to the gateway. When it sends the user's LIN, the signaling is performed in accordance with the CorNet-NQ protocol. The HiPath 8000 sends the LIN in the SIP body in the clear to the RG 8700.
2. The gateway converts the LIN to the 10-digit NANP CAMA MF format.
3. The gateway uses a CAMA trunk to transmit the LIN to the local PSAP.

8.3.3 Cisco Gateway

When the Cisco gateway is used:

1. The HiPath 8000 uses a SIP-Q interface to deliver the CPN to the Cisco gateway.
2. The Cisco gateway uses 2-wire FX trunks to send the LIN or CPN to the Telident STS. The number is sent via DTMF tones.
3. **If the Cisco gateway sends the LIN to the Telident STS:** The Telident STS converts the LIN to the 10-digit NANP CAMA MF format.

   If the Cisco gateway sends the CPN to the Telident STS: The Telident STS matches the public network number with the LIN in its database.
4. The Telident STS uses a CAMA trunk to transmit the LIN (and CPN, if available) to the local PSAP.

8.4 Guidelines for Implementation and Use

- The emergency number digits (such as 911, 9-911, or another pattern based on country requirements) are administered in the business group's dialing plan. The digit pattern is flagged as an emergency number.
- **If the LIN is administered in the Telident STS:** This feature relies on the calling party number of the caller to determine the LIN; therefore, it is viable only for emergency calls placed from devices that have a static or fixed location. The Telident STS database must be updated whenever a telephone is moved from one location to another. The customer is responsible to ensure local E911 regulations are followed with respect to device labeling.
- **Siemens gateway:** If an on-site operator is not used, the HiPath 8000 administrator must ensure that emergency calls are correctly routed. Although the Siemens gateway itself need not be in the same jurisdiction, it must be able to route the call to a gateway or Telident STS that is.

The HiPath 8000's rate area capabilities provide for source-based routing of emergency calls to the correct Siemens gateway when the enterprise network encompasses multiple E911 tandem switch jurisdictions.

- **Cisco gateway:** If the HiPath 8000 network spans PSAP jurisdictions, each local PSAP jurisdiction requires its own Cisco gateway and Telident STS.

  The HiPath 8000's rate area capabilities determine the local Cisco gateway to route the emergency call. For example, if the user originates from Los Angeles, the call must be routed to a gateway located in Los Angeles; if the user originates in Dallas, the call must be routed to a gateway located in Dallas.

  The emergency number digits in the transmitted called number must be "911". Although the emergency number can be configured to be other digits in the HiPath 8000, it must then be converted to "911" when the call is sent to the Cisco gateway.

  Contact your Siemens representative about the feasibility of variable emergency call digits within the Cisco gateway.

9 Routing and Translation Features

This chapter describes the HiPath 8000 features that provide routing and translation, including public numbering plan compliance and routing that varies depending upon such factors as origin, traffic, and bearer capability.

Refer to the following for information about administration and operational practices associated with these features:

- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*

9.1 Digit Modification for Digit Outpulsing

The digit modification for digit outpulsing feature provides support for selectively deleting any number of leading digits (up to all digits) from the destination number, prefixing new leading digits to the destination number, or both. Digit modification is based on the combination of the destination code and the route.

Calls to different destinations that share the same route may require modifying digits differently; and calls to the same destination that are routed over different routes (as with alternate routing) may also require modifying digits differently.

9.2 Directory Number Announcement

9.2.1 Definition

The directory number (DN) announcement feature permits callers to determine the DN of the line that they're calling from. This feature is especially useful for service personnel, because it enables them to verify that the correct line pair is assigned to the DN that is expected.

9.2.2 Functional Operation

When the user enters *99, a connection is made to an announcement that states the DN of the line from which the call is being made.

9.3 E.164 Compliance

9.3.1 Definition

The E.164 compliance feature provides the ability to dial or receive any E.164 compliant number.

9.3.2 Functional Operation

The subscriber can dial any number, including international prefixes and country codes. The international public telecommunication number code fields are the country code and the national (significant) number. The national (significant) number may consist of a national destination code (NDC) and subscriber number, where the NDC may be optional in some countries.

9.4 Intercept Treatment

9.4.1 Definition

The intercept treatment feature provides the ability for the HiPath 8000 to use media servers to generate tones and announcements indicating various failure or other conditions the calling party may encounter on a dialed call.

9.4.2 Functional Operation

Intercepts are sequences of up to three tones, announcements, or a combination of tones and announcements. The HiPath 8000 and its media server repeats the intercept a specified number of times. The intercept helps to provide explanatory information when a call fails to complete as dialed. The tones and announcements are available as audio clips encoded on the media server.

The HiPath 8000 administrator can specify a tone's duration and also whether an announcement is barge-in or non-barge-in.

9.4.3 Networking

- Intercept destinations cannot exist across the network interface.
- Refer to Section 12.7.4, “Intercept Treatment”, on page 12-7 for information about the interworking that takes place for this feature between the HiPath 8000 and a legacy PBX.

9.5 International Translation Support

The international translation support feature provides E.164 capabilities needed to address international requirements, such as the handling of hexadecimal digits in the prefix table and the E.164 routing tables.

9.6 Leading Digit and Most-Matched Digit Translation

The leading digit and most-matched digit translation feature provides the following mechanisms to quickly and accurately route calls

- **Leading digit translation** can be completed at different points (*n* leading digits in the destination codes provisioning, where *n* is 1 through 15) in a destination code. This ability permits translation and routing decisions to be made based on country codes, area codes, or office codes.
- **Most-matched digit translation** always searches for the longest matching digits to determine the destination. It is used to resolve ambiguity in the codes.

9.7 North American Numbering Plan Compliance

The North American numbering plan (NANP) features provide support for NANP dialing, including toll-free, 555, N11 Codes, and vertical service codes. The NANP conforms to the E.164 specification.

Telephone numbers in the NANP are of the form NPA-NXX-XXXX, where:

- NPA is a 3-digit numbering plan area code and is of the form NXX.
- NXX is a 3-digit central office code.
- XXXX is a 4-digit station (or line) number.
- N represents any digit from 2 through 9.
- X represents any digit from 0 through 9.

The NXX form is restricted to exclude N11 codes.

9.7.1 555-1212 Line Numbers

The 555-1212 line numbers feature provides support for 555-1212 numbers for directory assistance.

9.7.2 Carrier Access Codes

The carrier access codes (CAC) feature provides three-digit access codes that are sent in conjunction with four-digit carrier identification codes (CICs). The format of CAC is three digits preceding a four-digit CIC. For example, the CAC/CIC for MCI is 1010222.

CICs are used to select a common carrier other than the pre-assigned default common carrier, on a per-call basis when originating an intra-LATA or inter-LATA public network toll call. This is known as *equal access*.

For certain PBX applications that provide telephone service to the general public (such as hotels, hospitals, universities, and airports), known as *call aggregators*, the FCC requires an originating user be given the opportunity to select the common carrier of his/her choice using equal access. Other PBX applications, such as private businesses, utilize equal access to save money by selecting the least expensive common carrier using least-cost routing (LCR). For calls placed via gateway trunks to an equal access central office:

- Both the CAC and CIC are signaled to the public network in a dialable format (digit string).
- Only the CIC is sent over SIP-Q.

9.7.3 Destination Codes

The destination codes (DN codes) feature provides destination codes for basic telephone service which may consist of 3 (N11), 7 (NXX-XXXX) or 10 digits (NPA-NXX-XXXX). The 3-digit format is limited to N11 codes. Vertical service codes (VSC), carrier access codes (CAC) and speed calling codes are not included. The HiPath 8000 allows 10-digit calls to as many as 150,000 NPA-NXX combinations.

9.7.4 Interchangeable NPA and NXX

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

9.7.5 Prefix Digit Translation

This feature provides the translation of the international and national prefixes that are used. Normally, the international prefix is 00 and the national prefix is 0, but this feature allows other combinations of digits to be used as the international or national prefix as specified by the dialing plan.

9.7.6 Service Access Codes

The service access codes (SAC) feature provides support for 700, 800, 877, and 900 services via NPA codes.

9.8 Routing Features

9.8.1 A-Side Signaling-Based Routing

The A-side signaling-based routing feature provides for the selection of a route to a destination based on the signaling protocol of the originating party.

9.8.2 Alternate Routing

The alternate routing feature provides flexibility to support different routes. It provides for the delivery of traffic from a specific subscriber to the network specified by the HiPath 8000 administrator. It also provides the capability to specify a prioritized list of possible routes to reach the destination.

The HiPath 8000 evenly distributes the load across routes with the same priority, but may use a lower-priority route if the first choice is overloaded or congested, or if the physical equipment is temporarily unavailable.

9.8.3 Alternate Routing with Overflow Among Route Types

The alternate routing and overflow among route types feature provides for calls to be routed to the same destination via alternate routes where a route can be a trunk group, a primary rate interface (PRI), a SIP-Q gateway or gatekeeper, or a SIP server. The routes leading to a destination can be prioritized for routing purposes. Moreover, if one route (such as a trunk group) is unavailable, the call can overflow to a different route even if it is of a different type (such as a PRI or a SIP server).

9.8.4 Bearer Capability Routing

The bearer capability routing feature allows the routing of calls to different trunk groups based on the originator's bearer capability. For example, all 64 kbps bearer calls can route to one trunk group and all other bearer capabilities to a different trunk group.

The bearer capability of a call can be one of the following:

- Speech
- 3.1 kilohertz (kHz) audio
- 64 kbps
- 56 kbps (or 64 kbps, rate adapted from 56 kbps)

9.8.5 Origin-Dependent Routing

The origin-dependent routing feature allows assigning rate area and class of service to trunk groups, lines, and PRI lines. During routing, originating rate area and class of service are obtained from the incoming trunk group, line, or PRI line and is used to select routes.

9.8.6 Rerouting Based on SIP Response Codes

SIP calls can be rerouted if:

- A gateway cannot process a connection request. The calls can be of type off-net (to the PSTN via a SIP gateway) or on-net (to another SIP network such as OpenScape).
- A WAN failure occurs. SIP calls between subscribers are rerouted through the PSTN.
- A SIP response code indicates a bandwidth restriction.

This ability is particularly useful for call admission control. Refer to Section 10.4, “CAC Rerouting”, on page 10-4.

The rerouting feature can be turned off and on system-wide, and the SIP response codes upon which rerouting is provided are provisionable in the system. A rerouting timer also provides rerouting if no response is received from the SIP gateway or SIP server after an INVITE has been sent.

In the following description of requirements to reroute calls, a *survivable branch* refers to a gateway switch such as the RG 8700 or Comdasys Convergence 1600. When the host (HiPath 8000) connection is lost, the survivable branch permits subscribers to continue to make calls locally (SIP-to-SIP), as well as calls to and from the PSTN (SIP-to-ISDN and ISDN-to-SIP), including E911 calls.

Refer to the *HiPath 8000 Overview Guide* for more information about survivable branches.

For a call to be rerouted, the calling subscriber must either be calling from a different survivable branch, or be directly registered with the HiPath 8000. The called subscriber must:

- Be registered from a survivable branch.
- Reside in that survivable branch. This means that the called subscriber must be registered with its provisioned survivable' IP endpoint. This endpoint is administered through the *i*SMC or HiPath 8000 Assistant.
- Have a valid public E.164 number.

9.8.7 Time-of-Day Routing

The time-of-day routing feature allows the routing of calls to the same E.164 destination code via different routes depending on the time of day and the day of the week.

The HiPath 8000 administrator can create time-of-day destinations. A time-of-day destination can have one or more day schedules (for example, a weekday schedule, a weekend schedule, and a holiday schedule) with each day of the week being associated with its own schedule.

9.9 Vertical Service Codes

The vertical service codes (VSCs) feature provides for user-dialed codes, such as feature access codes, that allow access to features and services. Services invoked by VSCs include HiPath 8000-based station call forwarding, customer-originated trace, and many others.

Refer to the individual feature descriptions for specific information about associated access codes.

Refer to Appendix B, “Feature Access Codes” for a comprehensive list of access codes the HiPath 8000 supports.

9.10 Virtual DN

The virtual DN feature permits the system administrator to create a DN that does not have a connection. The DN can be used for station RCF or it can be a means of reserving a number for future use.

If the DN is being used for station RCF, it cannot be subscribed to any other services. Refer to Section 4.8, “Call Forwarding, Station—Remote Call Forwarding”, on page 4-10 for more information.

10 Call Admission Control Features

This chapter describes the HiPath 8000's integrated call admission control (CAC) feature, which provides for management of the bandwidth used for the transport of media traffic (such as RTP audio and T.38 fax) through the bottleneck links that may exist in an enterprise network.

Refer to the following for information about administration and operational practices associated with this feature:

- *HiPath 8000 SOAP/XML Subscriber Provisioning Interface Guide*
- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*

10.1 Definition

The call admission control (CAC) feature ensures that real-time media calls are only established when the necessary bandwidth resources are available on all access links that exist between the two communicating endpoints.

Real-time media calls should not be routed over networks that cannot guarantee an acceptable quality of service (QoS). An enterprise core network and the subnets serving its branch offices must provide sufficient bandwidth to support the real-time media traffic they are required to handle. It is also necessary for the real-time media packets to be correctly classified so that the network routers can provide the appropriate priority processing through their queues.

Loss of media packets can still occur at the aggregation layer that exists on bandwidth-limited access link that exists between a branch office LAN and the core network WAN. This can happen when the total bandwidth capacity of the access link is overbooked to an extent that forces the access routers to drop even high-priority real-time media packets. The result is a poor quality connection for all multimedia calls that are routed over the overbooked access link.

CAC provides the bandwidth management that prevents these poor-quality connections from being established.

10.2 CAC Groups and Policies

A *CAC group* represents the group of endpoints being served by the bandwidth-limited link which needs to be monitored. CAC groups are defined based on one of the following parameters:

- Subnet
- Directory number: this can be a DN prefix (such as 1561555*) or the DN of a single user (such as 15615550110)
- IP address

A *CAC policy* specifies the information to be applied to the CAC group or groups associated with it. Each CAC policy contains the following information:

- The CAC group to which the policy applies. The policy applies to all calls to and from the CAC group.
- The traffic type controlled by the CAC policy— audio, fax, or both.
- The capacity limits the policy enforces for a primary link and optionally for a secondary (backup) link. The primary and secondary capacities can be defined based on the number of calls, bandwidth limit, or both, as follows:
  - **Number of calls:** The concurrent calls per policy are counted. When the limit is reached, no new calls are admitted.
  - **Bandwidth limit:** The HiPath 8000 calculates the used bandwidth based on the negotiated codecs in the session description protocol (SDP).

    This value is the common limit for both upstream and downstream traffic. For example, if a value of 1 Mbps is entered it indicates that the upstream bandwidth is 1Mbps and the downstream bandwidth is 1Mbps as well.
  - **Both**: If both are defined, the limit is enforced as soon as one is reached.

The primary and the secondary link capacities must use the same criteria. For example, if the primary capacity is based on bandwidth limit, the secondary capacity must also be based on bandwidth limit.

- Whether calls to the media server to play announcements/tones or to collect digits are allowed even if insufficient bandwidth is present.
- Whether answered calls are allowed even if insufficient bandwidth is present. This can occur in scenarios in which the resource reservation only takes place when the destination answers (when the SDP offer is included in the SIP 200 OK response).

- The IP address and name of the WAN access router serving the CAC group (such as a branch office) that sends SNMP traps indicating the link up/down status of the primary access link. This item is only required if the optional Link Failure Web Service is used. Refer to the *HiPath 8000 Web Services SDK (Software Development Kit), Application Developer's Guide for Link Failure Management* for more information about this Web service.

One CAC policy can be related to one CAC group. A CAC group, on the other hand, can be related to up to two CAC policies. This permits the use of allow different policies for audio and fax traffic for the same group.

Only the following combinations are allowed for CAC policies related to the same CAC group:

- One policy for audio and/or one policy for fax

  -or-

- One policy for both audio and fax

10.3 Functional Operation

A resource manager (RM) function within HiPath 8000's universal call engine (UCE) integrates bandwidth management with call processing in order to provide robust call handling, such as the rerouting of a call via the PSTN when there is insufficient bandwidth in the enterprise network to carry the call, based on bandwidth availability.

When a new call is placed, the following takes place:

1. The predicted bandwidth needed for the new call is compared to the remaining available bandwidth for each bottleneck link in the connection based on the CAC group and policies assigned to the originating and destination endpoints.
2. The HiPath 8000 reserves the bandwidth and allows the call to proceed if there is sufficient bandwidth on each bottleneck link in the route.
3. After the call is answered and connected, HiPath 8000 adjusts the bandwidth reservation for the call based on the actual negotiated codec that is selected by the source and destination endpoints.
4. After the call is released, the bandwidth resource is also released.

The HiPath 8000 reroutes or denies the call if there is insufficient bandwidth on any of the bottleneck links. Refer to Section 10.4, "CAC Rerouting" and Section 10.5, "Call Denial", on page 10-5.

10.4 CAC Rerouting

One of the benefits of the integrated CAC solution is the HiPath 8000's ability to provide rerouting via the PSTN in case there is not enough bandwidth in the bandwidth-limited link from the branch office to the WAN. The rerouting call scenarios are tightly coupled with the HiPath 8000's ability to reroute calls based on a provisionable set of SIP response codes. Refer also to Section 9.8.6, "Rerouting Based on SIP Response Codes", on page 9-6.

Among other things, this feature provides for the rerouting of calls to SIP gateways or SIP subscribers if the HiPath 8000 receives a SIP response code indicating a bandwidth restriction (for example, `606 Not Acceptable`).

For the integrated CAC solution, the HiPath 8000 does not actually receive a SIP 606 response code from the terminating B-side of the call. However, the RM function in the terminating SIP session manager internally responds with the same error message as if a SIP 606 response code was received in response to an INVITE message sent to the B-side. No INVITE message is actually sent to the B-party in case of bandwidth limitation.

10.4.1 Rerouting Calls to SIP Subscribers

Rerouting of calls to SIP subscribers via the PSTN can be performed if the following conditions are met:

- The called SIP subscriber is registered from a survivable branch.
- The called SIP subscriber resides in that survivable branch. This means that the called SIP subscriber is registered with its provisioned survivable SIP endpoint (its SIP proxy). The administration of the called SIP subscriber to become survivable is enabled by assigning the Survivable SIP Proxy as the associated SIP Endpoint to the SIP subscriber.
- The called subscriber has a valid public E.164 number. Refer also to Section 9.3, "E.164 Compliance", on page 9-2.
- The calling SIP Subscriber is calling from a different survivable branch or is directly registered with the HiPath 8000.

  - or -

- The calling device is a SIP endpoint (SIP gateway) that has the rerouting option set, and there is a last diverting user for the call which is a provisioned SIP subscriber of the HiPath 8000.

For example, assume that a SIP subscriber in the Boca Raton, Florida, branch calls a SIP subscriber in the San Jose, California, branch. This scenario requires the RTP payload to route through the bandwidth-limited links that connect the Boca and the San Jose branch offices to the WAN.

If there is not enough bandwidth available in either link, the resource reservation is not successful and the RM function sends a negative response equivalent to a SIP 606 response code. The HiPath 8000 then reroutes the call between these two subscribers through their local SIP gateways and the PSTN.

10.4.2 Rerouting PSTN Calls to Alternate SIP Gateways

PSTN calls can also be rerouted to alternate SIP gateways.

For example, assume that the HiPath 8000 is provisioned for tail-end hop-off. Whenever a Boca Raton subscriber dials a local number in San Jose, the PSTN gateway in San Jose is chosen as the first route out the network, making this otherwise long-distance call a local call in San Jose and therefore less expensive.

This scenario, however, requires the RTP media stream to go through the bandwidth-limited links that connect the Boca and the San Jose branch offices to the WAN.

If there is not enough bandwidth available in either link, the resource reservation is not successful and the RM function generates a negative response equivalent to a SIP 606 response code. The HiPath 8000 then reroutes the call via the local gateway in Boca Raton to reach the San Jose number via the PSTN.

10.5 Call Denial

Important Note

The information in this section is only applicable to non-emergency calls. CAC never denies emergency calls.

When CAC rerouting is not possible or is not configured, the HiPath 8000 returns the SIP 606 response code to the calling SIP endpoint. It is a function of the SIP endpoint as to how the 606 response code is handled; the tone/announcement and display that is provided to the calling user for a 606 response code is a local function of the endpoint.

10.6 Dynamic Handling of Link Failures

The HiPath 8000 permits optional provisioning of primary and secondary link capacities for each CAC policy. The ability permits the supports of an access router that can switch over to a backup link (with a different bandwidth capacity) than the primary link, if the primary link to the WAN fails.

The primary or secondary capacity can be dynamically selected by the customer's network management system (NMS) via a SOAP/XML interface. If the NMS becomes aware of an access router's link failure, it uses the Link Failure Web Service to notify the HiPath 8000 to use

the secondary capacity for the CAC policy of the associated access link. If the primary link access is restored, the Link Failure Web Service also provides a command to the HiPath 8000 to switch back to the primary capacity of the CAC policy.

10.7 Traffic Measurement

The following measurements are collected for each provisioned CAC group:

- CAC Group Name
- Number of Offered Calls
- Number of Blocked Calls

The CAC measurements are stored in a log file for post-processing.

11 PRI Features

This chapter describes HiPath 8000 features that support network-side PRI capabilities.

Refer to the following for information about administration and operational practices associated with this feature:

- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*

Contact your Siemens representative about the HiPath 4000 publications that pertain to these features.

11.1 Calling Number Delivery over PRI

This feature provides for the delivery of the calling party number for calls terminating to the PRI.

11.2 Calling Number Delivery over PRI—Emergency Calls

For emergency call originations, this feature identifies the DN to use as the calling number, the received number, or the default DN defined against the PRI.

11.3 Calling Number Screening over PRI

This feature provides for the screening of the received calling number from the PRI to compare against the list of DNs related to the PRI.

11.4 PRI—Supported and Unsupported Features

The following PRI features are supported:

- B-channel selection algorithm: Low-Low and High-High
- PRI hunt group policies:
  - Sequential forward
  - Sequential backward
  - First-in-first out
  - Round robin forward
  - Round robin backward
- B-channel availability control, also known as *B-channel availability signaling (BCAS) procedures*.
- Delivery of redirecting number

The following PRI features are not supported:

- Non-facility associated signaling (NFAS) (20 DS1)
- NFAS with D-channel backup (20 DS1 + 2 D-channel)
- Channel negotiation
- Calling name delivery
- Delivery of redirecting name
- Call-by-call service
- PRI 2 B-channel transfer
- Redirecting number privacy override

11.5 PRI Trunking

The PRI trunking feature provides for control of network-side PRIs terminating at a trunk gateway. Support of the National ISDN 2 (NI-2) protocol, as well as Nortel DMS and Lucent 5ESS variants, is provided.

12 QSIG Tunneling Features

This chapter describes SIP-Q, which permits the HiPath 8000 to interwork with another HiPath 8000, the HiPath 4000, or a QSIG PBX connected via the RG 8700 gateway.

- Refer to the following for information about administration and operational practices associated with this feature:
  - *HiPath 8000 Configuration and Administration Using CLI Guide*
  - *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
  - *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
  - *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
  - *HiPath 8000 Assistant Administrator Documentation*
  - *HiPath 8000 Configuration and Administration Using HiPath Assistant*
  - *HiPath 8000 Assistant Feature Configuration Administration Guide*
- Refer to the *HiPath 8000 Network Planning Guide* for information about network planning.
- Contact your Siemens representative about the HiPath 4000 and RG 8700 publications that pertain to this feature.

12.1 Definition

- *QSIG* is a signaling protocol that permits the interconnection of other vendors' QSIG-compliant PBXs (*QSIG PBXs*) to Siemens PBXs. It also provides for IP network connectivity.
- *CorNet-NQ* is a Siemens proprietary QSIG-based signaling protocol for interconnecting HiPath 8000 systems to one or more QSIG PBX systems. It is a superset of the QSIG-defined Q.931/Q.932 protocol extensions.

The SIP-Q signaling method permits the HiPath 4000 and RG 8700 to interoperate with the HiPath 8000. It also supports tunneling of QSIG/CorNet-NQ protocol over SIP protocol as a trunking interface— for example, between two HiPath 8000s.

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

SIP-Q supports the following CorNet-NQ sections and supplementary services:

- Sections 1 through 4: CorNet Signaling, Protocol Structure, Messages, Information Elements (IEs), and Call Control Procedures
- Section 5, Generic Functions
  - Section 5.1.2, CorNet-N Transport
    - CDR
  - Section 5.1.8, Manufacturer-Specific Information
  - Section 5.1.9, Classmarks
  - Section 5.2.2, Call Completion (CCBS/NR)

    Refer also to Section 5.2, “Automatic Callback”, on page 5-3.
  - Section 5.3.1, Identification Services

    This includes support for Additional Party Number (APN), which permits the calling party’s public number (for sending to PRI) and private number (for billing purposes) to be sent to a gateway.
  - Section 5.3.3, Message Waiting Indication

    Refer also to Section 18.9, “Message Waiting Indicator”, on page 18-3.
  - Section, 5.3.6 Name Identification Services
  - Section 5.3.10, Emergency Services (E911 LIN)

    Refer to Chapter 8, “Emergency Calling Features” for information about differences in how the HiPath 8000 sends the LIN to each type of gateway in emergency calling scenarios.
  - Section 5.4.1, Call Diversion/Forwarding
  - Section 5.6.1, Hold/toggle/consultation
  - Section 5.6.2, Call transfer (blind, semi-attended and consultation)
- Section 7.1, Private Numbering plan
- Section 7.2, Carrier Services: Carrier Identification Code

  The digits are sent out-of-band rather than inband.

- Section 9.1, Path Replacement
- Section 9.8, Additional Progress Description

SIP-Q also provides the following features network-wide:

- SIP-Q-to-SIP-Q pass-through—for example, when a legacy user is routed over IP to another legacy user located a distance away. This capability can save TDM costs for an enterprise.
- Failover recovery superior to that of H.323 standard communications.

12.2 Functional Operation

The following are the interworking requirements:

- Interworking between the HiPath 8000 and the HiPath 4000 requires the HiPath gateway 3540 (HG 3540) board, which is an integrated gateway used for IP network connectivity that gives the HiPath 4000 access to IP-based trunking. It serves both line- and trunk-side SIP interfaces.
- Interworking between the HiPath 8000 and a non-Siemens QSIG PBX requires the RG 8700 gateway.

The following support is provided:

- SIP-Q session manager requirements
- ECMA 355 standards
- IPsec over SIP

The HiPath 8000 acts as a SIP user agent server (UAS) for outgoing calls on behalf of the gateway. In the other direction, the HiPath 8000 acts as a SIP user agent client (UAC) for incoming calls on behalf of the gateway.

12.3 Release Links

Release links are implemented as part of the SIP-Q functionality, and can also be used in a mixed (multi-vendor) environment. Release links provide the following:

- A solution that optimizes the media path through the network
- A clean solution that allows for releasing unnecessary media and signalling links in mixed networks

This is accomplished by implementing the following:

- Supplementary Service Call Transfer (SS-CT)
- Transit functionality
- Path Replacement additional network feature (ANF-PR)

Refer also to Section 12.6, “Transfer”, on page 12-5.

12.4 Call Diversion Over Multiple Platforms

The SIP-Q Interworking for the Call Diversion Service feature is implemented as part of the SIP-Q functionality so it can be used in a mixed (multi-vendor) environment. This feature provides:

- The ability to avoid trombone trunk connections between HiPath 8000 and gateways (by the implementation of throwback forwarding when necessary)
- The ability to forward calls to messaging systems across multiple platforms

Refer also to Section 18.9, “Message Waiting Indicator”, on page 18-3.

12.5 Call Hold

Refer also to the applicable user manual for a description of this feature.

- If a legacy user calls a HiPath 8000 subscriber, the legacy user puts the HiPath 8000 subscriber on hold. The originating caller can optionally use a local music source for the party on hold.
- If a HiPath 8000 subscriber calls a legacy user, the call is placed on hold. A reroute occurs if a music source is attached.

12.6 Transfer

Refer also to Section 5.28, “Transfer”, on page 5-32.

The QSIG SS-CT and ANF-PR operations are supported for transfer by join (both attended and semi-attended transfers) and blind transfer scenarios in which one of the parties is a SIP-Q gateway. From the QSIG perspective, the HiPath 8000 can be a transferring, transferred and transferred-to PBX.

- Subscribers can invoke transfer by join if provisioned (existing permission/classmark required).
- The transferring party (User A) can invoke transfer by join regardless of the features (such as forwarding or call waiting) that are enabled or disabled at the transferring device or system.
- If the transfer by join fails for any reason, the transferring party is reconnected to the transferred party of the original call. This reconnection occurs as a recall of the transferred party B on behalf of the transferring party A. This applies to both attended and semi-attended transfer cases. The same is also applicable to blind transfer scenarios.
- After a SIP-Q call transfer, the displays of the connected parties are updated with their partner's name and number.

12.7 Local Feature Interworking

For simplicity, the remainder of this section uses the term *legacy user* to refer to users located as follows:

- Behind a HiPath 4000 by way of the HG 3540 gateway
- Behind a non-Siemens QSIG PBX by way of the RG 8700 gateway

The following sections describe feature operation when a legacy user is involved in the connection.

12.7.1 Call Pickup—Group

Refer to Section 7.1, “Call Pickup—Group”, on page 7-1 for a description of this feature.

- If a HiPath 8000 subscriber calls a legacy user, another legacy user in the same PBX can pick up the call.
- If a legacy user calls a HiPath 8000 subscriber, another HiPath 8000 subscriber can pick up the call.
- A pickup group member can only pick up calls in the same PBX as the ringing telephone. For example:
  - If a HiPath 8000 subscriber calls a legacy user, a HiPath 8000 subscriber cannot pick up the call.
  - If a legacy user calls a HiPath 8000 subscriber, another legacy user cannot pick up the call.

12.7.2 Caller Identity Service

Refer to Section 5.4, “Caller Identity Service”, on page 5-4 for a description of this feature.

- Between the HiPath 8000 and the HiPath 4000, the HiPath 8000 sends both public and private calling party numbers if both are provisioned—for example, for use by CDR and sending to the public network.
- The displays of HiPath 8000 subscribers involved in call transfer, call forwarding, hold/retrieve, and call pickup situations provide the name and number of the calling, alerting, and connected parties as long as both parties are in the same business group.

12.7.3 Hunt Group

Refer to Section 7.2, “Hunt Group”, on page 7-3 for a description of this feature.

Hunting can only occur between users on the same PBX. For example:

- If a HiPath 8000 subscriber calls a legacy user, the call is hunted to a legacy user in the same PBX. This situation is treated similarly to station call forwarding.
- If a legacy user calls a HiPath 8000 subscriber, the call is hunted to a HiPath 8000 subscriber.

12.7.4 Intercept Treatment

Refer to Section 9.4, “Intercept Treatment”, on page 9-2 for a description of this feature.

- Intercepts can only occur at the terminating user’s PBX. For example:
  - If a HiPath 8000 subscriber calls a legacy user, the call can be intercepted to another legacy user in the same PBX.
  - If a legacy user calls a HiPath 8000 subscriber, the call can be intercepted to another HiPath 8000 subscriber.
- If a legacy user calls another legacy user in the same PBX, the call can be intercepted to a HiPath 8000 subscriber if the intercept destination at the legacy PBX is configured for a HiPath 8000 private network address.

12.7.5 Three-Way Calling and Voice Conferencing

Refer also to the following:

- The applicable user manual
- Section 5.11, “Conference, Station-Controlled”, on page 5-11
- Section 16.10, “Interworking with Voice Conferencing Applications”, on page 16-7

- Conference notification is not provided.
- If a HiPath 8000 subscriber (A) is connected to a legacy user (B) and another HiPath 8000 subscriber (C) calls A, A consults with C and then invokes conference with all three.
- If a legacy user (A) is connected to another legacy user in the same PBX (B) and a HiPath 8000 subscriber (C) calls A, A consults with C and then invokes conference with all three.

- If a HiPath 8000 subscriber (A) is connected to a legacy user (B) and another legacy user in the same PBX (C) calls A, A consults with C and then invokes conference with all three.
- If a legacy user (A) is connected to a HiPath 8000 subscriber (B) and a legacy user in the same PBX (C) calls A, A consults with C and then invokes conference with all three.
- If a legacy user (A) is connected to a HiPath 8000 subscriber (B) and another HiPath 8000 subscriber (C) calls A, A consults with C and then invokes conference with all three.

12.7.6 Voice Mail

Refer to Section 16.11, “Interworking with Voice Mail Systems”, on page 16-8 for a description of this feature.

If a HiPath 8000 subscriber calls a legacy user via voice mail, the call can be transferred to another legacy user in the same PBX.

12.8 CDR

When a call spans mode than one node, a global call identifier correlates and combines information from multiple CDRs that pertain to the same call. Refer to Section 13.2, “Call Detail Record Generation”, on page 13-1.

13 CDR Features

This chapter describes the CDR features that simplify call tracking and billing for the HiPath 8000.

- Refer to the *HiPath 8000 Call Detail Recording (CDR) Reference Guide* for detailed information about CDR.
- Refer to the following for information about administration and operational practices associated with these features:
  - *HiPath 8000 Configuration and Administration Using CLI Guide*
  - *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
  - *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
  - *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
  - *HiPath 8000 Assistant Administrator Documentation*
  - *HiPath 8000 Configuration and Administration Using HiPath Assistant*
  - *HiPath 8000 Assistant Feature Configuration Administration Guide*
- Refer to specific feature descriptions for information about the CDR data associated with the feature.

13.1 Billing for Business Groups

Refer to Section 6.5, “Business Group Billing”, on page 6-4.

13.2 Call Detail Record Generation

The CDR generation feature provides comprehensive call accounting data. The HiPath 8000 generates call records that include information such as the following:

- Date and time
- Originating account number
- Destination telephone number
- Carrier identifiers

- Trunk group or PRI group identifiers, if applicable
- Global call identifier, which correlates and combines information from multiple CDRs that pertain to the same call—for example, when a call spans more than one node
- Thread identifier, which correlates separate calls that are part of a complex call scenario—for example, when a call is transferred with consultation
- Other related information

The HiPath 8000 also provides CDR information for unsuccessful calls. A termination reason code describes the reason for termination for all calls, regardless of whether they are successful or unsuccessful.

When calls are forwarded, either via telephone-based or HiPath 8000-based forwarding, multiple CDRs (*standard CDRs* and *call forwarding CDRs*) are generated. Refer to Section 4.13, “CDR”, on page 4-14.

All CDRs are stored in flat files. After they are pushed to the billing server, the files can be:

- Deleted immediately
- Saved, then automatically deleted after a specified retention period
- Saved until the administrator manually deletes them

13.3 Intermediate Long Duration Records

The intermediate long duration call detail records feature provides the capability to generate intermediate CDRs containing full call information after an administrable time period elapses. The termination reason code associated with the record indicates *Intermediate CDR*. This information is stored as separate files for backup purposes.

13.4 Security

Refer to Section 14.2, “Billing Records Security”, on page 14-2 and Section 14.15, “Secure Storage of CDR Password”, on page 14-11.

13.5 Usage Reporting

The usage reporting feature provides for the generation of CDRs for all calls, distinguishing between completed and non-completed calls (ring no answer, busy status). The CDRs include, for example:

- Date and time
- Carrier ID code
- Originating account number
- Destination telephone number
- Duration of call in tenths of seconds
- Calling party number (if available)
- Call status

For the United States, the reference time clock is the United States Department of Commerce's atomic clock timeserver in Boulder, Colorado. Other local, national or international time servers may be used for international markets.

14 Security Features

This chapter describes the HiPath 8000 features that provide security for various aspects of the system, such as billing records, data files, and administration interfaces.

Refer to the following for information about administration and operational practices associated with these functions and features:

- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*

Refer to the *HiPath 8000 Security Reference and Planning Guide* for detailed information about HiPath 8000 security.

14.1 Account and Password Management Security

This feature provides password complexity, reuse, and aging rules. It also disables dormant accounts and locks out users after a number of failed logon attempts.

The HiPath 8000 implements these options at the OS level using standard pluggable authentication module (PAM) techniques. As is standard for Linux, changing the default options requires editing of PAM configuration files.

The administrator can specify attributes associated with the following:

- Password complexity—for example, minimum password length and required number of character classes
- Password reuse—for example:
  - Verification that a new password is not the same as any of the last six passwords used
  - Verification that a new password has not been used in the last six months
  - Number of days between password reuse

- Password aging—for example:
  - Waiting period between password changes
  - Number of days a password is valid
  - Warning interval to notify the user that the password is about to expire
- Dormant account handling—for example:
  - Dormancy time period before an account is disabled
  - Number of days of non-use after which an account is disabled or automatically deleted
  - Administrators who are authorized to activate a disabled account
- Locked-out account handling—for example:
  - Number of failed logon attempts before the account is locked out
  - Whether an administrator must manually remove the lockout, or if it is automatically removed after a specified time period
  - Administrators who are authorized to remove locks

14.2 Billing Records Security

14.2.1 Definition

The security of billing records feature provides for the secure and reliable generation and storage of CDRs. This feature is also known as *CDR security*.

Refer to Section 14.15, “Secure Storage of CDR Password”, on page 14-11 for information about how the HiPath 8000 secures CDR passwords.

14.2.2 Functional Operation

CDRs are buffered in the duplicated main memory of the HiPath 8000 and their content transferred to a CDR file on the duplicated persistent storage. Therefore, the maximum amount of data that could be lost in the event of a total system outage is limited to the content of the CDR buffer of the main memory. The CDR data output to a disk file ensures that the probability of CDR data loss is minimized.

The type of file transfer protocol depends on the entity that initiates the CDR transfer:

- If the HiPath 8000 initiates CDR transfer (also known as file transfer by *push*), file transfer protocol (FTP) must be used.

- If the billing server initiates the transfer (also known as file transfer by *pull*), either FTP or secure file transfer protocol (SFTP) can be used.

Because HiPath 8000 Assistant is installed on the compact HiPath 8000 itself, it uses neither FTP nor SFTP to access data.

Both types of connections can be protected with IPsec as long as the billing mediation server supports it. Refer to Section 14.9, “IPsec Baseline”, on page 14-8.

14.3 Data File Security

The security for data files feature protects access to data files by extensive password procedures, such as:

- Suppression of password display during entry
- One-way encryption for different file groups
- Suppression of secret log-in parts within session script (protocol) files
- Restoration of all file group passwords after recovery or software upgrade

Each file group can be administered by different attributes and different password groups defining the access modes (for example, guest, administrator, and user).

14.4 Defending Denial of Service Attacks

14.4.1 Definition

This feature provides the capability to provide protection from VoIP-based denial of service (DoS) attacks—for example, a large volume of SIP messages from a hostile user.

This protection is in addition to the network-level protection against traditional DoS attacks.

The main defense against DoS attacks is provided by the network design. In addition, border gateway elements, session border controllers, and VoIP firewalls can be used to control the volume of VoIP traffic to protect against a SIP-based DoS attack.

Refer to the *HiPath 8000 Security Reference and Planning Guide* for more information.

14.4.2 Functional Operation

A host-based intrusion detection system (IDS) monitors incoming traffic in parallel to the traffic being sent to normal application processing. When incoming traffic from an IP address exceeds the provisioned threshold, all traffic from that IP address is placed on a *black list*, and is temporarily blocked.

The black list operates as follows:

1. A rule is created in the internal firewall that blocks all traffic from that IP address.
2. After the block period expires, the rule for that IP address is automatically removed from the internal firewall.

The following administrable options permit the system administrator to customize the DoS defense mechanism thresholds and values:

- **Rate Threshold:** This threshold is used for most traffic. This value is generally a low threshold for end-user traffic.
- **Trusted Hosts exception list:** This threshold is used for specific IP addresses that are exempt from rate monitoring. This exception list is generally used for servers that have higher volumes of traffic.
- **Block Period:** This value specifies the duration the temporary firewall rule is in place to block traffic from a blacklisted IP address.

This feature also provides alarms when the system starts discarding messages due to DoS message filtering.

14.5 Event Logging

The security event logging feature permits the HiPath 8000 to record security administration actions and OAM&P activity originated over CLI, SNMP, SOAP/CLI or SOAP/XML interfaces to the HiPath 8000. It also records OS-level CLI activity.

This feature provides:

- The ability to track down system abusers and hackers that may be involved in system and network intrusions, interruptions, damage and unauthorized configuration changes—for example, to disrupt service or enable toll fraud.
- The ability to investigate recent security-related activity such as the following:
  - Changes to security attributes, services, and access controls such as successful and unsuccessful changes to user IDs and passwords; and successful and unsuccessful login attempts, logouts, or session termination (either local or remote) via the *security audit trail*

– Recent non-security related OAM&P activity via the *recent change log*

This security event log is different from, and is kept completely separate from, the system event log, which logs abnormal runtime activity.

14.5.1 Functional Operation

The security log files are rotated on a daily basis. Archived security log files for the previous 30 days are retained; files older than 30 days are automatically removed.

Although the active security event log files are not encrypted, they are accessible only to *i*NMC users who have the proper authorization. However, after the data is transferred to the *i*NMC, the file can be archived to long-term storage as either an encrypted or unencrypted file.

FTP (using IPsec) is used for the secure transfer of the log file data from the HiPath 8000 to the *i*NMC.

14.5.1.1 Security Audit Trail

The security audit trail supports logging capabilities based on ANSI T1.276-2003 and Telcordia GR-815-CORE—for example:

- Any action that changes the security attributes and services, access controls, and other configuration parameters of each network element and management system that is part of the HiPath 8000 infrastructure
- Logins attempts, regardless of their success
- Logouts or session termination, whether local or remote
- Critical security administration actions, both successful and unsuccessful, such as actions affecting user IDs, login passwords, IKE pre-shared keys for IPsec, and other security-related system characteristics

  Logging of both OS- and application-level critical security administration activity is performed.

14.5.1.2 Recent Change Log

The recent change log records all OAM&P activity (whether successful or unsuccessful), including:

- Changes to system resources, system parameters, network elements, and end-user devices
- Provisioning commands

- Commands that retrieve customer data
- Data synchronization commands
- Data or network element recovery commands

14.6 File Transfer Security

14.6.1 Definition

The file transfer security feature provides for the transfer of CDR files or traffic measurement data files. Either the billing mediation server or the HiPath 8000 can initiate the transfer; however, it is preferable for the HiPath 8000 to do so.

14.6.2 Functional Operation

The HiPath 8000 provides file transfer capability via TCP/IP using FTP, which is based on Internet Engineering Task Force (IETF) RFC 959, *File Transfer Protocol (FTP).*

Because HiPath 8000 Assistant is installed on the compact HiPath 8000 itself, it does *not* use FTP to access data.

The following security mechanisms for FTP file transfer are provided:

- **FTP authentication:** When a remote user or remote application opens an FTP session, it has to transfer the user ID and password for system access control. The validity of these parameters is checked by the authentication procedure.
- **File security:** For each action affecting the file system, the user ID transferred with the authentication procedure is used to check the authority to access each specified file.

14.6.3 FTP Security Options

14.6.3.1 Access Control

FTP is disabled by default by the HiPath 8000 security policy. However, FTP can be enabled on the billing and management subnets for specific interface partners.

14.6.3.2 Confidentiality

Supported FTP confidentiality options vary by interface and include the following:

- ***i*NMC and *i*SMC: FTP transfers may be protected via IPsec.
- **Basic traffic tool:** Secure FTP is used to securely retrieve data from the HiPath 8000.
- **CDR delivery:** Refer to Section 14.2.2, “Functional Operation”, on page 14-2.
- **OS-level FTP for management of the HiPath 8000 Linux servers:** Secure FTP is supported.

14.7 Hypertext Transfer Protocol over SSL

Hypertext transfer protocol over SSL (HTTPS) is an extension to HTTP that secures web browser interfaces. There is a server side certificate.

Any authentication with HTTPS is typically done via digest authentication or application-level login.

HTTPS is used to provide security for the following interfaces:

- *i*SMC user to *i*SMC server
- *i*SSC user to Web server
- ComAssistant user to CAP/ComAssistant server
- HiPath 8000 Assistant client to compact HiPath 8000

14.8 *i*NMC and *i*SMC Security

14.8.1 Definition

The *i*NMC and *i*SMC security feature provides secure storage of the *i*NMC and *i*SMC user login passwords. The password protection mechanism is based on a one-way encryption algorithm.

14.8.2 Functional Operation

The *i*NMC user passwords are stored in compliance with *American National Standard for Telecommunications T1.276-2003, Baseline Security Requirements for the Management Plane*. When these passwords are provisioned, they are stored in the *i*NMC and *i*SMC servers in encrypted form.

When the user attempts to log on, the *i*NMC or *i*SMC performs OS-level authentication of the user name and password against the server system/domain on Windows. The *i*NMC and *i*SMC servers also support the modification of user's password if the user exists on the server system itself, rather than on the Windows domain.

14.9 IPsec Baseline

14.9.1 Definition

Internet Protocol Security (IPsec) is a security protocol in the network layer that provides cryptographic security services that flexibly support combinations of authentication, integrity, access control, and confidentiality.

The HiPath 8000 uses a generic mechanism to provide authentication, integrity, access control, and confidentiality for any server-to-server interface. This implementation makes use of Linux SUSE SLES9, the most recent enterprise server Linux version.

The IPsec subsystem is configured during system startup using the *i*NMC to configure IPsec rules and profiles.

Because an incorrect configuration can lead to a total outage of network communication, it is strongly recommended that these tools be used *only* to monitor the status of the IPsec subsystem.

Usually, IPsec is only configured during installation of the system; a reconfiguration is not required unless the network configuration changes. The HiPath 8000 automatically controls the setup of IPsec during system startup.

14.9.2 Guidelines for Implementation and Use

If required by the enterprise's security policy, IPsec can be used:

- Between the HiPath 8000 and the *i*NMC to protect the SNMP/FTP interfaces
- Between the *i*NMC client and *i*NMC server to protect the common object request broker architecture (CORBA) interface
- Between the HiPath 8000 and the *i*SMC or *i*SSC to protect the SOAP interface
- Between the HiPath 8000 and ComAssistant to protect the CSTA interface
- Between the HiPath 8000 and the billing server to protect the FTP interface
- Between two HiPath 8000s to protect the SIP-Q interface
- Between the HiPath 8000 and the media server to protect the SIP over UDP interface

- Between the HiPath 8000 and the OpenScape server to protect the CSTA and SIP over TCP interfaces
- Between the HiPath 8000 and a third-party trusted host or peer server that is not bound to a known HiPath 8000 element type
- Between the compact HiPath 8000 and the HiPath 8000 Assistant Web client to protect the Web interface

The default security policy for the signaling IP addresses is to allow all sources to talk to the HiPath 8000 signaling IP address/port. All ports are blocked for that IP address except the ones required for that signaling protocol.

The default security policy for the management and billing IP addresses is to allow all sources to talk to the HiPath 8000 with SSH. All other ports on the management and billing IP addresses are blocked. As an option, access control can be applied to SSH to restrict which source addresses can log on to the HiPath 8000 secure CLI interface.

Access control is mandatory for FTP, CORBA, and SNMP, with or without the use of IPsec.

14.10 Login Categories

14.10.1 Definition

The login categories feature provides the ability to create customized login categories, each with its own permitted level of access. The enterprise can create as many categories as necessary, and can use the permission tree to assign the applicable authorizations to each.

The ability ensures that RTP CLI users only have access to the minimum privileges needed to perform their job responsibilities.

14.10.2 Functional Operation

The HiPath 8000 administrator creates individual OS-level user accounts and associated OS privileges for each RTP CLI user without having to grant superuser OS-level privileges to each RTP CLI user's OS-level account.

14.11 Password Encryption

The *i*NMC and *i*SMC password encryption feature provides secure storage of the passwords the *i*NMC uses to perform FTP operations with the HiPath 8000.

The *i*NMC and the HiPath 8000 store these passwords in compliance with *American National Standard for Telecommunications T1.276-2003, Baseline Security Requirements for the Management Plane*.

The password protection mechanism is based on the Twofish algorithm, which is a two-way encryption algorithm. This is different from the requirement for one-way encryption on normal user passwords because the *i*NMC must be able to retrieve the password from the database to insert it into the command with the remote network element (NE).

When the *i*NMC needs to perform a FTP operation with a remote NE, the *i*NMC retrieves the password from the database, decrypts it, and uses it in the FTP operation with the NE.

14.12 Provisioning and Security Logging

14.12.1 Definition

The provisioning and security logging feature provides the ability to log all activities and commands in a log file to assist in detecting hacker and access violations.

14.12.2 Functional Operation

Alarm reports are generated according to International Telecommunications Union-Telecommunications (ITU-T) Recommendation X.736, *Systems Management: Security Alarm Reporting Function*.

Provisioning and security events can be logged using the log control function of the *i*NMC, *i*SMC, and HiPath 8000 Assistant, according to ITU-T Recommendation X.735, *Systems Management: Log Control Function*.

14.13 Secure CLI

The secure command line interface (CLI) feature provides secure command-line and file-transfer interfaces on the HiPath 8000 using Secure Shell and SFTP.

Secure Shell is also present in the *i*NMC/*i*SMC/HiPath 8000 Assistant interface. Refer to Section 14.14, “Secure Shell on the iNMC/iSMC/HiPath 8000 Assistant Interface”, on page 14-10.

14.14 Secure Shell on the *i*NMC/*i*SMC/HiPath 8000 Assistant Interface

Secure Shell on the *i*NMC/*i*SMC Interface allows the *i*NMC and the *i*SMC to use a Secure Shell package to protect CLI access and file transfers for OS-level platform/server maintenance of the HiPath 8000.

In the compact HiPath 8000, the HiPath 8000 Assistant client offers secure shell access for nonrecurrent operations on the CLI level.

This feature is used for Siemens service access only.

Secure Shell is also present in the CLI. Refer to Section 14.13, “Secure CLI”, on page 14-10.

14.15 Secure Storage of CDR Password

Passwords for the HiPath 8000 CLI login are stored encrypted within the Linux OS. Application-level passwords for transferring CDRs from the HiPath 8000 to the billing mediation server are stored via two-way encryption within the HiPath 8000 database.

14.16 SIP Privacy Mechanism

14.16.1 Definition

The privacy mechanism for SIP feature provides the following SIP privacy capabilities according to IETF RFC 3323, *A Privacy Mechanism for SIP:*

- Guidelines for the creation of messages that do not divulge personal identity information
- A *privacy service* logical role for intermediaries to handle some privacy requirements that user agents cannot satisfy themselves
- Means by which a user can request particular functions from a privacy service

This feature uses digest authentication to permit a user to hide identity and related personal information when issuing requests. Correspondingly, intermediaries and designated recipients of requests can reject requests whose originator cannot be identified.

14.16.2 Functional Operation

In SIP, identity is most commonly carried in the form of a SIP URI and an optional display-name. A SIP Address of Record (AoR) has a form similar to an E-mail address with a SIP URI scheme (for example, sip:alice@atlanta.com). A display-name is a string that contains a name for the identified user (for example, "Alice"). SIP identities of this form commonly appear in the To and From header fields of SIP requests and responses. Users can have many identities that they use in different contexts.

There are numerous other places in SIP messages in which identity-related information can be revealed. For example, the Contact header field contains a SIP URI, one that is commonly as revealing as the address-of-record in the From. In some headers, the originating user agent can conceal identity information as a matter of local policy without affecting the operation of the SIP protocol. However, certain headers are used in the routing of subsequent messages in a dialog, and must therefore be populated with functional data.

The privacy problem is further complicated by proxy servers (also known as *intermediaries* or, generically, *the network*) that add headers of their own, such as the Record-Route and Via headers. Information in these headers might inadvertently reveal something about the

originator of a message—for example, a Via header might reveal the service provider through whom the user sends requests, which might in turn strongly hint at the user's identity to some recipients. For these reasons, the participation of intermediaries is also crucial to providing privacy in SIP.

14.17 TLS Support

14.17.1 Definition

The transport layer security (TLS) support feature provides for secure signaling based on TCP and the TLS protocols.

TLS is an application-independent security protocol defined by the IETF that provides encryption and data integrity between two communicating applications. TLS is able to protect SIP signaling messages against loss of integrity, loss of confidentiality, and against replay. It is defined in IETF RFC 2246, *The TLS Protocol, Version 1.0*.

The IETF's requirements for SIP signaling, which are defined in IETF RFC 3261, *SIP: Session Initiation Protocol*, indicate that TLS must be used to provide encryption and data integrity of the SIP signaling stream between proxies, redirect servers, and registrars. The HiPath 8000 also optionally supports TLS to protect the SIP signaling stream between the HiPath 8000 and SIP endpoints, which is an IETF recommendation but not a requirement. TLS should be used if the enterprise security policy requires encryption of the SIP signaling stream.

- All Siemens SIP telephones used with the HiPath 8000 support UDP, TCP, and TLS for SIP signaling transport. The transport protocol that is used is a configuration option of the SIP telephone.

  Other SIP telephones used with the HiPath 8000 may only support a subset of this functionality. Refer to the telephone's documentation for more information.

- Refer to Section 16.14, "SIP Over TCP/TLS Support", on page 16-9 for more information about this feature.

14.17.2 Functional Operation

An *administrative domain* is a collection of end systems, intermediate systems, and subnetworks operated by a single organization or administrative authority. In the HiPath 8000, each business group represents a separate administrative domain.

The HiPath 8000 supports the following stages of authentication:

- When setting up the TLS connection from the SIP endpoint to the HiPath 8000

- When responding to a 401 (or 407) challenge from the HiPath 8000 in response to any form of a SIP request, such as a SIP REGISTER or SIP INVITE

Endpoint authentication is performed using HTTP digest authentication over the TLS-secured link. Refer to Section 16.2, “HTTP Digest Authentication”, on page 16-1.

Within a single administrative domain, server authentication takes place when the TLS connection is established. In the HiPath 8000, the SIP server is a proxy with a collocated registrar; because of this, the TLS connection between the SIP endpoint and the server is left open for the duration of the registration.

When TLS is used for SIP endpoint-server communication, a unilateral authentication is performed as part of the TLS handshake. On top of the established TLS connection, the SIP endpoint authenticates towards the server using HTTP digest authentication.

After authentication is successful, subsequent communication is done over an encrypted connection. The SIP endpoint uses this connection to attempt to register with the server (without credentials in the first instance). The user ID and password for HTTP digest authentication are stored in the database of the SIP endpoint device; therefore, the user does not manually supply the ID and password.

With TLS protection of SIP signaling, the SIP telephone takes on the role of a TLS client and the HiPath 8000 takes on the role of a TLS server. If the TLS connection fails, the TLS client detects and re-establishes the connection.

It is useful to note that during this process, it is the SIP endpoint device, and *not* its user, that is being authenticated.

14.17.3 Guidelines for Implementation and Use

- In addition to TLS, the HiPath 8000 also supports TCP and UDP as transport layer options for SIP signaling protocols. Therefore, SIP over TCP and SIP over UDP are viable alternatives to SIP over TLS.
- When the SIP URI is used to place a call, it is possible for TLS to be used as the transport protocol by one SIP endpoint and for a different signaling protocol (such as SIP-Q or MGCP, with or without signaling security) to be used by the other device.
- The HiPath 8000 supports TLS on the signaling connection between a SIP endpoint and the SIP signaling manager. Because TLS is applied on a hop-by-hop basis, end-to-end signaling security is achieved only when all hops of the signaling connection use TLS. End-to-end TLS security is not guaranteed if the call leaves the local administrative domain.

15 Serviceability Features

This chapter describes the HiPath 8000 features that improve serviceability, such as diagnostics and debug tools, code controls, and administrator controls.

Refer to the following for information about administration and operational practices associated with these features:

- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*

15.1 Administrator Identification and Authentication

The administrator identification and authentication feature:

- Provides authorization control by requiring user IDs and passwords
- Provides for the administration of user IDs
- Provides for the handling of unauthorized attempts to execute commands via the *i*NMC, *i*SMC, or HiPath 8000 Assistant

Different access levels can be assigned to users based on command groups and applications. All log-in attempts, all unauthorized attempts to execute administration commands, and all attempts to access data can be recorded and routed to an operation system.

For every external request an access control check is performed. The access control function uses the services of the scheduling function according to ITU recommendation X.746. The administration of access control is performed according to X.741.

15.2 Backup and Restore

15.2.1 Definition

The backup and restore features provides for full system backup of the HiPath 8000 data as well as the code, including the operating system and all applications. This supports the restoration of the entire single- or dual-node cluster in case of a catastrophic event.

The backup and restore process is applicable to the following scenarios:

- Failure of a complete dual-node cluster.
- Failure of either individual node, such that the local (system) disks are unrecoverable. The partner node remains in operation.

This feature addresses these scenarios by providing the following:

- A backup script to facilitate creation of a backup image of each node. The backup image is removed from the node and is stored on a customer-provided backup server for use during recovery.
- A restore script to control the recovery of one or both nodes, using the archived disk image.

15.2.2 Functional Operation

The backup job takes approximately 45 minutes on an idle system and utilizes 50 megabytes (MB) of memory.

The time needed for the restore process per node is approximately 60 minutes.

15.2.3 Guidelines for Implementation and Use

15.2.3.1 General Guidelines

- System backups should be created at the following intervals:
  - After initial installation.
  - Before and after any patching or upgrade activity. In the event that there is a failure during the patching/upgrade, the system can easily be recovered to the most recent state.
  - After any non-database related configuration change, such as IP networking modifications, security modifications, and so on.
  - Periodically, with a maximum interval of one month. More frequent intervals, such as weekly backups, are recommended.

- The backup feature described in this section does *not* back up the following elements:
  - **Database contents:** The database backup procedures is required.
  - **Database archive logs:** As long as a database backup is created, these files are not required.
  - **Call data records:** These records are generally transferred from the system on a regular basis, and therefore need not be backed up.
  - **Log files and software core dumps:** These items are for informational purposes, and therefore are not backed up.

15.2.3.2 Effect on Call Processing Real Time

The generation of a backup file requires 10% to 20% of the HiPath 8000 CPU resources. Backups should only be performed at off-peak hours when the CPU usage for call processing is at 50% or less. The backup job should be given a low priority to help ensure that there is no interference with call processing.

There is no impact on call processing during the restore of a single node back into the cluster.

15.3 Basic Traffic Tool

15.3.1 Definition

The basic traffic tool is a performance monitoring tool. Customers and service personnel can use this tool to view snapshots of the traffic for incoming SIP calls to the HiPath 8000. The information is provided in graphical and numeric form.

The business group traffic measurements feature provides counts of several types of HiPath 8000 activity on a per-business group basis. Refer to Section 6.9, “Business Group Traffic Measurements”, on page 6-7.

15.3.2 Functional Operation

15.3.2.1 Graphical Data

The following data appears in graphical form, each on a separate screen:

- Number of SIP calls over a selected period
- Number of SIP calls for the current day
- Busy hour call attempts over a selected period

- Busy hour call attempts for the current day
- Statistical data for selected period
- Statistical data for today

The graphical output is based on data the system collects every 15 minutes. The user can print the output from any of the graphical screens.

15.3.2.2 Numerical Data

In addition to the graphical data, the following data appears in numeric form:

- Number of calls within the specified time period
- Number of incoming calls within the specified time period
- Number of outgoing calls within the specified time period
- Unsuccessful call attempts within the specified time period
- Busy hour call attempts within the specified time period

The user can:

- Print the tab sheet that provides the numerical output.
- Copy and paste the data in another file.

15.4 Call Gapping Code Controls

The call gapping code controls feature provides manual code controls which block traffic to destination codes that are difficult or impossible to reach. This conserves network resources for other traffic.

Code controls are effective for controlling focused overloads, a condition characterized by a surge of traffic from many parts of the network to a single office or destination—for example, increased traffic due to callers trying to win a radio station' call-in contest.

15.5 Diagnostics Tool

The diagnostics tool feature provides a management function to display all diagnostics tests, to start and stop specific diagnostic tests, and to display the results.

15.6 Element Mass Provisioning

15.6.1 Definition

The element mass provisioning feature provides for the mass processing of provisioning commands. This feature supports those commands that are available via the *i*NMC and HiPath 8000 Assistant.

15.6.2 Functional Operation

This feature uses command line scripts implemented via the CLI to simplify the provisioning of network elements. The mass provisioning utility loops through the processing all of the commands in the script file. Output results are displayed to the computer screen; the user may instead redirect the output to a file.

15.7 Endpoint Control Licensing

The endpoint control licensing feature provides a mechanism to prevent the administration of unauthorized endpoints or interfaces.T he authorization is available by type, by number of endpoints, or both.

The control mechanism can be provided via encrypted enable keys assigned per HiPath 8000, per endpoint, or per customer. A support tool is needed to administer the keys.

15.8 Feature Profiles

15.8.1 Definition

The feature profiles feature provides the capability to create a shared profile object that is contained as an index (similar to a business group) as part of the subscriber data record. The data is combined with the discrete service data stored for a given subscriber.

Theoretically, the HiPath 8000 supports up to 100,000 feature profiles. In practice, however, the actual number of profiles in use is generally much lower.

15.8.2 Functional Operation

Feature profiles are a set of features, including their corresponding data. The operation is comparable to that of business group features, except that the group may be subdivided with varying feature profiles.

When creating or modifying subscribers, the administrator can assign a feature profile to apply to all HiPath 8000 subscribers, or can assign a business group-specific feature profile to the subscriber.

15.9 Log File Retrieval Tool

The log file retrieval tool helps to simplify problem analysis by:

- Collecting all log files from all HiPath 8000 nodes
- Storing the log files in one database or spreadsheet
- Sorting the log records chronologically
- Filtering the information according to categories and keywords

15.10 Maintenance Manager

15.10.1 Definition

The maintenance manager (MMGR) feature provides for the activation and control of maintenance tasks, such as backing up and restoring files, on the HiPath 8000.

The MMGR feature runs, controls, and queries jobs through the client-server interface.

15.10.2 Functional Operation

A maintenance task is handled via an MMGR job, which is any MMGR program that allows end users to query state information and run the details of the job. The MMGR controls HiPath 8000 maintenance tasks via maintenance manager server requests. These tasks, called *jobs*, may vary in their scope and behavior. Jobs include the following:

- Backup and restore
- Data provisioning
- Software upgrades
- Package installation, removal, and information
- Software version query

15.11 On-Demand Audits

The on-demand audits feature provides the capability for service personnel to immediately obtain the status of the system resources.

Two different times (peak and off-peak) define different timer values between each Trunk/PRI channel audit. The default value of the timers are 1 second for peak times and 0.25 seconds for off-peak times. These times are also configurable, and can be fine-tuned to ensure that the audit cycles through all the resources at least twice a day without taking system time away from call processing.

15.12 Process Debug Tool

The process debug tool feature provides on-line debug options allowing different levels of logging and tracing. The debug function can be turned on and off for:

- Specific processes
- Specific functional areas—for example, subsystems or components such as the UCE
- The system as a whole

15.13 Query of Subscriber Transient Operational Status

This feature provides the capability to determine the transient operational status of a subscriber.

The term *transient operational status* refers to a snapshot of the status of the subscriber at the instant that the request is issued by administration or service personnel. A subscriber is identified by the associated DN.

The administrator or service person can enter the subscriber's DN into a CLI menu, an iNMC screen, or a HiPath 8000 Assistant screen, and receive details concerning the connections active for that subscriber.

15.14 Remote Restart

The remote restart feature provides remote restart and recovery of a node with the capability to manage individual processes that run on the different nodes of the predefined clusters.

15.15 System Software and Patch Level Status

This feature provides the operator and support teams the ability to display and automatically update a billboard-type area with the current issue and revision of the application software.

At the time of the initial loading of the application and every time thereafter, a product reflects exactly what application software version, inclusive of base release and patchset level, it is running. Furthermore, if a patch has been somehow removed, the billboard reflects that information easily and clearly.

The updating and downgrading of this area is an automated part of the patchset loading instructions or file. This information can be displayed locally or remotely, and can be printed.

15.16 System Upgrade

The system upgrade feature provides for an automated software installation process and software upgrade process. It can be activated remotely and is non-service affecting. It also includes a fallback to a "Safe" configuration.

15.17 VLAN Provisioning

The VLAN provisioning feature:

- Provides the ability to separate administration-related and billing-related traffic and route them across different Ethernet interfaces
- Gives the administrator the flexibility to provision the IP addresses and interfaces according to enterprise-specific requirements

16 SIP Signaling Features

This chapter describes the HiPath 8000 features that support SIP signaling and the interworking with other elements such as application servers, voice conferencing applications, and voice mail systems.

Refer to the following for information about administration practices associated with these functions and features:

- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*

16.1 Audit Mechanisms

The SIP audit mechanisms feature provides mechanisms to ensure against hung resources and overbilling. The HiPath 8000 actively audits the SIP sessions it initiated by periodically sending INVITE messages that can modify the media during a confirmed session and maintain keep-alive sessions timers. In addition, if a user agent client (UAC) does not audit its sessions, the HiPath 8000 audits sessions in which it functions as a user agent server (UAS).

16.2 HTTP Digest Authentication

16.2.1 Definition

The hypertext transfer protocol (HTTP) digest authentication feature is a SIP capability that provides the mechanism to protect against registration hijacking, remote server impersonation attacks, mid-call attacks (re-INVITES) and forged BYE requests. The HTTP digest authentication mechanism is also designed to defend against replay attacks.

In accordance with RFC 3261, *SIP: Session Initiation Protocol*, it is always used for authentication in the HiPath 8000.

Refer to Section 14.17, “TLS Support”, on page 14-12 for information about how digest authentication is used with TLS.

16.2.2 Functional Operation

HTTP digest authentication can be enabled or disabled on the HiPath 8000 for all SIP endpoints on a systemwide basis via a provisioning option of the SIP signaling manager. When HTTP digest authentication is enabled, a list of trusted entities can be assigned for which digest authentication will be waived. Trusted entities can be assigned based in their IP address, IP address/port number, or fully qualified domain name (FQDN).

Important Note

In the *i*NMC and HiPath 8000 Assistant, the default setting of the HTTP digest authentication feature is *disabled*. It is strongly recommended that the HTTP digest authentication feature be enabled for all HiPath 8000 installations. Refer to the *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide* or *HiPath 8000 Assistant Administrator Documentation*.

User authentication is done via HTTP digest authentication. The client starts by making an unauthenticated request to the server. The server’s response indicates that it supports digest authentication.

The following are the most important security aspects of digest authentication:

- In contrast to basic authentication, the password is never transmitted in clear-text.
- The server can optionally monitor and track the response, which makes it resistant to replay attacks.
- The server can carefully choose and restrict nonce values, such that a particular nonce is only valid for a certain time, only from a particular client, or only for a certain request.

A *nonce* is a parameter, used in digest authentication, that varies with time. A nonce can be a time stamp, a visit counter on a Web page, or a special marker intended to limit or prevent the unauthorized replay or reproduction of a file.

16.3 Integration with HiPath Xpressions

This feature provides SIP support for routing to and from the Siemens HiPath Xpressions system. Xpressions is Siemens' preferred unified messaging product.

This feature supports the following:

- SIP connectivity (Make Call, SIP information such as DN identifying)
- Message waiting indication (MWI)
- Activation of blind transfer
- DTMF detection according to RFC 2833
- Inband voice codec
- Making a call with play wave

16.4 Integration with HiPath ProCenter

16.4.1 Definition

This feature provides support for HiPath ProCenter Enterprise, which is a contact center solution that offers advanced multimedia skills-based routing for any enterprise, supporting up to 750 active agents. The offering delivers:

- Next-generation visual management tools
- Advanced multimedia skills-based routing
- Unified queuing and reporting for voice, E-mail, web collaboration and outbound interactions
- Intuitive agent desktops
- Presence and collaboration tools
- Flexible, customizable real-time, cumulative and historical reporting
- Self-service and transaction-based IVR support
- Multi-site networking support
- Integration kits for Siebel and SAP
- A Software Developer's Kit (SDK) for easy CTI integration
- Modular options that allow seamless upgrades, growth, and expandability

16.4.2 Functional Operation

With the HiPath 8000 integration, the HiPath ProCenter server communicates with the HiPath 8000 via CSTA XML. This allows the HiPath ProCenter server to monitor user (agent) and group (hunt group) devices.

The media server is always used to play music in queue, and is the default during any HiPath ProCenter queue processing flow when there is no other step. If only a basic announcement is needed, the media server can also be used to play an announcement based on the configuration at the hunt group level, but the announcements are not really controlled by the HiPath ProCenter Manager.

If more sophisticated announcements and call treatment are required, including announcements per routing strategy, performance announcements, menus and digit collection, the Call Director feature should be used. Refer to the following for more information:

- *HiPath ProCenter, V7.0, Hardware Integration Guide*
- *HiPath ProCenter, V7.0, Installation and Maintenance Guide*
- *HiPath ProCenter, V7.0, Manager Guide*
- *HiPath ProCenter, V7.0, Planning and Design Guide*

All calls to the contact center are routed to an initial hunt group that is configured in a pair with a music on hold hunt group. This pair of hunt groups must be configured in the HiPath 8000 to support the HiPath ProCenter solution as follows:

- **Initial hunt group:** This hunt group with a manual hunting sequence with an intercept treatment configured to play ringback, followed by an announcement to the caller through the media server associated with the HiPath 8000. All dialable numbers that provide access to the contact center should point to an initial hunt group.
- **Music on hold hunt group:** This hunt group is also configured with a manual hunting sequence, with an intercept treatment configured to play music on hold to the caller through the media server associated with the HiPath 8000.

With a manual hunting sequence, the switch does not directly distribute calls from the hunt group. Provided that a CSTA monitor is in place on the hunt group, calls remain queued unless HiPath ProCenter moves them using CSTA.

Refer to Section 7.2, “Hunt Group”, on page 7-3 for more information about hunt groups and manual hunting.

If HiPath ProCenter is not functioning properly, users can continue to answer calls through backup routing. The core backup routing concept of HiPath ProCenter is that if the application becomes unavailable, the switch routes calls to available users who are logged on to the switch until the application is restored.

If HiPath ProCenter fails to communicate with the HiPath 8000, the HiPath 8000's CSTA signaling manager detects the communications failure. The HiPath 8000 then removes all associated monitor points queued in the hunt groups so they are distributed by the switch instead of by HiPath ProCenter.

16.5 Integration with OpenScape

16.5.1 Definition

This feature provides access to OpenScape, which integrates a wide array of communication devices and services for easy access and use. In turn, the OpenScape user can efficiently use the HiPath 8000 as an interworking gateway to the PSTN.

The interface to the PSTN is via standard PSTN trunking. The HiPath 8000 provides the external PSTN gateway and legacy corporate networks.

The Common Application Platform (CAP) server may be deployed with the HiPath 8000 or with OpenScape. A Microsoft Live Communication (LC) server is included in this solution to provide instant messaging support.

16.5.2 Functional Operation

The system administrator provisions HiPath 8000 subscribers with classmarks to indicate they have access to OpenScape features and should be considered OpenScape users.

The published identity of the user is the OpenScape AoR. The HiPath 8000 subscriber's device also supports an AoR; however, this AoR is local to the HiPath 8000 and appears as an associated device AoR within OpenScape for the published AoR. HiPath 8000 CSTA monitoring provides OpenScape up-to-date status information for the associated AoR device.

Depending on how a call is initiated, its processing differs as follows:

- For calls initiated by the user through the OpenScape portal, calls are processed as normal for OpenScape Users based on the published AoR.
- For calls initiated by the user using the HiPath 8000 associated AoR device, the AoR identity provided by the HiPath associated device is *not* the published OpenScape AoR. Instead, the user's identity is conveyed as a local HiPath AoR.

Calls from the local HiPath 8000 AoR to other HiPath users are routed using normal translation and routing. Calls to OpenScape published AoRs are routed to OpenScape for processing via the LC server, and are processed by OpenScape based upon the published AoR presence and

rules. Based on the HiPath 8000 associated AoR device availability and rules, the call may be routed to the HiPath 8000 where normal translation is performed, resulting in the call being routed to the HiPath 8000 user's device.

Calls from external interfaces to the published OpenScape AoR are processed the same as calls initiated by HiPath 8000 users to the OpenScape published AoR.

16.6 Interworking with Application Servers

The SIP interworking with application servers feature provides the SIP signaling manager on the HiPath 8000 to interact with application servers. By interfacing to third-party SIP-based application servers, the HiPath 8000 solution can deliver optional enhanced services such as unified messaging and E-mail callback, which may not be available natively on the HiPath 8000, or that may provide a choice for alternative user interfaces to satisfy an enterprise's preferences.

16.7 Interworking with Genesys Call Center

This feature provides signaling and interworking with the Genesys call center, which routes calls to an agent registered with the HiPath 8000 via the SIP endpoint. Call information is also presented to the agent via the Genesys Agent Console application.

The Genesys call center is configured as SIP endpoint or DN on the HiPath 8000. Applicable routing and configuration parameters are configured on the HiPath 8000 to route calls to the Genesys call center application.

The click-to-answer feature provides the capability for a SIP endpoint to use a command of the Genesys Agent Console application to answer a SIP call when it is presented. As a result of the command, an answer event is generated and is passed via the HiPath 8000. Refer to Section 5.10, "Click to Answer", on page 5-10.

16.8 Interworking with RG 8700

Multiple business groups can use the functions of a single HiPath 8000 and RG 8700. The service used by each business group is independent of each other. The facilities on the RG 8700, used by each business group, are also independent of each other.

The RG 8700 performs interworking between ISDN and SIP. Relevant SIP services are mapped to ISDN; the reverse also takes place. The HiPath 8000 and the SIP endpoints are not aware of ISDN as the transport protocol.

The RG 8700 also provides a survivable media gateway when connection to HiPath8000 is lost. The RG8700 has minimum service knowledge; all service knowledge is with the HiPath 8000. After the HiPath 8000 selects the service and routes to a specific endpoint, the RG 8700 maps the requested service to its ISDN equivalent.

Depending on the customer's needs, dedicated RG 8700 trunks can be associated with each business group, or the trunks can be shared among business groups.

Refer to the *HiPath 8000 Overview Guide* for more information about survivability.

16.9 Interworking with Unified Messaging Systems

The interworking with unified messaging systems feature provides signaling and interworking with SIP-based third party unified messaging systems.

16.10 Interworking with Voice Conferencing Applications

16.10.1 Definition

The interworking with voice conferencing applications feature provides signaling and interworking with SIP-based third-party conferencing servers. The IP Unity and Convedia media servers are certified for use with the HiPath 8000.

The compact HiPath 8000 has its own integrated media server.

The media server's conference bridge enables users in multiple locations to participate in remote conferences. The application offers telephone access to a conference bridge for both participants and a moderator through a telephone, with a standard set of conference controls accessed by way of the keypad.

In addition to telephone conferencing access, the application offers a Web interface for setting up conferences and creating a virtual space where multiple participants can share presentations, control the volume of individual participants, and ask questions. In addition to these features, the moderator can control many other features including the conference flow.

16.10.2 Networking

Refer to Section 12.7.5, "Three-Way Calling and Voice Conferencing", on page 12-7 for information about the interworking that takes place for this feature between the HiPath 8000 and a legacy PBX.

16.11 Interworking with Voice Mail Systems

16.11.1 Definition

The interworking with voice mail systems feature provides signaling and interworking with SIP-based third-party voice mail systems. The capability to support a visual message waiting indicator as well as stutter dial tone is provided by the HiPath 8000 as long as the support for this capability is also provided by the voice mail system and the customer premises equipment.

Message waiting indicators are also supported via SIP-Q. Refer to Section 18.9, “Message Waiting Indicator”, on page 18-3.

16.11.2 Networking

Refer to Section 12.7.6, “Voice Mail”, on page 12-8 for information about the interworking that takes place for this feature between the HiPath 8000 and a legacy PBX.

16.12 Provisional Responses Reliability

The reliability of provisional responses feature provides support for sending and receiving reliable provisional responses using positive acknowledgments, timers, and retransmission.

This feature ensures the proper delivery of session description protocol (SDP) sent in an 18x provisional response for early media (for example, to allow a SIP subscriber to hear PSTN ringback tone). Without this feature, the 180/183 might be lost because there is no guarantee of delivery if there is no retry mechanism.

16.13 SIP Endpoint Support

The SIP endpoint support feature provides the following SIP functionalities:

- SIP registrar functionality
- SIP back-to-back user agent (B2BUA)
- SIP location functionality

16.14 SIP Over TCP/TLS Support

16.14.1 Definition

The SIP over TCP/TLS support feature provides SIP over TCP and SIP over TLS, in accordance with RFC 3261.

The TCP-TLS-UDP dispatcher (TTUD) process is implemented to provide UDP, TCP, and TLS or SSL transport services for:

- SIP
- CSTA
- Any other application requiring TCP, SSL, or UDP connectivity

The TTUD process is designed to be independent of the application protocol used over the basic transport service of UDP, TCP, or TLS/SSL and to provide services to multiple diverse applications at the same time.

16.14.2 Functional Operation

The HiPath 8000 complies with the TLS security mechanisms defined for SIP in RFC 3261, including section 26.3.2.1, which requires the HiPath 8000 to reuse the TCP/TLS connection that is established by the SIP endpoint. The TCP/TLS connection that is established by the SIP endpoint during SIP registration must be kept open and reused for all SIP transactions that occur between the HiPath 8000 and the SIP endpoint. The responsibility to keep this TCP/TLS connection open rests solely with the SIP endpoint.

It is not possible for the HiPath 8000 server to re-establish the TCP/TLS connection toward the SIP endpoint if it fails. This is because RFC 3261 does not require SIP endpoints to support TLS server functionality. For example, as with most SIP telephones, the optiPoint 410 S SIP telephone only supports TLS client functionality and does not support TLS server functionality. The HiPath 8000 server must rely on the SIP endpoint to establish the TCP/TLS connection when it fails. If the TLS connection fails, the HiPath 8000 cannot deliver SIP messages to the SIP endpoint—for example, it cannot deliver an incoming call to the SIP endpoint.

16.14.3 Guidelines for Implementation and Use

As defined by RFC 3261 and implemented by the HiPath 8000, the TLS security mechanism has known limitations related to scalability and reliability. These limitations are described in section 26.4.3 of RFC 3261. In the HiPath 8000, these limitations manifest themselves as follows when TLS is used:

- HiPath 8000 port capacity is reduced.
- It is the responsibility of the TLS client (the SIP endpoint) to detect and recover the TLS connection whenever it fails. Therefore, the SIP endpoint must monitor the TLS connection to detect a loss of signaling communication with the HiPath 8000 server.

  The HiPath 8000 supports a rapid recovery mechanism for TCP/TLS connections, which is only supported for Siemens SIP endpoints that also support it. This mechanism is based on a frequent connectivity check, or *keep-alive message*, that the SIP endpoint sends to the HiPath 8000. If the connectivity check fails, the SIP endpoint establishes a new TCP/TLS connection.

16.15 SIP Privacy Mechanism

Refer to Section 14.16, “SIP Privacy Mechanism”, on page 14-11.

16.16 SIP REFER Method Support

The SIP REFER method support feature provides the functionality to process a REFER message from a SIP endpoint to support such features as SIP call transfer.

Operating as a B2BUA, the HiPath 8000 does not propagate the REFER message, but instead remains in control of the call. The processing of the REFER message follows the requirements in RFC 3515, *The SIP Refer Method*.

16.17 SIP Session Management—Concurrent Sessions

The SIP session management—concurrent sessions feature allows the HiPath 8000 to limit the maximum number of SIP sessions per subscriber. The limit is provisionable from the graphical user interface (GUI) or CLI.

16.18 SIP UA Registration Renewal During WAN Outage

This feature provides a mechanism to improve recovery from intermittent losses of connectivity by allowing SIP UA registrations to be renewed on a provisional basis. From the perspective of the SIP UA, this feature maintains its registration during a WAN outage until the configured time in seconds expires.

This feature is targeted to SIP UAs that are located in a branch, and for which a WAN status provider has been assigned.

To determine the status of the WAN, an audit of the proxy server is performed. These audits can be performed through scheduling or automatically whenever a possible WAN failure is detected. If the SIP UA contact is determined to be in a *Suspended* state, the SIP INVITE messages are no longer sent. Subscriber rerouting may be applied immediately if all contacts of a BGL are in this state.

By maintaining the registration binding, the SIP UA can still be reached by other branch/main office SIP UAs via the PSTN, provided that the subscriber rerouting feature is enabled and a survivable SIP endpoint is provisioned correctly by the administrator. By keeping track of the state of the SIP UAs, the rerouting takes place immediately when both the endpoint and the SIP UA are inaccessible.

16.19 SIP UPDATE Method Support

The SIP UPDATE method support feature provides the functionality to permit a client to update parameters of a session (such as the set of media streams and their codecs), but has no impact on the state of a dialog. In that sense, it is like a re-INVITE, but unlike re-INVITE, it can be sent before the initial INVITE has been completed. This makes it very useful for updating session parameters within early dialogs.

17 CSTA Support Features

This chapter describes how the HiPath 8000 provides a standard European Computer Manufacturers' Association (ECMA) Computer Supported Telecommunications Applications (CSTA) protocol interface to external CTI applications, which permits applications such as ComAssistant, OpenScape, and HiPath ProCenter to control the HiPath 8000 SIP endpoints. It also describes other HiPath 8000 capabilities relevant to applications that utilize the CSTA interface.

Important Note

Although this chapter uses the application examples of ComAssistant and CAP, the CSTA interface is *not* designed solely for these applications.

Refer to the *HiPath 8000 Overview Guide* for more information about CSTA-supported applications.

Refer to the following for information about administration and operational practices associated with this feature:

- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*

Contact your Siemens representative about the ComAssistant publications that pertain to these features.

17.1 CSTA Protocol Interface

17.1.1 Definition

This feature provides a CSTA protocol interface to applications, such as CAP and ComAssistant, that support the ECMA standard. This feature has been released only with the Siemens Common Application Platform (CAP) to control and monitor telecommunication activities on SIP endpoints.

The native CSTA III XML interface provided by the HiPath 8000 is an open-standard interface that enables computing systems to provide third-party call control. It supports up to 60,000 users.

CAP is an external software platform for CSTA applications; it bridges the communication from the applications to the HiPath 8000.

17.1.2 Functional Operation

The CAP is used as the platform for applications to communicate with the HiPath 8000 CSTA interface. It controls the connection/link to the HiPath 8000.

The system administrator provisions the CSTA service against the subscriber directory number (DN) via the *i*SMC or HiPath 8000 Assistant.

Because CSTA is effectively an application programming interface (API) which is used to enable an application such as ComAssistant, it has no end-user interface.

IPsec is used to secure the CSTA III XML data between the CAP and the HiPath 8000 CSTA Manager. Refer to Section 14.9, “IPsec Baseline”, on page 14-8.

17.1.3 Networking

CSTA-monitored users must reside on the local HiPath 8000.

17.2 CSTA Services Support

Table 17-1lists the CSTA services the HiPath 8000 supports.

Category	Services Supported
Capability exchange services	Get CSTA features Get logical device information Get switching function capabilities Get switching function devices Switching function devices
System registration services	System register
System status services	Request system status System status
Monitoring services	Change monitor filter Monitor start (device monitor only) Monitor stop (device monitor only)
Snapshot services	Snapshot device Snapshot device data
Application session services	Start application session Stop application session Reset application session timer Application session terminated
Call control services (C->S)	Alternate call Answer call Callback call-related Clear connection Conference call Consultation call Deflect call (target is the alerting party) Hold call Make call Reconnect call Retrieve call (from hold) Single-step transfer Transfer call

Table 17-1 HiPath 8000-Supported CSTA Services (Sheet 1 of 2)

Category	Services Supported
Call control events	Conferenced Connection cleared Delivered Diverted Established Failed Held Network reached Originated Queued Retrieved Service initiated Transferred
Call associated features	Change connection information Generate digits Call information
Logical device feature services	Call back non-call-related Get agent state Get do not disturb Get forwarding Set agent state Set forwarding
Logical device feature events	Agent busy Agent not ready Agent ready Agent working after call Callback event Do not disturb Forwarding
Device maintenance events	Back in service Out of service

Table 17-1 HiPath 8000-Supported CSTA Services (Sheet 2 of 2)

17.3 Flexible Digit Processing

The flexible digit processing capability can be used on all calls originated from CSTA-enabled applications, including the Make Call, Consultation Call, and Deflect Call messages.

17.4 Data Synchronization

CSTA-enabled applications can make use of the data synchronization feature. Refer to Section 18.4, “Data Synchronization”, on page 18-2.

17.5 HiPath 8000-Provided Calling Name

The HiPath 8000 provides the calling name via the call monitoring events to the CSTA-enabled application. This calling name is only presented to the application user if the external directory does not match an entry for the user's DN.

17.6 Integration with Fault Management

With HiPath CAP V2.0, an internal mechanism is available to send SNMP traps and notifications and to integrate this information seamlessly into HiPath Fault Management.

17.7 Message Waiting Indicator

The HiPath 8000 allows for a CSTA-monitored device to report MWI changes to the monitoring application.

17.8 Multiple Time Zone Support

The CAP supports time zone information as delivered by the system database regardless of zone or location.

18 System Functions and Features

This chapter describes the HiPath 8000 functions and features that support such tasks as alarm reporting, message waiting indicator control, and recovery handling.

Refer to the following for information about administration and operational practices associated with these functions and features:

- *HiPath 8000 Configuration and Administration Using CLI Guide*
- *HiPath 8000 Configuration and Administration Using NetManager iNMC Guide*
- *HiPath 8000 Subscriber Accounts/Services Administration Using NetManager iSMC Guide*
- *HiPath 8000 System Feature Configuration Using NetManager iNMC and iSMC Guide*
- *HiPath 8000 Assistant Administrator Documentation*
- *HiPath 8000 Configuration and Administration Using HiPath Assistant*
- *HiPath 8000 Assistant Feature Configuration Administration Guide*
- *HiPath 8000 SOAP/XML Subscriber Provisioning Interface Guide*

18.1 Agent for OAM&P

The agent for operation, administration, maintenance and provisioning (OAM&P) feature provides management capabilities via the OAM&P agent. It provides the OAM&P interface to the *i*NMC or HiPath 8000 Assistant to allow all management tasks associated with the HiPath 8000, including the sending of alarms, database updating, and system configuration.

18.2 Alarm Reporting

The alarm reporting feature provides for the reporting of faults detected by the application software executing on the HiPath 8000 using the common interface provided by the resilient telco platform (RTP) event manager. Detected faults are identified by RTP events with a priority of 1, 2, or 3 which corresponds to critical, major, and minor alarm levels, respectively.

18.3 Announcements

The announcements feature provides:

- Audible notifications for the status of certain HiPath 8000 features
- User prompts to enter information when it is required to execute a feature

The media server provides announcements for the HiPath 8000; the compact HiPath 8000's integrated media server provides its announcements.

Refer to the individual feature descriptions for specific information about associated announcements.

Refer to the *HiPath 8000 Configuration and Administration Using CLI Guide* for a comprehensive list of the available announcements.

18.4 Data Synchronization

When subscribers are created, modified, or deleted, the *i*SMC or HiPath 8000 Assistant generates a log file with the XML stream for subscribers registered for the relevant external application—for example, ComAssistant. This file is transferred on a daily basis to the CAP server. At a predetermined time during the night, CAP runs a script to import the file and update its database.

When the data is imported, the CAP processes the data, modifying its database as required. Data messages are received for all subscribers, including those who are not using the relevant external application. Data for the other subscribers is discarded. Also, if the relevant external application is removed as an attribute from a previous subscriber, that subscriber is removed from the CAP database.

Communication links between external applications and CAP applications, as well as between CAP SCC8000 and the HiPath 8000 system, are based on TCP/IP connections. Any process restart or failover action requires these links to be re-established after the partners have come up again in the same software environment (on the same hardware or, transparently, on the failover cluster hardware).

18.5 Internal Audits

The internal audits feature provides for an audit process that performs a context scanning operation, first for UCE contexts and then for each type of signaling manager contexts.

18.6 Interworking with Automated Attendant Systems

An *automated attendant system* accepts all incoming calls and leads the caller through a menu offering different options, such as company operator assistance, direct extension dialing, voice-controlled services, and voice mail connection.

Automated attendant functions are included with the IP Unity Messaging application.

The interworking with automated attendant systems feature permits the use of an automated system with the HiPath 8000.

18.7 Local Management

The local management feature provides a command line interface for local management purposes. Local management includes configuration, monitoring, and maintenance of the internal HiPath 8000 software processes.

18.8 Media Server Support

The media server support feature provides the ability for the HiPath 8000 to interwork with:

- The IP Unity media server, either Version 1.5e, Version 2.7, or Version 3.1
- The Convedia CMS 1000
- The compact HiPath 8000's integrated media server

18.9 Message Waiting Indicator

18.9.1 Definition

The message waiting indicator (MWI) feature permits the reception of a subscriber's MWI status from a voice mail system via SIP. In a multiple-platform environment (for example, when a HiPath 4000 is present), the HiPath 8000 sends and receives MWI over SIP-Q.

Depending on the type of SIP endpoint the subscriber uses, the following indications are possible:

- Audible message waiting indication, which provides a special dial tone (sometimes called *message-waiting dial tone*)
- Visual message waiting indication (VMWI), which illuminates a light (indicator) on the telephone
- Both

The HiPath 8000 ensures that subscribers continue to receive accurate MWI in any of the following circumstances:

- The SIP endpoint loses power temporarily.
- A restart of the SIP endpoint becomes necessary.
- A temporary WAN outage prevents an update of the MWI when a message was left for the subscriber.
- A hot desking subscriber logs in at a remote office telephone. Refer also to Section 5.14, “Hot Desking”, on page 5-14
- The SIP endpoint is not registered at the time the SIP message would otherwise be sent.

- For MWI to be delivered, the station call forwarding—voice mail feature must be subscribed to. Refer to Section 4.12, “Call Forwarding, Station—Voice Mail”, on page 4-13.
- For subscribers to continue to receive accurate MWI in the circumstances listed above, the feature profile for status notification must be provisioned for the subscriber’s DN. Refer also to **Section 5.13, “Feature Status Notification”, on page 5-13**.

18.9.2 Functional Operation

When a call cannot be answered by a subscriber of a voice mail system (sometimes known as a *message storage and retrieval [MSR] system*), the following takes place:

- **If the voice mail system is connected to the HiPath 8000 via SIP**: Whenever a call is automatically redirected by a station call forwarding feature from the subscriber's DN to the voice mail system, the caller is automatically redirected to the called party’s voice mailbox.
- **If the voice mail system is connected to the HiPath 8000 via SIP-Q (the voice mail system is located in the HiPath 4000 SIP-Q network):**
  - If the call is not forwarded to another subscriber, the caller is automatically redirected to the called party’s voice mailbox.
  - If the call is forwarded to another subscriber, the caller must enter the originally called party’s mailbox number to leave a message in the correct mailbox.

After the call is redirected, the calling party can then leave a message for the voice mail system subscriber.

After the voice mail system sends a request, the HiPath 8000 updates the status of the MWI in order to provide the subscriber notification of the waiting message.

The HiPath 8000 supports the message waiting indicator notification function according to the mandatory requirements of GR-866-CORE. VMWI is supported according to GR-1401-CORE.

The indications are provided through signaling and interworking with Siemens or third-party voice mail systems.

18.9.3 Guidelines for Implementation and Use

The HiPath 8000 meets the requirements for simplified message desk interface (SMDI)/MWI support of private numbering plans. The default is for translation to take place against the E.164 numbering plan.

It is possible to provision the HiPath 8000 such that translation takes place against the private numbering plan assigned to one of the following:

- **If the voice mail system is adjacent to the HiPath 8000:** The endpoint profile of the voice mail system
- **If the voice mail system resides on a HiPath 4000**: The endpoint profile of the incoming SIP-Q gateway

Refer to the *HiPath 8000 Configuration and Administration Using CLI Guide* for information about the RTP parameter settings required for support of translation against private numbering plans.

However, it is highly recommended that the routing be provisioned in the E.164 default numbering plan as an E.164 number. Doing so avoids the possibility of having to repeat the provisioning process if the organization's growth leads to overlapping extensions. This is also true for hosting scenarios where different companies might use the same extensions.

Refer also to the following:

- Section 6.7, "Business Group Dialing Plan", on page 6-5
- Section 9.3, "E.164 Compliance", on page 9-2

18.10 Overload Handling

18.10.1 Definition

The overload handling feature:

- Provides for alerts to the signaling managers and other applications if overload or congestion situations occur
- Provides protection from overload-induced node failure

- Ensures that accepted calls result in completed calls

Overload can occur due to random periods of high traffic or administration and maintenance activities. Therefore, the overload mechanism monitors response time and tracks the number of messages on input queues. The signaling managers and applications then respond to the situations appropriately.

Overload controls do not require administration.

18.10.2 Functional Operation

Each signaling type (such as SIP, SIP-Q, MGCP, and CSTA) has its own overload protection manager. When the system runs below 70% utilization, all calls that are initiated are completed. After the percentage goes above 70%, calls are rejected based on the current overload level calculation, which reduces the load on the system. As response times increase, the rate of rejected calls also increases. Call requests that were accepted before going into the overload condition are unaffected.

The overload feature handles lost messages by creating a report to indicate that the message was lost. The system logs the number of calls rejected in a specific time period (for example, 5 or 10 seconds).

The overload handling manager calculates load level indicators by measuring the actual congestion and load levels against configured congestion and load level thresholds. Each time a signaling manager or application's load level indicator changes, the overload handling manager reports this change.

For example, the overload handling manager controls the number of new call attempts that occur over a specified period of time by reporting all instances in which the number of new call attempts exceeds a configured threshold value. The corresponding signaling managers can then react accordingly to prevent an overload condition.

Table 18-1 lists and describes the load level thresholds. These levels can be viewed via the *i*NMC or HiPath 8000 Assistant.

Threshold	Threshold Description	Maximum Value
Cycle timer (ms)	This value represents how often the Overload Handling Manager recalculates the load level indicators and updates the congestion level indicators.	5000
Maximum new call attempts	This value represents the upper limit of new call attempts. This limit is configured as a rate of calls per second, and is converted internally to the number of new calls permitted within the scanning cycle time.	200

Table 18-1 Overload Handling Feature—Load Level Thresholds (Sheet 1 of 2)

Threshold	Threshold Description	Maximum Value
Minor CPU usage	This value represents the minor load congestion level threshold value (as a percent) for CPU usage.	90
Major CPU usage	This value represents the major load congestion level threshold value.	95
Critical CPU usage	This value represents the critical load congestion level threshold value.	98
Minor memory usage	This field displays the minor load congestion level threshold value (as a percent above a high water mark of 98.5%) for resident memory usage.	10
Major memory usage	This field displays the minor load congestion level threshold value.	50
Critical memory usage	This field displays the critical load congestion level threshold value.	75

Table 18-1 Overload Handling Feature—Load Level Thresholds (Sheet 2 of 2)

18.11 Recovery Handling

The recovery handling feature provides a mechanism for controlling failure situations via a fault manager process. This process registers with the RTP node manager for notification of certain critical events occurring in the system. In addition to the fault manager, each call processing process manages its own internally detected faults and maps them to protocol-specific cause values.

18.12 SDP Transparency

18.12.1 Definition

The session description protocol (SDP) transparency feature enables the end-to-end signaling required to realize the negotiation capabilities of disparate network elements. It is required to enable multiple media descriptions and the associated codec attribute information to the destination.

The growth and maturity of IP-based networks have enabled vendors to offer integrated voice and data services. Solutions for the replacement of circuit-switched networks as well as next generation voice and multimedia services based on voice over broadband (VoBB) are available. Inside these networks, various gateway, and media services with different capabilities are available. To allow for network optimization and best bandwidth utilization inside the network, a session or media negotiation framework is required.

In addition, within a session media type, various encodings in the form of codec specifications are available, which permits efficient utilization of the bandwidth resource for the media session. The network elements involved in the media exchange are able to negotiate their media encoding requirements at various stages of the media session or call.

SDP transparency is required to enable the end-end signaling for realizing these negotiation capabilities. For example, it permits the following to take place:

- Negotiating media types for the session—for example, video, image, or audio
- Negotiating the codecs to be used for the various media types
- Communicating supported attributes related to the negotiated codecs
- Renegotiating the media session when conditions change—for example, fax or modem detection.
- Communicating desired signaling capabilities using the media stream—for example, DTMF telephone events and T.38 fax
- Combining media types—for example, audio and video for video calling

For user telephone event signaling, DTMF inband signaling using G.711 has been the preferred method. With the increased use of compressed codecs, e.g., G.72x, sending DTMF inband is not possible. As a result, similar to T.38 Fax, new inband signaling procedures in accordance with RFC 2833, *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, have been defined.

18.12.2 Functional Operation

The HiPath 8000 transports SDP information transparently end-to-end, similar to a SIP proxy. For endpoint-originated session descriptions negotiated with the HiPath 8000, the associated SDP attributes enable signaling the applicable session requirements to the destination.

In the process, the SDP transparency feature:

- Considers the requested session description from the endpoint making the session offer, the allowed session capability from the network operator's perspective for the endpoint and the session description answer of the destination endpoint.
- Considers the various media types, codecs, and their associated attributes for transport.
- Allows the transport of the SDP information transparently not only at the beginning of the session, but also mid-session to enable signaling modifications to the media stream.

The HiPath 8000 supports multiple signaling types including SIP, SIP-Q, and CAS that convey media information. To enable SDP transparency, UCE messages that convey media information between the UCE and the signaling managers contain data to support the data transport.

For SIP endpoints, SDP data is transported transparently without parsing, which permits the SIP session manager to forward the received SDP data to the second leg of the call without any modification in the parameters.

Within the HiPath 8000, the UCE is the interacting coordinator among different signaling types. The connection control manager (CCM) is not aware of the remote endpoint it is talking to. However, because the UCE does not decode the SDP, the CCM parses the minimum required elements and passes it to UCE or session manager, as applicable. The UCE uses this information to establish B-side connections.

18.12.3 Application Examples

In the HiPath 8000, SDP transparency is employed primarily in support of, but not limited to, video calling, DTMF signaling, and modem/fax capabilities, as follows:

- Video calling scenarios involve point-to-point video-capable SIP user endpoints. The session capability negotiation is end-to-end, and requires a transparent SDP transport between the session users.
- DTMF handling scenarios require DTMF tone signaling to a number of media gateway devices. These include the media server used for subscriber-controlled input for features, the UM server, and the PSTN. These instances require negotiation of RFC 2833 telephone events to each media gateway device through the HiPath 8000. The session capability for handling this class of signaling requires the transparent transport of these session capabilities end-to-end.
- For fax handling, the method of sending faxes requires the fax user to negotiate sending the fax to the called destination, preferably using T.38 Fax procedures. If the T.38 negotiation fails, G.711 is used as a fallback. The transport of the needed session parameters requires them to be transported transparently to allow the end-to-end session negotiation to occur.

  Likewise, modem calls require similar negotiations to fax. The negotiation can be a result of modem calling from the PSTN to users in the HiPath 8000-managed network or to those supported by an application server.

18.12.4 CDR

The CDR information reflects the negotiated session description in both directions.

18.13 Silence Suppression Disabling

The silence suppression disabling feature enables proper fax transmission through the applicable gateways when the start of the fax is detected. This feature is needed when G.711 is used for fax/modem transmission.

18.14 SOAP Interface

The simple operations and administration protocol (SOAP) interface feature provides an interface between the HiPath 8000 and the following management tools:

- **Service Management Center (*i*SMC):** The *i*SMC is a full-featured interface that system administrators use to control all subscriber-related capabilities and features.
- **HiPath 8000 Assistant:** HiPath 8000 Assistant is a network management software product used in the compact HiPath 8000. It performs the functions the *i*NMC and *i*SMC normally perform in the HiPath 8000.
- **Subscriber Self-Care Center (*i*SSC):** The *i*SSC is a toolkit for providing call feature control to subscribers via a Web portal. In essence, the *i*SSC provides a SOAP/XML interface into selected feature configuration subsystems on the HiPath 8000. When integrated into a carrier Web portal, subscribers have the option to configure their features (such as call forwarding, selective call rejection, and so on) via the Internet or via the conventional telephone keypad interface.

  The *i*SSC is a subset of the *i*SMC. The system administrator specifies the features subscribers are permitted to change.

Configuring the HiPath 8000, the *i*SMC or HiPath 8000 Assistant, and the *i*SSC to transfer SOAP over IPsec provides security for the SOAP interface. Refer to Section 14.9, “IPsec Baseline”, on page 14-8.

The SOAP interface also permits the generic export mechanism (GEM) to send queries to the HiPath 8000 that permit data synchronization between the HiPath 8000 and the CAP/CSTA interface. Refer to Section 18.4, “Data Synchronization”, on page 18-2.

18.15 System History Log

18.15.1 Definition

The system history log feature provides a log that is used to maintain a history of significant events pertaining to a particular HiPath 8000 installation.

18.15.2 Functional Operation

The system administrator can define a significant event to be any of the following:

- Initial installation
- Patch installations
- Upgrade activities

- Backup and restore activities
- Recent change functions

Logging configurations (level, filename, output destination) are controlled by process level through either the GUI, command line interface, or SNMP.

Each process in the system generates its own log. The log is formatted as a flat file which can be viewed by using a standard editor and includes the option of being output to the screen or to some other type of viewpoint.

The log entry contains the following:

- Source process
- Date and time of log
- Severity level
- Debugging text (output)

18.16 T.38 Fax Support

The T.38 fax support feature provides support for T.38 Facsimile UDP transport layer protocol (UDPTL) according to RFC 2833. The capability to send, receive, and process the signals to and from the gateway for tone detection and T.38 fax relay events is provided. Only support of the loose call agent controlled mechanism is provided, since it is not required to identify the support for T.38 at the start of the call.

An administration parameter is provided for trunk gateways and SIP endpoints to select the T.38 fax relay support capability.

A Alphabetical Feature Listing

This appendix provides a comprehensive, alphabetical list of HiPath 8000 features, classified by feature type. It includes a cross-reference to assist in easily locating each feature description in this guide.

The following feature types represent user features provided by the HiPath 8000:

- HiPath 8000-based station call forwarding
- Other user features

Refer to Chapter 2, “SIP Endpoint User Features” for information about user features provided locally by SIP endpoints.

Where applicable, Table A-1 also includes alternate names for HiPath 8000 features.

Feature	Feature Type	Description
555-1212 line numbers	Routing and translation	Section 9.7.1 on page 9-4
A-side signaling-based routing	Routing and translation	Section 9.8.1 on page 9-5
Account and password management security	Security	Section 14.1 on page 14-1
Account codes	Business group	See *business group account codes*.
Administrator identification and authentication	Serviceability	Section 15.1 on page 15-1
Agent for OAM&P	System functions and features	Section 18.1 on page 18-1
Alarm reporting	System functions and features	Section 18.2 on page 18-1
Alternate routing	Routing and translation	Section 9.8.2 on page 9-5
Alternate routing with overflow among route types	Routing and translation	Section 9.8.3 on page 9-5
Anonymous call rejection	Other user features	Section 5.1 on page 5-1
Announcements	System functions and features	Section 18.3 on page 18-2

Table A-1 HiPath 8000 Feature Listing and Cross-Reference (Sheet 1 of 13)

Feature	Feature Type	Description
Application servers—interworking	SIP signaling	See *interworking with application servers.*
Attendant answering position	Business group	Section 6.1 on page 6-1
Audible ringing on rollover lines	Keyset telephone user	Section 3.1 on page 3-2
Audit mechanisms	SIP signaling	Section 16.1 on page 16-1
Audits, internal	System functions and features	See *internal audits.*
Authorization codes	Business group	See *business group authorization codes*.
Automated attendant systems—interworking	System functions and features	See *interworking with automated attendant systems.*
Automatic callback	Other user features	Section 5.2 on page 5-3
Automatic recall	Other user features	See *return call.*
Backup and restore	Serviceability	Section 15.2 on page 15-2
Basic traffic tool	Serviceability	Section 15.3 on page 15-3
Bearer capability routing	Routing and translation	Section 9.8.4 on page 9-6
Billing records security	Security	Section 14.2 on page 14-2
Business group access codes	Business group	Section 6.2 on page 6-3
Business group account codes	Business group	Section 6.3 on page 6-3
Business group authorization codes	Business group	Section 6.4 on page 6-3
Business group billing	Business group	Section 6.5 on page 6-4
Business group department names	Business group	Section 6.6 on page 6-4
Business group dialing plan	Business group	Section 6.7 on page 6-5
Business group main number	Business group	Section 6.8 on page 6-7
Business group traffic measurements	Business group	Section 6.9 on page 6-7

Table A-1 HiPath 8000 Feature Listing and Cross-Reference (Sheet 2 of 13)

Feature	Feature Type	Description
Business group web portal	Business group	Section 6.10 on page 6-9
Call admission control	Call admission control features	Section 10.1 on page 10-1
Call completion on busy subscriber	Other user features	See *automatic callback*.
Call detail record generation	CDR	Section 13.2 on page 13-1
Call forwarding—no reply	HiPath 8000-based station call forwarding	See *call forwarding—don't answer (CFDA).*
Call forwarding—selective	Other user features	See *selective call forwarding*.
Call forwarding—unconditional	HiPath 8000-based station call forwarding	See *call forwarding—all calls.*
Call forwarding—variable	HiPath 8000-based station call forwarding	See *call forwarding—all calls.*
Call forwarding, station—all calls	HiPath 8000-based station call forwarding	Section 4.1 on page 4-2
Call forwarding, station—busy line (CFBL)	HiPath 8000-based station call forwarding	Section 4.2 on page 4-4
Call forwarding, station—courtesy call	HiPath 8000-based station call forwarding	Section 4.3 on page 4-5
Call forwarding, station—don't answer (CFDA)	HiPath 8000-based station call forwarding	Section 4.4 on page 4-6
Call forwarding, station—enhanced	HiPath 8000-based station call forwarding	See *call forwarding—time-of-day*.
Call forwarding, station—fixed	HiPath 8000-based station call forwarding	Section 4.6 on page 4-8
Call forwarding, station—remote activation (RACF)	HiPath 8000-based station call forwarding	Section 4.7 on page 4-9
Call forwarding, station—remote call forwarding (RCF)	HiPath 8000-based station call forwarding	Section 4.8 on page 4-10
Call forwarding, station—return	HiPath 8000-based station call forwarding	Section 4.9 on page 4-10

Table A-1 HiPath 8000 Feature Listing and Cross-Reference (Sheet 3 of 13)

Feature	Feature Type	Description
Call forwarding, station—time-of-day	HiPath 8000-based station call forwarding	Section 4.11 on page 4-11
Call forwarding, station—voice mail	HiPath 8000-based station call forwarding	Section 4.12 on page 4-13
Call gapping code controls	Serviceability	Section 15.4 on page 15-4
Call pickup—group	Other group features	Section 7.1 on page 7-1
Called name delivery	Other user features	See *caller identity service*.
Caller ID	Other user features	See *caller identity service*, *calling identity delivery and suppression, calling name delivery blocking (CNAB),* and *calling number delivery blocking (CNDB),* and *customer-originated trace.*
Caller identity service	Other user features	Section 5.4 on page 5-4
Calling identity delivery and suppression	Other user features	Section 5.5 on page 5-6
Calling name delivery	Other user features	Section 5.6 on page 5-7
Calling name delivery blocking (CNAB)	Other user features	Section 5.7 on page 5-8
Calling number delivery	Other user features	Section 5.8 on page 5-9
Calling number delivery blocking (CNDB)	Other user features	Section 5.9 on page 5-10
Calling number delivery over PRI	PRI	Section 11.1 on page 11-1
Calling number delivery over PRI—emergency calls	PRI	Section 11.2 on page 11-1
Calling number screening over PRI	PRI	Section 11.3 on page 11-1
CDR—intermediate long duration records	CDR	See *intermediate long duration records.*
Cisco gateway	Emergency calling	Section 8.3.3 on page 8-5
Carrier access codes	Routing and translation	Section 9.7.2 on page 9-4

Table A-1 HiPath 8000 Feature Listing and Cross-Reference (Sheet 4 of 13)

Feature	Feature Type	Description
Click to answer	Other user features	Section 5.10 on page 5-10
Conference, station-controlled	Other user features	Section 5.11 on page 5-11
Convedia CMS 1000 media server support	System functions and features	See *media server support.*
Courtesy call	HiPath 8000-based station call forwarding	See *call forwarding—courtesy call.*
CSTA protocol interface	CSTA support	Section 17.1 on page 17-2
CSTA services support	CSTA support	Section 17.2 on page 17-3
Customer-originated trace	Other user features	Section 5.12 on page 5-13
Data file security	Security	Section 14.3 on page 14-3
Data synchronization	System functions and features	Section 18.4 on page 18-2
Department names	Business group	See *business group department names.*
Destination codes	Routing and translation	Section 9.7.3 on page 9-4
Diagnostics tool	Serviceability	Section 15.5 on page 15-4
Dialing plan—business group	Business group	See *business group dialing plan.*
Digit modification for digit outpulsing	Routing and translation	Section 9.1 on page 9-1
Direct inward dialing	Business group	Section 6.11 on page 6-9
Direct outward dialing	Business group	Section 6.12 on page 6-10
Direct station select keys	Keyset telephone user	Section 3.3 on page 3-4
Directory number announcement	Routing and translation	Section 9.2 on page 9-1
Displays during calling	Other user features	See *caller identity service.*
Distinctive ringing	Business group	Section 6.13 on page 6-10
E.164 compliance	Routing and translation	Section 9.3 on page 9-2
E911 support	Emergency calling	Section 8.1 on page 8-1
Element mass provisioning	Serviceability	Section 15.6 on page 15-5

Table A-1 HiPath 8000 Feature Listing and Cross-Reference (Sheet 5 of 13)

Feature	Feature Type	Description
Endpoint control licensing	Serviceability	Section 15.7 on page 15-5
Enhanced call forwarding (ECF)	HiPath 8000-based station call forwarding	See *call forwarding—time-of-day*.
Event logging	Security	Section 14.5 on page 14-4
Extension dialing	Business group	Section 6.14 on page 6-11
Feature status notification	Other user features	Section 5.13 on page 5-13
File transfer security	Security	Section 14.6 on page 14-6
Flexible digit processing	CSTA support	Section 17.3 on page 17-4
Focus	Keyset telephone user	See *line focus*.
Genesys call center—interworking	SIP signaling	See *interworking with Genesys call center.*
Group call pickup	Other group features	See *call pickup—group*.
Group-level feature administration	Business group	Section 6.15 on page 6-11
HiPath 8000-provided calling name	CSTA support	Section 17.5 on page 17-5
HiPath ProCenter integration	SIP signaling	See *integration with HiPath ProCenter.*
HiPath Xpressions integration	SIP signaling	See *integration with HiPath Xpressions*.
Hold, manual	Keyset telephone user	See *manual hold*.
Hot desking	Other user features	Section 5.14 on page 5-14
Hoteling	Other user features	See *hot desking.*
HTTP digest authentication	SIP signaling	Section 16.2 on page 16-1
Hunt group	Other group features	Section 7.2 on page 7-3
Hunt group—make busy	Other group features	Section 7.3 on page 7-5
Hunt group—night service	Other group features	Section 7.5 on page 7-6
Hunt group—no answer advance	Other group features	Section 7.6 on page 7-7

Table A-1 HiPath 8000 Feature Listing and Cross-Reference (Sheet 6 of 13)

Feature	Feature Type	Description
Hunt group—queuing	Other group features	Section 7.8 on page 7-8
Hunt group—stop hunt	Other group features	Section 7.9 on page 7-9
Hunt group—traffic measurements	Other group features	Section 7.10 on page 7-9
Hypertext transfer protocol over SSL	Security	Section 14.7 on page 14-7
In-use indication	Keyset telephone user	See *visual indicators for line and feature key status*.
*i*NMC and *i*SMC security	Security	Section 14.8 on page 14-7
Integration with Fault Management	CSTA support	Section 17.6 on page 17-5
Integration with HiPath ProCenter	SIP signaling	Section 16.4 on page 16-3
Integration with HiPath Xpressions	SIP signaling	Section 16.3 on page 16-3
Integration with OpenScape	SIP signaling	Section 16.5 on page 16-5
Intercept treatment	Routing and translation	Section 9.4 on page 9-2
Interchangeable NPA and NXX	Routing and translation	Section 9.7.4 on page 9-4
Intermediate long duration records	CDR	Section 13.3 on page 13-2
Internal audits	System functions and features	Section 18.5 on page 18-2
International translation support	Routing and translation	Section 9.5 on page 9-3
Interworking with application servers	SIP signaling	Section 16.6 on page 16-6
Interworking with automated attendant systems	System functions and features	Section 18.6 on page 18-3
Interworking with Genesys call center	SIP signaling	Section 16.7 on page 16-6
Interworking with RG 8700	SIP signaling	Section 16.8 on page 16-6

Table A-1 HiPath 8000 Feature Listing and Cross-Reference (Sheet 7 of 13)

Feature	Feature Type	Description
Interworking with unified messaging systems	SIP signaling	Section 16.9 on page 16-7
Interworking with voice conferencing applications	SIP signaling	Section 16.10 on page 16-7
Interworking with voice mail systems	SIP signaling	Section 16.11 on page 16-8
IP Unity media server support	System functions and features	See *media server support.*
IPsec baseline	Security	Section 14.9 on page 14-8
Keyset operation modes	Keyset telephone user	Section 3.4 on page 3-5
Language announcements, multiple	Business group	See *multiple language announcements.*
Last number redial	Other user features	See *automatic callback.*
Leading digit and most-matched digit translation	Routing and translation	Section 9.6 on page 9-3
Line focus	Keyset telephone user	Section 3.5 on page 3-8
Line key operation modes	Keyset telephone user	Section 3.6 on page 3-8
Line reservation	Keyset telephone user	Section 3.7 on page 3-9
Line restriction	Business group	See *station restrictions.*
Local management	System functions and features	Section 18.7 on page 18-3
Log file retrieval tool	Serviceability	Section 15.9 on page 15-6
Login categories	Security	Section 14.10 on page 14-9
Maintenance manager	Serviceability	Section 15.10 on page 15-6
Make busy	Other group features	See *hunt group—make busy.*
Malicious call trace	Other user features	See *customer-originated trace.*
Manual hold	Keyset telephone user	Section 3.8 on page 3-10
Media server support	System functions and features	Section 18.8 on page 18-3
Message waiting indicator support	System functions and features	Section 18.9 on page 18-3
	CSTA support	Section 17.7 on page 17-5
Multiline appearance	Keyset telephone user	Section 3.9 on page 3-11

Table A-1 HiPath 8000 Feature Listing and Cross-Reference (Sheet 8 of 13)

Feature	Feature Type	Description
Multiline origination and transfer	Keyset telephone user	Section 3.10 on page 3-13
Multiline preference	Keyset telephone user	Section 3.11 on page 3-14
Multiple language announcements	Business group	Section 6.16 on page 6-12
Multiple time zone support	CSTA support	Section 17.8 on page 17-5
Music on hold—HiPath 8000-based	Other user features	Section 5.16 on page 5-15
Multiline hunt group (MLHG)	Other group features	See *hunt group.*
Name delivery	Other user features	See *calling name delivery (CNAM).*
NANP compliance	Routing and translation	Section 9.7 on page 9-3
Night service	Other group features	See *hunt group—night service.*
No answer advance	Other group features	See *hunt group—no answer advance.*
OpenScape integration	SIP signaling	See *integration with OpenScape.*
Origin-dependent routing	Routing and translation	Section 9.8.5 on page 9-6
Outgoing caller ID presentation status (name)	Other user features	See *calling name delivery blocking (CNAB).*
Outgoing caller ID presentation status plus (number)	Other user features	See *calling number delivery blocking (CNDB).*
Outgoing name delivery block	Other user features	See *calling name delivery blocking (CNAB).*
Outgoing number delivery block	Other user features	See *calling number delivery blocking (CNDB).*
Overload handling	System functions and features	Section 18.10 on page 18-5
Password encryption	Security	Section 14.11 on page 14-9
Password management security	Security	See *account and password management security.*

Table A-1 HiPath 8000 Feature Listing and Cross-Reference (Sheet 9 of 13)

Feature	Feature Type	Description
Phantom lines	Keyset telephone user	Section 3.12 on page 3-15
Pickup group	Other group features	See *call pickup—group*.
Prefix digit translation	Routing and translation	Section 9.7.5 on page 9-5
PRI supported and unsupported features	PRI	Section 11.4 on page 11-2
PRI trunking	PRI	Section 11.5 on page 11-2
Process debug tool	Serviceability	Section 15.12 on page 15-7
Provisional responses reliability	SIP signaling	Section 16.12 on page 16-8
Provisioning and security logging	Security	Section 14.12 on page 14-10
Query of subscriber transient operational status	Serviceability	Section 15.13 on page 15-7
Queuing	Other group features	See *hunt group—queuing.*
QSIG tunneling for basic call	QSIG tunneling	Section 12.1 on page 12-1
Recall	Other user features	See *return call.*
Recovery handling	System functions and features	Section 18.11 on page 18-7
Redial—last number with monitoring	Other user features	See *last number redial with monitoring.*
Remote activation call forwarding (RACF)	HiPath 8000-based station call forwarding	Section 4.7 on page 4-9
Remote restart	Serviceability	Section 15.14 on page 15-7
Rerouting based on SIP response codes	Routing and translation	Section 9.8.6 on page 9-6
Return call	Other user features	Section 5.17 on page 5-16
Ring tone, distinctive internal and external	Business group	See *distinctive ringing.*
Rollover ringing	Keyset telephone user	See *audible ringing on rollover lines*.
Routing—A-side signaling-based	Routing and translation	See *A-side signaling-based routing*.
Routing—alternate	Routing and translation	See *alternate routing.*

Table A-1 HiPath 8000 Feature Listing and Cross-Reference (Sheet 10 of 13)

Feature	Feature Type	Description
Routing—alternate with overflow among route types	Routing and translation	See *alternate routing with overflow among route types.*
Routing—bearer capability	Routing and translation	See *bearer capability routing.*
Routing—origin-dependent	Routing and translation	See *origin-dependent routing.*
Routing—time-of-day	Routing and translation	See *time-of-day routing.*
Screen list editing	Other user features	Section 5.18 on page 5-17
SDP transparency	System functions and features	Section 18.12 on page 18-7
Secure CLI	Security	Section 14.13 on page 14-10
Secure HTTP	Security	See *hypertext transfer protocol over SSL.*
Secure Shell on the iNMC/*i*SMC/HiPath 8000 Assistant interface	Security	Section 14.14 on page 14-10
Selective call acceptance	Other user features	Section 5.19 on page 5-17
Selective call forwarding	Other user features	Section 5.20 on page 5-19
Selective call rejection	Other user features	Section 5.21 on page 5-21
Serial ringing	Other user features	Section 5.22 on page 5-22
Service access codes	Routing and translation	Section 9.7.6 on page 9-5
Silence suppression disabling	System functions and features	Section 18.13 on page 18-9
Simultaneous ringing	Other user features	Section 5.23 on page 5-25
SIP audit mechanisms	SIP signaling	See *audit mechanisms*.
SIP endpoint support	SIP signaling	Section 16.13 on page 16-8
SIP interworking with application servers	SIP signaling	See *interworking with application servers.*
SIP over TCP/TLS support	SIP signaling	Section 16.14 on page 16-9
SIP privacy mechanism	Security	Section 14.16 on page 14-11

Table A-1 HiPath 8000 Feature Listing and Cross-Reference (Sheet 11 of 13)

Feature	Feature Type	Description
SIP REFER method support	SIP signaling	Section 16.16 on page 16-10
SIP session management—concurrent sessions	SIP signaling	Section 16.17 on page 16-10
SIP UA registration renewal during WAN outage	SIP signaling	Section 16.18 on page 16-11
SIP UPDATE method support	SIP signaling	Section 16.19 on page 16-11
SOAP interface	System functions and features	Section 18.14 on page 18-10
Softswitches—interworking	SIP signaling	See *interworking with softswitches.*
Speed dial	Other user features	See *station speed calling—HiPath 8000-based.*
Station call forwarding	HiPath 8000-based station call forwarding	See *call forwarding* and *call forwarding, station.*
Station-controlled conference	Other user features	See *conference, station-controlled.*
Station dialing	Other user features	Section 5.24 on page 5-27
Station restrictions	Business group	Section 6.17 on page 6-12
Station-to-station calling	Business group	See *extension dialing*.
Stop hunt	Other group features	See *hunt group—stop hunt.*
System history log	System functions and features	Section 18.15 on page 18-10
Station speed calling—HiPath 8000-based	Other user features	Section 5.25 on page 5-29
System software and patch level status	Serviceability	Section 15.15 on page 15-7
System upgrade	Serviceability	Section 15.16 on page 15-8
T.38 fax support	System functions and features	Section 18.16 on page 18-11
Teleworking	Other user features	Section 5.26 on page 5-30

Table A-1 HiPath 8000 Feature Listing and Cross-Reference (Sheet 12 of 13)

Feature	Feature Type	Description
Time-of-day call forwarding	HiPath 8000-based station call forwarding	See *call forwarding—time-of-day.*
Time-of-day routing	Routing and translation	Section 9.8.7 on page 9-7
TLS support	Security	Section 14.17 on page 14-12
Toll and call restrictions	Other user features	Section 5.27 on page 5-31
Traffic measurements—business group	Business group	See *business group traffic measurements.*
Traffic measurements—hunt group	Hunt group	See *hunt group traffic measurements.*
Traffic tool, basic	Serviceability	See *basic traffic tool.*
Transfer	Other user features	Section 5.28 on page 5-32
Transfer security	Other user features	Section 5.29 on page 5-36
Unified messaging systems—interworking	SIP signaling	See *interworking with unified messaging systems.*
Usage reporting	CDR	Section 13.5 on page 13-3
Usage-sensitive call forwarding variable	HiPath 8000-based station call forwarding	See *call forwarding—all calls.*
Vertical service codes	Routing and translation	Section 9.9 on page 9-7
Virtual DN	Routing and translation	Section 9.10 on page 9-8
Visual indicators for line and feature key status	Keyset telephone user	Section 3.14 on page 3-17
VLAN provisioning	Serviceability	Section 15.17 on page 15-8
Voice conferencing applications—interworking	SIP signaling	See *interworking with voice conferencing applications*.
Voice mail systems—interworking	SIP signaling	See *interworking with voice mail systems.*
Voice VPN	Business group	Section 6.18 on page 6-14

Table A-1 HiPath 8000 Feature Listing and Cross-Reference (Sheet 13 of 13)

B Feature Access Codes

Users can invoke features that reside in the HiPath 8000 without special feature keys by entering feature access codes. Feature access codes are sometimes known as *vertical service codes.*

Features that reside in the SIP endpoint are *not* invoked with feature access codes. Refer to the applicable user manual for more information.

Table B-1 lists the default feature access codes. Features that do not have specified default access codes are not listed in this table.

Feature	Access Code
Anonymous call rejection	*77 (activate) *87 (deactivate)
Automatic callback	*66 (activate) #66 (deactivate)
Call forwarding—all calls	*72 (activate) *73 (deactivate)
Call forwarding—busy line	*90 (activate) *91 (deactivate)
Call forwarding—don't answer	*92 (activate) *93 (deactivate)
Call forwarding—selective	*63 (activate) *83 (deactivate)
Call pickup—group	**3
Calling ID delivery and suppression	*64 (deliver) *45 (suppress)
Calling name delivery blocking	*68
Calling number delivery blocking	*67
DN announcement	*99
Hunt group—stop hunt	#*93 (activate) #*92 (deactivate)
Return call	*69 (activate) *89 (deactivate)

Table B-1 Default Feature Access Codes (Sheet 1 of 2)

Feature	Access Code
Selective call acceptance	*27 (activate) *28 (deactivate)
Selective call rejection	*60 (activate) *80 (deactivate)
Station speed calling, HiPath 8000-based—one-digit list programming	*74
Station speed calling, HiPath 8000-based—two-digit list programming	*75
Trace, customer-originated	*57

Table B-1 Default Feature Access Codes (Sheet 2 of 2)

C Supported SIP Methods

Several feature descriptions in this guide make references to *SIP methods*. This appendix provide a brief description of each. Contact your Siemens representative for sources of detailed information about SIP, its operation, and its uses.

Table C-1 lists and describes the SIP methods the HiPath 8000 supports.

Method	Description
ACK	This method indicates successful session setup. It is sent by the node that initiates a call.
BYE	This method terminates a session.
CANCEL	This method nullifies a previously issued request.
INVITE	This method initiates a call. It contains a session description protocol (SDP) descriptor of the call. This method can also be used to modify the media during a confirmed session and to maintain keep-alive timers.
PRACK	This method provides a provisional response used to establish a connection before call completion.
REFER	This method provides the signaling for a user to transfer one user to another.
REGISTER	This method provides the mechanism for a device to identify itself as capable of processing requests for a given DN by identifying its contact address. A device may unregister using the same method by identifying an immediate expiration.
UPDATE	This method provides the mechanism for a client to update parameters of a session (such as the set of media streams and their codecs), but has no impact on the state of a dialog.

Table C-1 HiPath 8000 Supported SIP Methods

Index

Numerics

A

B

C

D

E

F

G

H

I

N

O

P

T

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 Enterprise Communications GmbH & Co. KG or their respective owners.

Hofmannstraße 51 • D-81359 München, Germany
Reference No.: A31003-H8022-F100-2-7618