Voice over IP (VoIP)
NetPerformer® System Reference

MEMOTEC
redefining network efficiency

COPYRIGHTS AND DISCLAIMERS

Published Date: April 2011

Document # 1608

Memotec Inc. reserves the right to make changes without notice in product or component design as warranted by evolution in user needs or progress in engineering or manufacturing technology. Changes which affect the operation of the unit will be documented in the next revision of the manual.

We have made every effort to ensure the accuracy of the information presented in our documentation. However, Memotec assumes no responsibility for the accuracy of the information published. Product documentation is subject to change without notice. Changes, if any, will be incorporated in new editions of these documents. Memotec may make improvements or changes in the products or programs described within the documents at any time without notice. Mention of products or services not manufactured or sold by Memotec is for informational purposes only and constitutes neither an endorsement nor a recommendation for such products or services.

Memotec Inc. is a wholly owned subsidiary of Comtech EF Data Corp., and its parent company Comtech Telecommunications Corp (NASDAQ: CMTL).

AccessView, CXTool, CX-U Series, CX-UA Series, AbisXpress, NetPerformer, AccessGate, ACTView, SDM-8400, and the SDM-9000 series of products are either registered trademarks or trademarks of Memotec Inc.in Canada, the United States of America, and in other countries.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Any other trademarks are the property of their respective companies.

Memotec Inc.
7755 Henri Bourassa Blvd. West
Montreal, Quebec
Canada H4S 1P7
Tel.: (514) 738-4781
FAX: (514) 738-4436
www.memotec.com

Contents

Chapter 1: NetPerformer Support of SIP VoIP 1-1

1. 1 NetPerformer SIP VoIP Characteristics 1-2

1. 2 Session Initiation Protocol (SIP) 1-3

1. 3 SIP Connection Types on the NetPerformer 1-3

1.3.1 Point-to-point SIP Connection 1-3
1.3.2 NetPerformer to SIP Proxy Server Connection 1-4
1.3.3 Multipoint SIP Units without SIP Proxy Server 1-5
1.3.4 NetPerformer VoIP Gateway Product 1-5

1. 4 SIP Registration 1-8

1. 5 SIP Call Authentication and Accounting 1-9

1.5.1 RADIUS Authentication and Accounting 1-9
1.5.2 SIP Challenge Call Authentication 1-12
1.5.3 Proxy Server Call Authentication 1-12

1. 6 Other SIP Features Supported 1-14

1.6.1 Enhanced Fax Support 1-14
1.6.2 Clearmode 1-14
1.6.3 CLIR 1-15
1.6.4 ptime Attribute 1-15
1.6.5 Out-of-band Digit Transport 1-15
1.6.6 Private Extensions 1-15
1.6.7 ISUP to SIP Mapping 1-16
1.6.8 Reason Header 1-16

1. 7 Other Components of the NetPerformer SIP VoIP Network 1-17

1.7.1 Clarent Command Center and Database 1-18
1.7.2 Clarent Gateway 1-19
1.7.3 Clarent Connect 1-19
1.7.4 Clarent Call Manager 1-19

1. 8 Network Management Components of the Clarent Softswitch Solution . 1-21

1.8.1 Clarent Application Server 1-21
1.8.2 Clarent Distribution Manager and Package Distributor 1-21
1.8.3 Clarent Domain Controller 1-21
1.8.4 Clarent Network View 1-22
1.8.5 Clarent Assist 1-22

Chapter 2: Configuring SIP VoIP 2-1

2. 1 Selecting SIP VoIP Mode 2-2

2.1.1 Effects of Selecting SIP VoIP Mode 2-2

2. 2 Defining SIP Characteristics on the NetPerformer 2-3

2. 3 Enable SIP and Configure the Global SIP Properties 2-4

2. 4 Configuring the SIP Timer Parameters 2-6

2. 5 Configuring the SIP Authentication Parameters 2-7

2. 6 Configuring the SIP Proxy Parameters 2-8

2. 7 Setting up the Voice Mapping Table 2-10

2.7.1 Adding a MAP Entry 2-11
2.7.2 DIALSTRING Map Type 2-11
2.7.3 DIALIP Map Type 2-12
2.7.4 SUPERMAP Map Type 2-13
2.7.5 Modifying a MAP Entry 2-14
2.7.6 Deleting a MAP Entry 2-15
2.7.7 Ingress and Egress Dial Rule Definitions 2-16

2. 8 Configuring the UA as a Gateway or Endpoint 2-19

Chapter 3: Codec Negotiation 3-1

3. 1 About Codec Negotiation 3-2

3. 2 Negotiation Procedure. 3-3

3.2.1 Negotiation Limitations 3-4

3. 3 Effects of Product Type on the Negotiation Process. 3-5

3.3.1 SDM-9220 and SDM-9230 3-5
3.3.2 SDM-9360, SDM-9380 and SDM-9585 3-5

3. 4 Example Scenarios 3-6

3.4.1 INVITE Lists G7XX 3-6
3.4.2 INVITE Lists ACELP-CN Only 3-6

3. 5 Other Factors Affecting Codec Selection 3-8

3.5.1 DSP Algorithm Limitations (Quadra File). 3-8
3.5.2 Combined Effect of All Factors 3-12

3. 6 Configuring the NetPerformer for Codec Negotiation 3-14

3.6.1 Configuration Tips 3-16

Chapter 4: SIP Hairpin 4-1

4. 1 About the SIP Hairpin function 4-2

4. 2 How SIP Hairpin Works 4-3
4. 3 Hairpin Ingress Calls 4-4
4.3.1 Benefits 4-4
4.3.2 Characteristics 4-4
4. 4 Hairpin Egress Calls 4-5
4.4.1 Benefits 4-5
4.4.2 Characteristics 4-5
4. 5 Configuring the NetPerformer for SIP Hairpin 4-6
4.5.1 Using a DIALIP MAP Entry 4-6
4.5.2 Using Overloaded MAP Entries 4-7
4. 6 Example Applications 4-9
4.6.1 Scenario 1: Using Overloaded MAP Entries 4-9
4.6.2 Scenario 2: Bypassing the SIP Proxy Server 4-10
4.6.3 Scenario 3: Dialing 911 using SIP Hairpin 4-13

Chapter 5: SIP Redirect Server 5-1

5. 1 About the SIP Redirect Server 5-2
5. 2 Call Negotiation 5-3
5. 3 Traffic Volume Considerations 5-4
5.3.1 Examples 5-5
5. 4 Configuring the NetPerformer as a Redirect Server 5-6
5.4.1 Unit 1 5-6
5.4.2 Unit 2 5-7
5.4.3 Redirect Server 5-8

Chapter 6: Monitoring VoIP Functions 6-1

6. 1 About VoIP Functions 6-2
6. 2 Voice Channel Status 6-3
6. 3 SIP Session Status 6-4
6. 4 Negotiated Codec Payload 6-5
6. 5 SIP Counters 6-7
6. 6 Codec Negotiation Table 6-8
6. 7 Voice Channel Parameters 6-9

Chapter 7: SE/SIP Configuration Parameters 7-1

7. 1 GLOBAL Parameters 7-2

7.1.1 Administrative status 7-3
7.1.2 UDP Port 7-3
7.1.3 Gateway ID 7-4
7.1.4 Server group 7-4
7.1.5 ANI digits 7-4
7.1.6 DTMF Payload 7-4
7.1.7 DTMF in SIP INFO packets 7-5
7.1.8 Redirect Server 7-6
7.1.9 Call Accounting 7-6
7.1.10 Call Authentication 7-7
7.1.11 PIN Length 7-7
7.1.12 Caller Line Identity Restriction 7-8

7. 2 TIMER Parameters 7-9

7.2.1 Resend INVITE 7-9
7.2.2 Receiving ACK 7-9
7.2.3 Disconnect (BYE or CANCEL) 7-10
7.2.4 Registration duration 7-10

7. 3 AUTHENTICATION Parameters 7-11

7.3.1 UserName 7-11
7.3.2 UserPassword 7-12

7. 4 CODEC NEGO Parameters 7-13

7.4.1 G729 7-13
7.4.2 G723 7-14
7.4.3 G726-16K 7-14
7.4.4 G726-24K 7-15
7.4.5 G726-32K 7-15
7.4.6 G726-40K 7-15
7.4.7 G711 alaw 7-16
7.4.8 G711 ulaw 7-16

7. 5 PROXY Parameters 7-17

7.5.1 SIP Proxy entry number 7-17
7.5.2 Enable registration 7-18
7.5.3 Proxy server address 7-18
7.5.4 Proxy server UDP Port 7-19
7.5.5 REGISTER expires (s) 7-19
7.5.6 Proxy authentication username 7-19
7.5.7 Proxy authentication password 7-20

Chapter 8: SE/MAP Configuration Parameters 8-1

8. 1 DIALSTRING Map Type 8-2

8.1.1 Operation 8-2
8.1.2 Map type 8-2
8.1.3 Entry digits 8-3
8.1.4 Digits string length 8-3
8.1.5 Egress hunt group pattern 8-4
8.1.6 Egress hunt group ports 8-5
8.1.7 Strip prefix number of digits 8-5
8.1.8 Ingress/Egress prepend string 8-5
8.1.9 Ingress/Egress append string 8-6
8.1.10 Add another map entry 8-7
8. 2 DIALIP Map Type 8-8
8.2.1 Enter an IP address 8-8
8. 3 SUPERMAP Map Type 8-8

Chapter 9: DISPLAY Command Statistics 9-1

9. 1 DS/SIP 9-2
9.1.1 Version 9-2
9.1.2 Current operational state 9-2
9.1.3 Registration status 9-2
9. 2 DC/SIP 9-3
9.2.1 Number of SIP request messages Rx 9-3
9.2.2 Number of SIP request messages Tx 9-3
9.2.3 Number of SIP response messages Rx 9-3
9.2.4 Number of SIP response messages Tx 9-3
9.2.5 Number of total transactions 9-3
9.2.6 Number of INVITE requests Rx 9-4
9.2.7 Number of INVITE requests Tx 9-4
9.2.8 Number of ACK requests Rx 9-4
9.2.9 Number of ACK requests Tx 9-4
9.2.10 Number of BYE requests Rx 9-4
9.2.11 Number of BYE requests Tx 9-5
9.2.12 Number of CANCEL requests Rx 9-5
9.2.13 Number of CANCEL requests Tx 9-5
9.2.14 Number of REGISTER requests Rx 9-5
9.2.15 Number of REGISTER requests Tx 9-6
9.2.16 Number of 1xx class SIP responses Rx 9-6
9.2.17 Number of 1xx class SIP responses Tx 9-6
9.2.18 Number of 2xx class SIP responses Rx 9-6
9.2.19 Number of 2xx class SIP responses Tx 9-6
9.2.20 Number of 3xx class SIP responses Rx 9-7

9.2.21 Number of 3xx class SIP responses Tx 9-7
9.2.22 Number of 4xx class SIP responses Rx 9-7
9.2.23 Number of 4xx class SIP responses Tx 9-7
9.2.24 Number of 5xx class SIP responses Rx 9-8
9.2.25 Number of 5xx class SIP responses Tx 9-8
9.2.26 Number of 6xx class SIP responses Rx 9-8
9.2.27 Number of 6xx class SIP responses Tx 9-8
9.2.28 Number of INVITE retries 9-8
9.2.29 Number of BYE retries 9-9
9.2.30 Number of CANCEL retries 9-9
9.2.31 Number of REGISTER retries 9-9
9.2.32 Number of RESPONSE retries 9-9

Index Index-1

NetPerformer Support of SIP VoIP

NOTE: On the NetPerformer, the SIP VoIP mode of operation is configured using the Global *Voice transport method* parameter, which must be set to **SIP VOIP**. Refer to "Selecting SIP VoIP Mode" on page 2-2 for details.

1.1 NetPerformer SIP VoIP Characteristics

NetPerformer SIP VoIP support is an IP-centric voice/data integration solution that employs Session Initiation Protocol (SIP). This protocol is based on existing Internet and SMTP/HTTP conventions that are well suited for large point-to-point and any-to-any networks. NetPerformer SIP VoIP mode is intended for a broad range of applications and serves the wide area internetworking needs of central sites, regional offices and both large and small branch offices.

- Converges voice and data over PPP links, Frame Relay RFC-1490, ATM RFC-1483 and IP/Ethernet circuits
- Uses Memotec's Signaling Engine technology for SIP-based VoIP transport, standard voice algorithms and both standard and proprietary data protocols and data compression algorithms
- Provides T1/E1 connectivity, including digital connections to PBXs via T1 and E1 using CAS and CCS (QSIG), and offers drop and insert multiplexing for both data and voice
- Maximizes bandwidth usage with high throughput levels, low overhead and minimal delays, and guarantees reliable integration of voice, fax and data traffic.
- Optimizes line utilization with cell-based multi-protocol prioritization, Bandwidth-On-Demand and Load Balancing, and adds provision for line failure with Virtual Connections and dial backup functions
- Significantly reduces communications costs, since it cuts long distance charges, handles time-sensitive applications with reduced delays, and eliminates the need for dedicated voice and data circuits in the network
- Available on the NetPerformer base product as a configurable voice transport mode.

1.2 Session Initiation Protocol (SIP)

SIP is an efficient VoIP protocol that was built on existing Internet and SMTP/HTTP conventions, and in recent years has become the standard protocol for VoIP applications. It provides intelligence at the edge of the network, which allows the end user to take advantage of recent enhancements in voice and Internet applications.

The NetPerformer SIP VoIP mode uses standard SIP (Version 2.0), which allows carriers to:

- Deliver new services quickly and inexpensively
- Offer enterprise customers access to the next generation of IP networks that converge data and voice.

Additional networking capabilities are available to the enterprise market through the flexible NetPerformer base feature set. This provides integrated access to a wide variety of voice and data traffic types.

1.3 SIP Connection Types on the NetPerformer

The NetPerformer with SIP VoIP can transfer SIP in the following ways:

- Point-to-point SIP connection using two User Agents (or UAs, see next section)
- NetPerformer to SIP proxy server connection (see "NetPerformer to SIP Proxy Server Connection" on page 1-4)
- Multipoint NetPerformer network without SIP proxy server (see "Multipoint SIP Units without SIP Proxy Server" on page 1-5).

1.3.1 Point-to-point SIP Connection

In a point-to-point SIP connection, two NetPerformer SIP VoIP units can communicate with each other without an intervening SIP proxy server. Both NetPerformers are SIP enabled endpoints in the network, or User Agents (UAs).

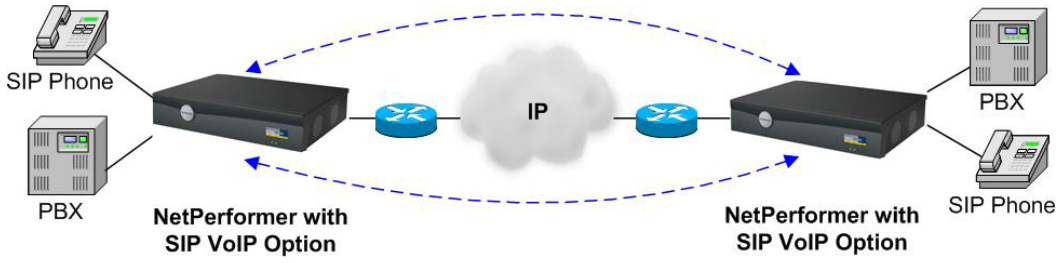

Figure 1-1: NetPerformers with Point-to-point SIP Connection

- On each NetPerformer the *Proxy server address* refers to the IP address of the other unit. For details on this parameter refer to "Proxy server address" on page 7-18.

NOTE: When using the SIP *Proxy server address*, a point-to-point SIP connection (without a SIP proxy server) results in a network composed of only 2 gateways.

- No call logs are maintained. This application can be used in an enterprise network that does not need detailed billing information.

1.3.2 NetPerformer to SIP Proxy Server Connection

In a more complex network, a SIP proxy-compliant IP device (SIP proxy server) is used. The NetPerformer units are User Agent Clients (UACs) in this application, initiating requests to the proxy server.

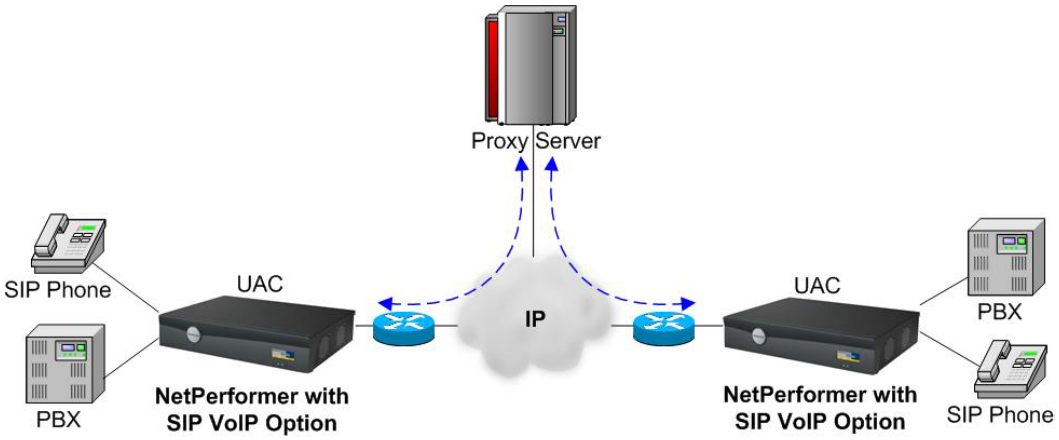

Figure 1-2: NetPerformer Connection to SIP Proxy Server

- The SIP proxy server handles call detail records, dialing rules and other management and accounting functions. It offloads the calling table functions from the NetPerformer.
- This application is generally used for a carrier network or wherever detailed billing information is required.

1.3.3 Multipoint SIP Units without SIP Proxy Server

A network of NetPerformer SIP VoIP units can be interconnected in a multipoint application without requiring a SIP proxy server.

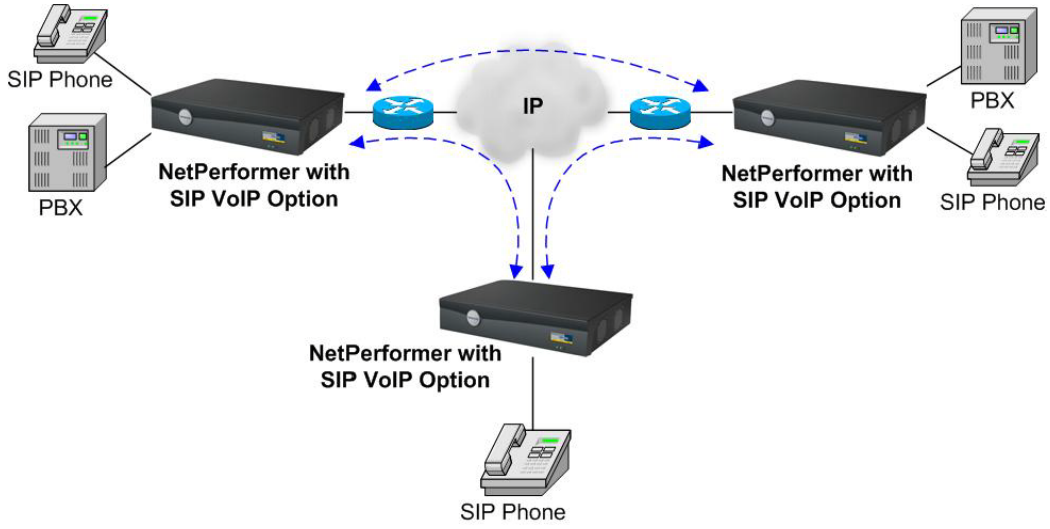

Figure 1-3: Interconnecting a network of NetPerformer SIP VoIP units

- This application uses MAP entries of the type **DIALIP**. Turn to DIALIP Map Type on page 12 for configuration details.
- The IP address configured in the MAP entry overrides the NetPerformer *Proxy server address*.

1.3.4 NetPerformer VoIP Gateway Product

The NetPerformer VoIP Gateway products: the SDM-9220/9220GW and SDM-9230/9230GW, provide economical VoIP gateway functionality in an IP-based network:

- Deliver circuit-switched telephony connectivity to a packet-based network using Ethernet for physical connectivity (IP protocol). The circuit-switched telephony may be:
  - Public: provided by a carrier (PSTN), or
  - Private: using PBX and key system connectivity.
- Primarily used for:
  - Digital telephony interfaces, but can be extended to analog as well. The SDM-9230/9230GW supports up to 60/72 voice channels on T1/E1 (requires high-density DSP). The SDM-9220/9220GW supports up to 30 channels (with DSP-160 SIMM module)
  - SIP User Agent (UA) functions, interoperating with other UAs, Back-to-Back User Agents (B2BUA), SIP Proxy Servers, Registration Server and Session Border Controller.

  - Provides gateway functionality, but can also be used as an endpoint by configuring the extended parameter **EP SIP USERAGENTTYPE** to **ENDPOINT** (refer to Configuring the UA as a Gateway or Endpoint on page 19).

- Hardware derived from SDM-9220/9230 hardware:
  - One Ethernet port serves as the user LAN port connecting to customer equipment
  - The other Ethernet port serves as a WAN port connecting to network equipment. It can also be used to cascade multiple NetPerformer units.
- Uses the NetPerformer base unit software with the following data features removed:
  - Legacy data support, including HDLC, HDLCOFR, T-ASYNC, R-ASYNC, PASSTHRU, COP, BSC, X.25 and SNA over SDLC, LLC or Frame Relay links
  - PowerCell over leased lines, Frame Relay and ATM
  - WAN protocol support on serial or digital interfaces (T1, E1, ISDN-BRI S/T), including FR-USER, FR-NET, PVCR, SDLC, HDLC, PPP, PASSTHRUOFR and Transparent 56/64K or Nx64K
  - Bridging of WAN connections
- Reduced support of routing functions. **The following routing functions are supported:**
  - Transport of IP traffic on both Ethernet ports
  - IP routing (RIP or OSPF)
  - PPPoE, to permit a DSL type of connection
  - PowerCell over IP, including using the NetPerformer VoIP Gateway in PowerCell voice mode rather than SIP, and data compression over PVCRoIP
  - IP addresses for the Ethernet ports and PPPoE connections
  - FTP and Telnet access and control (authorization of incoming connection requests)
  - NAT/PAT and NAT with SIP
  - PPP (including PPP dial backup) and RFC1490 on serial and digital ports, including ISDN-BRI/PRI ports and ports on the dual serial interface card.
  - **Not supported:** IPX routing, IP forwarding using PowerCell over IP.
- Software licensing for VoIP Gateway products:
  - Both VoIP Gateway products run in SIP VoIP mode to support SIP voice.
  - The basic Gateway can be upgraded to the full NetPerformer feature set, including data features and PowerCell voice, through installation of the PowerCell licensed software option.

NOTE: When the PowerCell license is installed, the WAN can be PVCR-based while voice transport uses SIP. However, **PowerCell voice cannot coexist with SIP VoIP.** If PowerCell voice is desired, SIP VoIP mode cannot be selected.

- The SkyPerformer and ATM licensed software options are not supported on the VoIP Gateway products.

1.4 SIP Registration

The NetPerformer can register with up to two SIP registration servers (also called *SIP Proxy servers* or *SIP Proxies*) to allow the network to find the current IP address of a called party. SIP registration ensures than an **INVITE** request will always be sent to the right place, even though the IP address of a particular location is reassigned from one session to the next.

- Each of the SIP registration servers is accessed according to the **SIP PROXY** definitions on the local unit. Refer to "Configuring the SIP Proxy Parameters" on page 2-8 for the configuration procedure.

NOTE: When two **SIP PROXY** units are defined, the second can be used in **BACKUP** or **LOAD BALANCING** mode, as defined with the **SIP GLOBAL** *Proxy rule* parameter (see).

- Each SIP-enabled endpoint (or UA) in the network sends a SIP **REGISTER** request to the currently active SIP registration server, with the SIP Universal Resource Locator (URL) of the UA included in the request message.
- If registration is successful, the SIP registration server sends a **200 OK** response back to the UA.
- From the **REGISTER** request, the registration server can determine the IP address of the UA, match it with the SIP URL contained in the request, and store both values in a database.
- An **INVITE** request from a UA is addressed to the SIP URL of the called party.
- When the SIP proxy server receives the **INVITE**, it accesses the database and retrieves the correct IP address of the UA that handles the called party.

Up to two registrations are permitted for each NetPerformer in the network:

- Enable registration with the **SIP PROXY** *Enable Registration* parameter (see Configuring the SIP Proxy Parameters on page 8)
- Set the *REGISTER expires (s)* parameter to the maximum amount of time, in seconds, that the registration can last (see Configuring the SIP Timer Parameters on page 6). By default this is 20 seconds.
- Another SIP registration is carried out once the *REGISTER expires (s)* timeout is reached.

NOTE: If two SIP proxies are defined in **LOAD BALANCING** mode, registration alternates from one proxy to the other after each *REGISTER expires (s)*.

1.5 SIP Call Authentication and Accounting

Call authentication and accounting are used together in a SIP prepaid telephone calling card scenario. In a calling card or prepaid application, the customer pays in advance for telephony services. The customer usually buys a card that represents a certain amount of usage time (in minutes or seconds).

The NetPerformer supports three types of call authentication:

- Remote Authentication Dial In User Service (RADIUS) for calls through a RADIUS server (see next section)
- SIP Challenge authentication for User-to-User calls (see "SIP Challenge Call Authentication" on page 1-12)
- Proxy server authentication for Proxy-to-User calls (see "Proxy Server Call Authentication" on page 1-12).

1.5.1 RADIUS Authentication and Accounting

The Remote Authentication Dial In User Service (RADIUS) server application was originally designed to allow centralization of user information for dialup remote access. Due to its flexibility and platform independence, RADIUS is used for a wide number of applications:

- VoIP call authentication
- Call accounting (in tandem with a Billing server that manages the accounting information database).

Call Authentication

NOTE: RADIUS call authentication is available on all NetPerformer products that support the SIP VoIP voice transport method, and is configured using **SIP AUTHENTICATION** parameters (see "Configuring the SIP Authentication Parameters" on page 2-7). The *Authentication type* parameter must be set to **RADIUS EGRESS**.

Each time a prepaid calling card is used, the customer must enter the correct Personal Identification Number (PIN), a series of digits which allows the RADIUS server to validate the usage of the card.

- The remote system seizes the destination number, the calling card number and the PIN
- The calling card number associates the user to a specific account
- The PIN validates that the user is the actual owner of this account

If the supplied credentials match what is stored on the RADIUS server, the server sends an

Access Accept response to the NetPerformer, which lets the call go through to the requested destination number.

If the RADIUS server is unable to authenticate the user with the given PIN, it sends an **Access Reject** response to the NetPerformer, which rejects the call with the error **401 Unauthorized**.

Call Accounting

NOTE: SIP call accounting is available on the SDM-9220, SDM-9230, SDM-9220/9220GW and SDM-9230/9230GW only, and is configured using the **SIP GLOBAL** *Call accounting* parameter (see).

When the use of a calling card has passed the authentication process. the RADIUS server includes the following information in the **Access Accept** response:

- Proprietary attributes using the Cisco® vendor ID (0x09) and vendor-specific attributes (VSA), which are already supported on most RADIUS servers.
- The number of seconds available on the user's account. If this value is 0, the call will not be placed. Instead, the call is rejected with the error **402 Payment Required**.

NOTE: Accounting information can be sent to the RADIUS server without knowing the user's password. Thus accounting can be implemented for both egress and ingress calls on the NetPerformer. Refer also to Ingress and Egress Dial Rule Definitions on page 16.

The NetPerformer sends two types of accounting packets to the RADIUS server:

- **Accounting Start:** Sent after the NetPerformer receives confirmation from the SIP UA that it has received the **200 OK** message when call setup is complete. This packet indicates the start time for calculating the call duration.
- **Accounting Stop:** Sent after the NetPerformer receives a **BYE** message from the SIP UA, indicating that the call has been disconnected. This packet indicates both the end time and the total call duration.

NOTE: The NetPerformer calculates the time difference between **Accounting Start** and **Accounting Stop**, and adjusts the result to the exact duration of the call without any interference from network delay.

The RADIUS server then forwards the accounting information to the Billing server for

update of the user's account.

Example Application

RADIUS call authentication and call accounting are used in the example application shown in Figure 1-1, which provides an inexpensive means of offering international telephone service to PC users over the Internet.

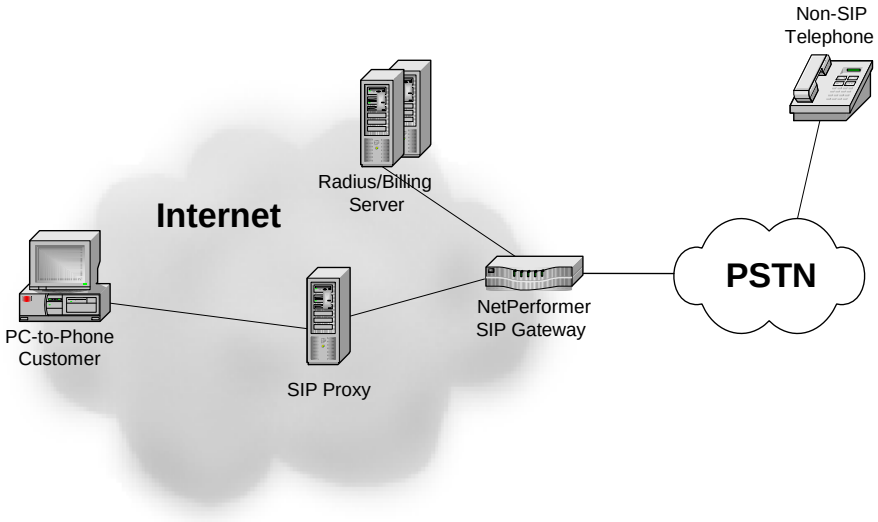

Table 1-1: RADIUS Call Authentication and Accounting in a Prepaid PC-to-Phone Application

In this application, the customer buys a calling card and installs a SIP user agent software via the Internet. The software is configured with the address of the SIP proxy server, so that all calls are automatically forwarded to this server.

- Calls are placed from the PC soft phone through the SIP proxy to the NetPerformer SIP gateway, which egresses the call to the PSTN
- When the NetPerformer receives the call, it seizes the caller's user ID and password, and requests the RADIUS server to validate that the user is authorized to place a call
- The NetPerformer also gets the account balance (the remaining number of seconds available for a call) from the Billing server via the RADIUS server in response to the access request
- Once the call is established, the NetPerformer gateway monitors the call duration, and terminates the call if it extends past the number of seconds available in the user account
- To update the user's calling card account, the NetPerformer sends an accounting request to the RADIUS server, which reports the call duration.
- The RADIUS server forwards the accounting information to the Billing server.

1.5.2 SIP Challenge Call Authentication

NOTE: SIP Challenge call authentication is available on all NetPerformer products running V10.3.1 or higher, and is configured using **SIP AUTHENTICATION** parameters (see "Configuring the SIP Authentication Parameters" on page 2-7). The *Authentication type* parameter must be set to **SIP CHALLENGE**.

SIP Challenge authentication is used for user-to-user call setup when the call request does not include authentication parameters in its *Authorization* header. When the UAS receives this request from the UAC, the UAS can authenticate the originator of the call before processing the request.

- The UAS challenges the UAC to provide the proper username and password. This challenge is sent with a **401 (Unauthorized)** response.
- When the UAC receives the **401 (Unauthorized)**, it repeats the original call request and provides the proper credentials, if possible. The username and password may be entered directly by the user, or discovered internally.

  Caution: On the NetPerformer, the *Challenge username* and *Challenge password* parameters are used as credentials in a SIP Challenge scenario. **Since only one *Challenge username* and *Challenge password* can be configured, all users in the network must share the same *Challenge username* and *Challenge password* to allow user-to-user authentication.**
- If the proper credentials cannot be located, the UAC will retry the request with an anonymous username and no password.
- Once the username and password have been supplied and accepted, the UAC can include them in the *Authorization* header field of subsequent requests to the same Call-ID without requiring another SIP challenge.

1.5.3 Proxy Server Call Authentication

NOTE: Proxy server call authentication is available on all NetPerformer products running V10.3.1 or higher, and is configured using **SIP PROXY** parameters (see "Configuring the SIP Proxy Parameters" on page 2-8).

SIP Challenge authentication is used for proxy-to-user call setup when the call request does not include authentication parameters in its *Proxy-Authorization* header. When the proxy server receives this request from the UAC, the proxy server can authenticate the originator of the call before processing the request.

- The proxy server challenges the UAC to provide the proper username and password. This challenge is sent with a **407 (Proxy Authentication Required)** response.
- When the UAC receives the **407 (Proxy Authentication Required)**, it repeats the original call request and provides the proper credentials, if possible.

NOTE: On the NetPerformer, the *Proxy authentication username* and *Proxy authentication password* parameters are used as credentials for proxy-to-user authentication.

- If the proper credentials cannot be located, the UAC will retry the request with an anonymous username and no password.
- Once the username and password have been supplied and accepted, the UAC can include them in the *Proxy-Authorization* header field of subsequent requests to the same **Call-ID** without requiring another proxy challenge.
- If a UA wants to authenticate itself, it can include its credentials with the original call request to identify itself to a proxy that requires authentication.
- A forking proxy may forward a request to more than one proxy server that requires authentication. These proxy servers will not forward the request until the originating UAC has authenticated itself in their respective realm.
- If a request is forked, more than one proxy server may wish to challenge the UAC. The forking proxy server comgines all challenges into a single response.

1.6 Other SIP Features Supported

1.6.1 Enhanced Fax Support

The NetPerformer with SIP supports the following enhanced fax functions:

- T.38 offered in the Session Description Protocol (SDP) message during the **re-INVITE**, for establishment of a T.38 fax session
- T.38 fax negotiation, which is handled during SIP codec negotiation
- The ability to switch to Modem Passthru if, after fax negotiation, the remote side indicates that it cannot support T.38
- Super G3 fax using a T.38 Fax Relay connection, which requires less bandwidth than Modem Passthru using G.711.

NOTE: With the **T.38_SG3** *Fax relay* setting, the NetPerformer forces a fallback to the G3 standard (at 14.4 Kbps) when it detects a Super G3 answering tone.

For further information, refer to the following:

- The chapter Codec Negotiation on page 1 of this document
- Details on voice channel configuration and Modem Passthru are provided in the *Digital Voice* fascicle of this document series
- The *Fax relay* parameter is detailed in the appendix *SE/SLOT/#/CHANNEL Configuration Parameters* of the *Analog Voice* fascicle.

1.6.2 Clearmode

The NetPerformer with SIP supports the *Clearmode* data streaming function, following RFC-2736. This mode is also referred to as *clear-channel data* or *64 Kbit/s unrestricted*.

- Provides transparent relay of 64 Kbit/s data streams in Real-time Transport Protocol (RTP) packets.
- No data processing is performed other than packetization and depacketization
- No encoder/decoder is required
- A unique RTP payload type is required
- The related MIME type must be registered for signaling purposes.

Clearmode can be used by any application that does not need encoding/decoding for transfer via an RTP connection. An example is where ISDN data terminals produce data streams which are not compatible with the non-linear encoding used for voice.

1.6.3 CLIR

The NetPerformer with SIP supports Calling Line Identification Restriction (CLIR), which allows a caller to disable the display of personal identification on the remote site telephone. On the NetPerformer, this feature applies to calls that ingress via PCM (ISDN-PRI) and egress through SIP.

CLIR is a configurable feature, set with the *Caller Line Identity Restriction* parameter in the **SIP/GLOBAL** submenu of the **SETUP** command.

By default, the NetPerformer uses the *P-Assert* setting (**P-Asserted-Identity**) in the ISDN/QSIG **SETUP** message. If a call is restricted, the *P-Assert* is set to private status (**Privacy: id**), and this value is forwarded with the call. You can force all calls to private status by changing the default setting of the *Caller Line Identity Restriction* parameter to **ALWAYS**.

1.6.4 ptime Attribute

The NetPerformer with SIP supports the **ptime** attribute to handle the rate at which a voice codec will send packets, or *packets per frame* (PPF).

The NetPerformer sets the **ptime** attribute to the rate configured on the voice channel, and sends it with an **INVITE** message. The **ptime** is then negotiated between UACs.

NOTE: If a unit switches from a G7xx voice algorithm to G723, it forces the rate to 5.3 Kbps.

You can view the current PPF from the NetPerformer console using the Display Channel States (**DCS**) command. The **DCS** command reflects the PPF according to the negotiated **ptime**.

1.6.5 Out-of-band Digit Transport

The NetPerformer with SIP supports out-of-band digit transport using a DTMF Relay method that relies on the SIP **INFO** message. This custom **INFO** method handles telephone keypad digits that are used in some countries for special functions, such as **#**, **A**, **B**, **C**, **D**, and **10**.

The *DTMF in SIP INFO packets* parameter permits sending the *DTMF payload* in the SIP **INFO** packets. This parameter should be set to **ALWAYS** for out-of-band digit transport. For details, refer to DTMF in SIP INFO packets on page 5.

1.6.6 Private Extensions

The NetPerformer supports private extensions in SIP, following the RFC-3325 standard. SIP private extensions are used to identify end users or end systems, and transport end-user privacy requests.

1.6.7 ISUP to SIP Mapping

The NetPerformer supports ISUP to SIP mapping, following the RFC-3398 standard. This allows ISDN cause codes to be mapped to SIP cause codes, and vice versa.

1.6.8 Reason Header

The NetPerformer with SIP follows the RFC-3326 standard concerning the addition of a *Reason* header in the SIP **CANCEL** and **BYE** methods.

1.7 Other Components of the NetPerformer SIP VoIP Network

Memotec products are based on a distributed, client/server hardware and software architecture that supports fault tolerance and a high level of system availability. They are designed to meet the needs of telecommunications carriers, Internet service providers and private enterprises.

In addition to NetPerformer SIP VoIP support, the Clarent Softswitch solution can include the following components:

- Clarent Command Center (required)
- A third-party ODBC compliant database (required)
- Clarent BHG series gateways
- Clarent Connect
- Clarent C4CM or C5CM Call Manager

The illustration below shows the elements in a typical Clarent Softswitch solution.

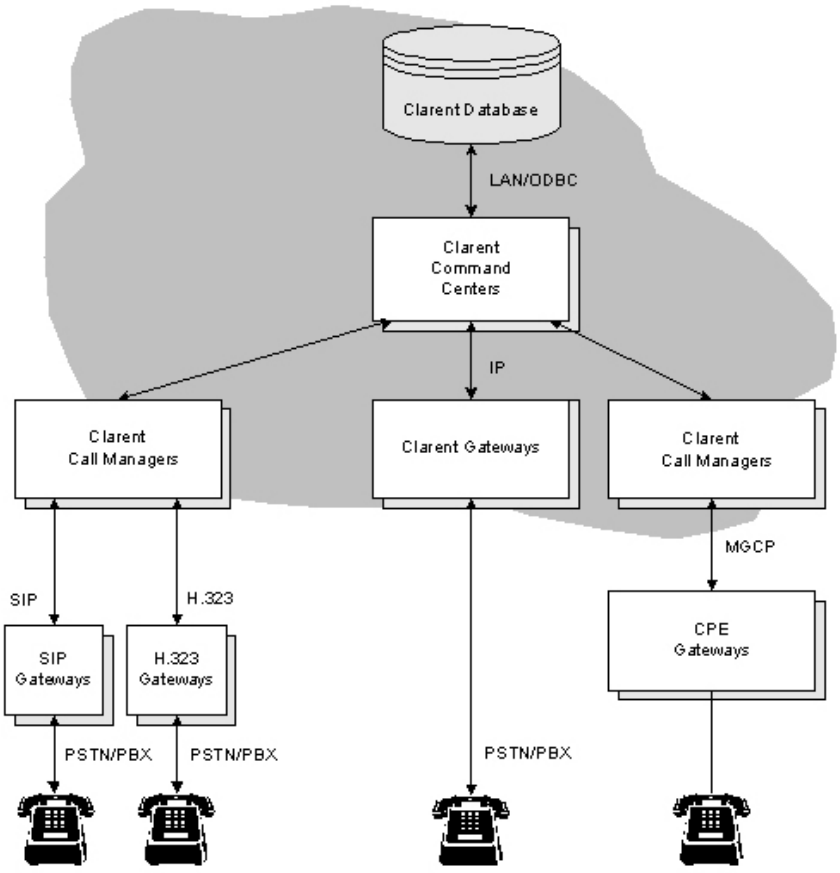

Figure 1-4: Elements of the Clarent Softswitch Network

All elements of the Clarent Softswitch network are designed to use SNMP, a protocol for managing TCP/IP-based networks. SNMP defines how network information, such as configuration parameters, is retrieved from Management Information Bases (MIBs) and updated according to user actions and current network status. The Memotec MIB includes variables and traps that are specific to Memotec products.

NOTE: All MIB variables that are used to define SIP characteristics on the NetPerformer are listed in the appendices to this document.

The setup of this network involves the following steps:

- Create the Clarent database using a third-party ODBC compliant database. See the *Clarent Database Administration Guide* for requirements.
- Set up, configure and start both primary and secondary Command Centers, referring to the *Clarent Command Center User Guide*.
- Set up, configure and start the Call Managers and any supported H.323, SIP or CPE gateways and clients. For more information, see *Clarent Call Manager User Guide* and *Clarent Gateway User Guide*.

Once started, a gateway or Call Manager automatically attempts to connect to its primary Command Center.

1.7.1 Clarent Command Center and Database

Clarent Command Center works in conjunction with a central, ODBC-compliant database to provide intelligence to Memotec telephony networks. The Command Center provides detailed call records for billing, dynamic call routing, flexible call rating as well as network management and administration for Memotec networks.

Call routing and rating information, subscriber account data, dial rules and call detail records all reside in the ODBC-compliant database that Clarent Command Center accesses.

NOTE: Memotec supports several database architectures, including replicated databases.

Command Center uses information in the database to:

- Authenticate callers, gateways, gatekeepers and Call Managers
- Provide call routes, dial rules and call rates
- Collect call detail information
- Track Gateway and Call Manager status and statistics
- Maintain system information

- Monitor network performance.

For more information, see *Clarent Command Center User Guide* and *Clarent Database Administration Guide*.

1.7.2 Clarent Gateway

Clarent Gateways are complete, turnkey hardware and software solutions that integrate a PSTN or PBX with the Internet or IP network, providing clear and reliable Internet telephony. Memotec pre-installs and factory-configures the gateway software according to your specific telephony requirements.

In addition to controlling voice, fax and data communications, Clarent Gateway performs the following functions:

- Processes incoming calls
- Prompts for and records outgoing call information
- Completes the connection to the destination (egress) gateway
- Keeps detailed records of each call.

For more information, see *Clarent Gateway User Guide*.

1.7.3 Clarent Connect

Clarent Connect enables service providers to join Memotec networks with partner providers for wider coverage and more efficient call routing. By linking multiple, independent networks into a single virtual network, Clarent Connect gives customers access to IP telephony services around the globe.

Clarent Connect also allows a service provider to operate as a clearinghouse for multiple, independent networks. With this implementation of Clarent Connect, an independent service provider need only establish a partnership with the clearinghouse to have access to IP telephony services around the world.

For more information, see *Clarent Connect User Guide*.

1.7.4 Clarent Call Manager

Clarent Call Manager allows you to integrate H.323 V2-compliant gateways and SIP gateways from various vendors into a single network. It provides access control and address translation for H.323 V2 gateways and SIP gateways, and performs call control functions for all the gateways in a mixed network.

Clarent Call Manager also allows you to integrate media gateways, or Customer Premises Equipment (CPE), from multiple vendors into the Memotec network. Call Manager controls CPE gateways using the Media Gateway Control Protocol (MGCP V1.0).

CPE gateways perform voice encoding and packetizing, providing analog FXS interfaces to the Memotec network. The analog interfaces, referred to as endpoints, can connect to conventional telephones, fax machines and modems to carry voice, pass-through fax and voice-band data traffic. CPE gateways connect to the Memotec network through any

10BaseT WAN connection, such as through ADSL (Asymmetric Digital Subscriber Line) modems or cable modems.

Clarent Call Manager gives H.323, SIP and CPE gateways access to Memotec's dynamic call routing, flexible call rating, billing information and other Memotec advanced features. It also allows Clarent Gateways to terminate calls to and from H.323, SIP and CPE gateways, and provides secure, transparent authentication of the endpoint when a call is made.

For more information, see *Clarent Call Manager User Guide*.

1.8 Network Management Components of the Clarent Softswitch Solution

Memotec provides a variety of products and services that enable you to efficiently manage your Clarent Softswitch solution. These products include:

- Clarent Application Server
- Clarent Distribution Manager and Package Distributor
- Clarent Domain Controller
- Clarent Network View
- Clarent Assist.

1.8.1 Clarent Application Server

Clarent Application Server provides a common framework for:

- Initiating remote software downloads and configuration changes
- Allowing multiple administrators simultaneous access to network applications
- Providing distributed and secure access to network data.

For more information, see *Clarent Application Server User Guide*.

1.8.2 Clarent Distribution Manager and Package Distributor

Clarent Distribution Manager is a Windows NT service that can reside on each Memotec network element running Windows NT. Clarent Distribution Manager's job is to receive software and configuration update requests from Clarent Package Distributor, download packages using Hypertext Transfer Protocol (HTTP) and report the real-time status of all operations to the network management system through SNMP traps.

You must install Clarent Distribution Manager on all Windows NT Memotec network elements to which you want to distribute packages. For more information, see *Clarent Package Distributor User Guide*.

1.8.3 Clarent Domain Controller

Clarent Domain Controller allows you to distribute the management of your Memotec network into smaller segments called domains. This is particularly helpful for large service providers who want to segment their networks for use by smaller service providers or enterprises.

With Domain Controller, domain administrators can securely access and update the Memotec database over an IP network. For more information, see *Clarent Domain Controller User Guide* and *Clarent Domain Controller Administration Guide*.

1.8.4 Clarent Network View

Clarent Network View is a Java applet that enables you to capture snapshots of the status of Memotec network elements. With Clarent Network View, you can create a *view* that consists of the IP addresses of selected Memotec network elements. You can then display this *view* to capture the status of these network elements.

You associate each *view* with a *view type*. A *view type* determines what information is gathered from the MIB(s) of a network element. You can use default *view types* or customize your own.

For more information, see *Clarent Network View User Guide*.

1.8.5 Clarent Assist

Clarent Assist is a Java applet that enables you to view, add, modify, delete and print information in the Memotec database. You can use Clarent Assist to quickly and easily navigate from one section of the database to another. You can view all the information in a given section, or you can set various filters to restrict what information is presented.

Using the Clarent Assist HTML generator, you can set up a unique login ID and password for each user or group of users that need access to the Memotec database. You can also use the HTML generator to limit the areas each user or group of users has access to.

For more information, see *Clarent Assist User Guide*.

Configuring SIP VoIP

2.1 Selecting SIP VoIP Mode

As of NetPerformer V10.2.3 R02, SIP VoIP support is offered with the base product software rather than as a licensed software option. **SIP VoIP mode must be activated on the NetPerformer unit before you can configure and use any SIP VoIP features.**

To select SIP VoIP mode from the NetPerformer console, change the value of the global *Voice transport method* parameter to **SIP VOIP**:

1. At the NetPerformer command line prompt, enter the menu sequence: **SE** ↵ **GLOBAL**
2. Enter carriage returns until you reach the *Voice transport method* parameter
3. Enter **SIP VOIP**.

```
9230-1>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/PHONE/
PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/SS7/USER/VLAN,
def:BRIDGE) ? GLOBAL
GLOBAL> Unit name (def:9230-1) ?
GLOBAL> Unit routing version (1-2,def:1) ?
...
...
GLOBAL> Exclusive access to console (def:DISABLE) ?
GLOBAL> Voice transport method (def:POWERCELL) ? SIP VOIP
```

If you are using SNMP, set the *npsysVoiceTransportMethod* variable to **sipVoIP**.

2.1.1 Effects of Selecting SIP VoIP Mode

The NetPerformer is equipped with a single binary code which handles either Voice over PowerCell or Voice over IP using SIP (SIP VoIP) applications. **A single NetPerformer unit cannot run Voice over PowerCell and SIP VoIP simultaneously.**

By default, the Voice over PowerCell application is resident on each NetPerformer unit as it leaves the factory. If you change the *Voice transport method* to **SIP VOIP**:

- When the unit boots up, the main application forces the SIP VoIP mode of operation.
- On all voice channels previously configured for Voice over PowerCell, the *Protocol* is forced to **OFF**.
- If this is the first reboot since selecting SIP VoIP mode, **all MAP entries are deleted from the MAP file**. PowerCell MAP entries are *not* automatically converted to SIP MAP entries.

NOTE: The same is true if you switch from SIP VoIP mode to PowerCell mode on the NetPerformer. **The MAP file will be emptied, since SIP MAP entries cannot be converted to PowerCell MAP entries.**

2.2 Defining SIP Characteristics on the NetPerformer

The following sections describe configuration procedures for the various SIP characteristics on the NetPerformer:

- Enable SIP operations and configure the global SIP properties (**SE/SIP/GLOBAL**, see next section)
- Define the SIP Timers (**SE/SIP/TIMER**, "Configuring the SIP Timer Parameters" on page 2-6)
- Define the SIP Authentication parameters (**SE/SIP/AUTHENTICATION**, "Configuring the SIP Authentication Parameters" on page 2-7)
- Define the SIP Proxy parameters for the SIP registration process (**SE/SIP/PROXY**, "Configuring the SIP Proxy Parameters" on page 2-8)
- Build a Voice Mapping Table (**SE/MAP**, "Setting up the Voice Mapping Table" on page 2-10)
- Configure the UA as a gateway or endpoint (**EP SIP USERAGENTTYPES**, "Configuring the UA as a Gateway or Endpoint" on page 2-19)

NOTE: To fully configure the voice channels that carry the SIP requests and responses, consult the *Analog Voice* and *Digital Voice* fascicles of this document series.

Configuration of related SIP applications is addressed in separate chapters:

- To configure the NetPerformer as a *SIP Redirect Server*, go to SIP Redirect Server on page 1
- To configure the Codec Negotiation parameters, refer to the chapter Codec Negotiation on page 1
- To configure a *SIP Hairpin* application that permits local calls, turn to SIP Hairpin on page 1
- Special considerations concerning Modem Passthru with SIP are included with the discussion of *Modem Passthru* in the *Digital Voice* fascicle of this document series.

2.3 Enable SIP and Configure the Global SIP Properties

The *SIP Global* parameters control various aspects of the NetPerformer configuration that affect all SIP sessions.

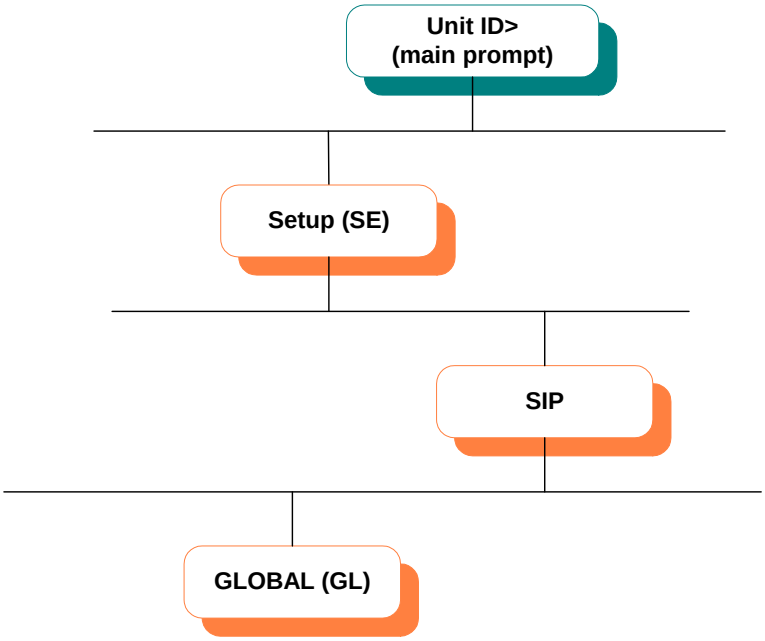

Figure 2-1: SETUP/SIP/GLOBAL Path in the CLI Tree

To enable SIP operations and define global SIP properties on the unit:

1. At the NetPerformer command line prompt, enter the menu sequence: **SE** ↵ **SIP** ↵ **GLOBAL**.

   As an alternative, you can enter the sequence: **SE** ↵ **SIP** ↵ **ALL** to access all SIP parameters at once.

2. Set the *Administrative status* to **ENABLE** to enable SIP functions.

   If SIP is disabled, you can configure the remaining SIP Global parameters, but their new values will not take effect.

3. Change the other SIP Global parameters from their default values, if desired.

SE/SIP/ GLOBAL example

```
9360-2>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/PHONE/
PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/SVC/USER/VLAN,
def:BRIDGE) ? SIP
SIP> (GLOBAL/TIMER/RETRIES/DIGEST/CODEC NEGO/ALL,def:ALL) ? GLOBAL
SIP Global> Administrative status (def:ENABLE) ?
SIP Global> Proxy server address (def:0.0.0.0) ? 10.3.1.21
SIP Global> UDP Port (1-65535,def:5060) ?
SIP Global> Gateway ID (0-999999999,def:0) ?
SIP Global> Server group (def:) ?
SIP Global> Registration (def:DISABLE) ?
SIP Global> ANI digits (def:) ?
SIP Global> DTMF Payload (96-127,def:104) ?
SIP Global> DTMF in SIP INFO packets (def:COMPATIBLE) ?
SIP Global> Redirect Server (def:DISABLE) ?
SIP Global> Call Accounting (def:NONE) ? RADIUS EGRESS
SIP Global> Call Authentication (def:NONE) ? RADIUS EGRESS
SIP Global> PIN Length (0-255,def:0) ? 10
SIP Global> Caller Line Identity Restriction (def:NORMAL) ?
```

These parameters are detailed in the appendix SE/SIP Configuration Parameters on page 1.

2.4 Configuring the SIP Timer Parameters

The *SIP Timer* parameters can be used to fine tune SIP **Request** retransmissions, thereby controlling the resource allocation during a SIP session. The NetPerformer mechanism for SIP Request Restransmission is RFC-3261 compliant, based on State-full transactions and triggered by the expiration of the various timers involved.

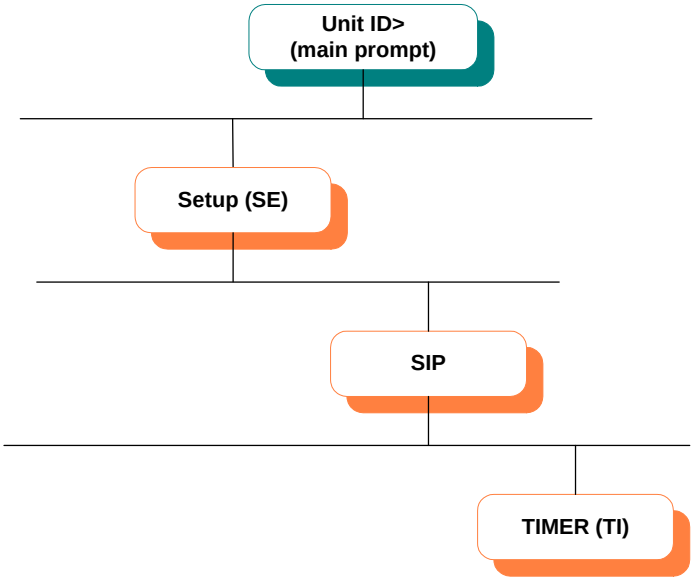

Figure 2-2: SETUP/SIP/TIMER Path in the CLI Tree

To define the SIP Timers:

1. At the NetPerformer command line prompt, enter the menu sequence: **SE** ↵ **SIP** ↵ **TIMER**.

   As an alternative, you can enter **SE** ↵ **SIP** ↵ **ALL** to access all SIP parameters at once.

2. Change the SIP Timer parameters from their default values, if desired.

   All timers are measured in milliseconds.

SE/SIP/TIMER example

```
9360-2>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/PHONE/
PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/SVC/USER/VLAN,
def:BRIDGE) ? SIP
SIP> (GLOBAL/TIMER/RETRIES/DIGEST/CODEC NEGO/ALL,def:GLOBAL) ? TIMER
SIP Timer> Resend INVITE (1-1000,def:5) ?
SIP Timer> Receiving ACK (1-1000,def:5) ?
SIP Timer> Disconnect (BYE or CANCEL) (1-1000,def:5) ?
SIP Timer> Registration duration (1-100000000,def:20) ?
```

The SIP Timer parameters are detailed in the section TIMER Parameters on page 9.

2.5 Configuring the SIP Authentication Parameters

The NetPerformer SIP Authentication definitions are used for authentication exchanges between the user agent (UA) and the server. The credentials you define will be included in the Authorization header in requests to the server.

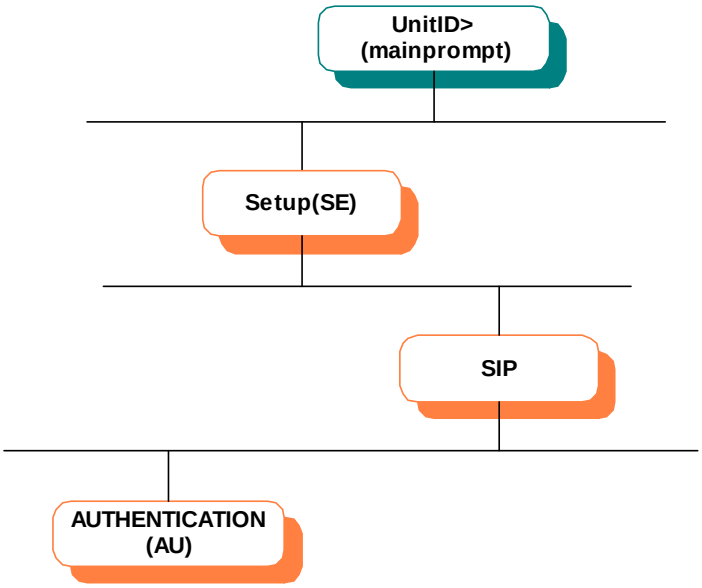

Figure 2-3: SETUP/SIP/AUTHENTICATION Path in the CLI Tree

To define the SIP Authentication parameters:

1. At the NetPerformer command line prompt, enter the menu sequence: **SE** ↵ **SIP** ↵ **AUTHENTICATION**.

> **NOTE:** As an alternative, you can enter the sequence: **SE** ↵ **SIP** ↵ **ALL** to access all SIP parameters at once.

2. Enter the authentication criteria for this NetPerformer unit after the SIP Authentication parameter prompts.

SE/SIP/AUTHENTICATION example

```
9360-2>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/PHONE/
PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/SVC/USER/VLAN,
def:BRIDGE) ? SIP
SIP> (GLOBAL/TIMER/RETRIES/DIGEST/CODEC NEGO/ALL,def:GLOBAL) ? DIGEST
SIP Digest> UserName (def:) ?
SIP Digest> UserPassword (def:) ?
```

2.6 Configuring the SIP Proxy Parameters

The SIP Proxy parameters are used to enable SIP Registration, define up to two SIP Registration servers, and configure the credentials for Proxy-to-user authentication (refer to “Proxy Server Call Authentication” on page 1-12).

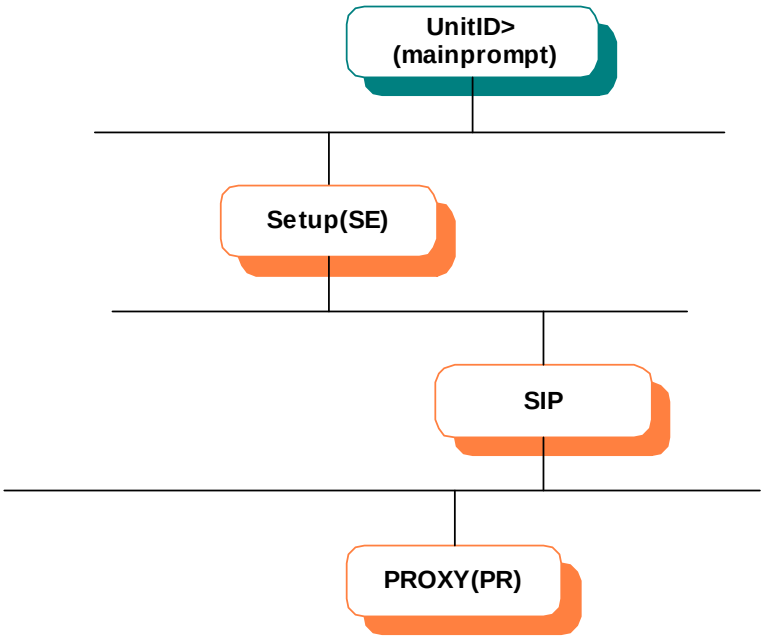

Figure 2-4: SETUP/SIP/PROXY Path in the CLI Tree

To define the SIP Proxy parameters:

1. At the NetPerformer command line prompt, enter the menu sequence: **SE** ↵ **SIP** ↵ **PROXY**.

   As an alternative, you can enter the sequence: **SE** ↵ **SIP** ↵ **ALL** to access all SIP parameters at once.

2. Enter the *SIP Proxy entry number*.

   If you define 2 SIP Proxies, the second can be defined as a **BACKUP** unit or used as an alternate in **LOAD BALANCING** mode, as defined by the **SIP GLOBAL** *Proxy rule* parameter (see)

3. To enable SIP Registration on this SIP Proxy, enter **YES** at the *Enable registration* prompt

4. Enter the required definitions for this SIP Proxy after the SIP Proxy parameter prompts.

SE/SIP/PROXY example

```
9360-2>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/PHONE/
PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/SVC/USER/VLAN,
def:BRIDGE) ? SIP
...
```

These parameters are detailed in the section

2.7 Setting up the Voice Mapping Table

The Voice Mapping Table (**MAP**) includes definitions of all dial numbers used for call setup on a voice channel. Up to 3000 MAP entries can be defined. The called location can be referenced using:

- A dial string via the SIP proxy server (**DIALSTRING** *Map type*, see "DIAL-STRING Map Type" on page 2-11), ***or***
- A dial string using a specific IP address (**DIALIP** *Map type*, see "DIALIP Map Type" on page 2-12), ***or***
- All configured dial strings, by searching all locations that can be reached on the specified hunt group ports (**SUPERMAP** *Map type*, see "SUPERMAP Map Type" on page 2-13).

You can add, modify or delete a MAP entry using the **MAP** submenu of the NetPerformer **SETUP** command.

NOTE: The MAP entries cannot be defined using SNMP.

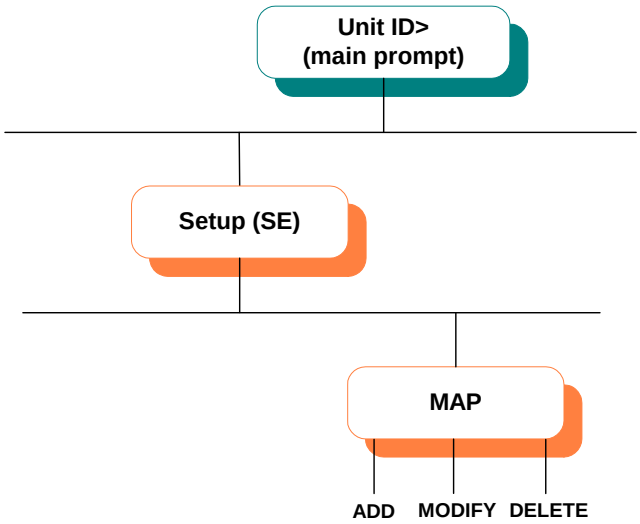

Figure 2-5: SETUP/MAP Path in the CLI Tree

2.7.1 Adding a MAP Entry

To define a new MAP entry for a voice channel:

1. Enter the menu sequence: **SE** ↵ **MAP**.
2. Set the *Operation* to **ADD**.
3. Select the *Map type*:
   - **DIALSTRING** (see next section)
   - **DIALIP** (see "DIALIP Map Type" on page 2-12)
   - **SUPERMAP** (see "SUPERMAP Map Type" on page 2-13).
4. For the **DIALSTRING** and **DIALIP** *Map types*, you must enter the *Entry digits* string.

NOTE: The same *Entry digits* can be used for several MAP entries to create what is called "overloaded" MAP entries. For an example using SIP Hairpin, refer to Using Overloaded MAP Entries on page 7.

5. For the **DIALIP** Map type, the *Enter an IP address* parameter must be defined.
6. Change the other **MAP** parameters from their default values, if desired.

NOTE: Values for the *Strip prefix number of digits*, *Ingress/Egress prepend string* and *Ingress/Egress append string* parameters must be identified with **I** for ingress and/or **E** for egress. Refer to Ingress and Egress Dial Rule Definitions on page 16.

2.7.2 DIALSTRING Map Type

The **DIALSTRING** *Map type* uses, for ingress calls, the *Proxy server address* specified in the SIP global parameters (refer to Enable SIP and Configure the Global SIP Properties on page 4). Egress calls are routed to the destination voice hunt ports defined in the MAP entry with the *Egress hunt group ports* parameter. Refer to Figure 2-6:, Ingress and Egress Calls, on page 17.

To add a MAP entry with the DIALSTRING *Map type*:

1. Set the *Map type* to **DIALSTRING**
2. Define a unique *Entry digits* string
3. Set the *Digits string length*
4. Change the other **MAP** parameters from their default values, if desired.

NOTE: You can define a single **DIALSTRING** MAP entry with a range of digits to access several locations at another site.

Define one or more **DIALSTRING** entries with wildcard characters (*) in the *Entry digits* string.

For example, the *Entry digits* **2**** represent all numbers from **200** to **299** for call setup purposes.

SE/MAP example: with DIALSTRING Map type

```
BOSTON>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/PHONE/
PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/USER/VLAN,
def:BRIDGE) ? SIP
Define speed dial numbers for voice mapping table
MAP> Operation (ADD/MODIFY/DELETE,def:ADD) ? ADD
MAP> Map type (DIALSTRING/DIALIP/SUPERMAP,def:DIALSTRING) ?
DIALSTRING
MAP> Entry digits (def:) : 450
MAP> Digits string length, max 30 (def:3) : 10
MAP> Egress hunt group pattern (SEQUENTIAL/ROTARY/NONE,def:NONE) ?
SEQUENTIAL
MAP> Egress hunt group ports (i.e. 101,102,203 or 101,103-106) (def:)
: 201
MAP> Strip prefix number of digits (def:I0 E0) : I2 E3
MAP> Ingress/Egress prepend string (def:) : E604
MAP> Ingress/Egress append string (def:) : I50E9
MAP> Add another map entry (NO/YES,def:NO) ? NO

Saving map entry...
```

For detailed descriptions of these parameters, consult the appendix SE/MAP Configuration Parameters on page 1.

2.7.3 DIALIP Map Type

For the DIALIP *Map type*, ingress calls are routed to the destination IP address defined in the MAP entry. Egress calls are routed to the destination voice hunt ports defined with the *Egress hunt group ports* parameter. Refer to Figure 2-6:, Ingress and Egress Calls, on page 17.

To add a MAP entry with the DIALIP *Map type*:

1. Set the *Map type* to **DIALIP**
2. Define a unique *Entry digits* string
3. Set the *Digits string length*
4. Change the *Enter an IP address* parameter to a non-zero IP address

5. Change the other **MAP** parameters from their default values, if desired.

SE/MAP example: with DIALIP Map type

```
BOSTON>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/PHONE/
PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/USER/VLAN,
def:BRIDGE) ? SIP
Define speed dial numbers for voice mapping table
MAP> Operation (ADD/MODIFY/DELETE,def:ADD) ? ADD
MAP> Map type (DIALSTRING/DIALIP/SUPERMAP,def:DIALSTRING) ? DIALIP
MAP> Entry digits (def:) : 398
MAP> Digits string length, max 30 (def:3) : 5
MAP> Egress hunt group pattern (SEQUENTIAL/ROTARY/NONE,def:NONE) ?
ROTARY
MAP> Egress hunt group ports (i.e. 101,102,203 or 101,103-106) (def:)
: 101-125
MAP> Strip prefix number of digits (def:I0 E0) :
MAP> Ingress/Egress prepend string (def:) :
MAP> Ingress/Egress append string (def:) :
MAP> Enter an IP address (def:000.000.000.000) ? 105.254.0.1
MAP> Add another map entry (NO/YES,def:YES) ? NO

Saving map entry...
```

- The *Operation*, *Map type*, *Entry digits*, *Digits string length*, *Egress hunt group pattern*, *Egress hunt group ports*, *Strip prefix number of digits*, *Ingress/Egress prepend string*, *Ingress/Egress append string* and *Add another map entry* parameters are common to other MAP entry types, and are detailed in the section DIALSTRING Map Type on page 2.
- The *Enter an IP address* parameter is specific to the **DIALIP** Map type. For details, turn to "DIALIP Map Type" on page 8-8.

2.7.4 SUPERMAP Map Type

The **SUPERMAP** *Map type* is composed of a digits string with 30 wildcard characters (all asterisks: *). It acts as a default entry for all VoIP calls, and accepts all digit strings with a minimum of 1 and maximum of 30 characters.

- Only one **SUPERMAP** entry can be defined on each NetPerformer unit.
- It is always the last MAP entry to be processed. That is, in SIP VoIP mode the NetPerformer always tries to find a match using the other MAP entries in the Voice Mapping Table before attempting the **SUPERMAP** entry.
- For call setup, a **SUPERMAP** entry uses:
  - On the ingress side: the *Proxy server address* specified in the SIP Global parameters (refer to "Enable SIP and Configure the Global SIP Properties" on page 2-4)

  - On the egress side: the destination voice hunt ports specified in the MAP entry

- The NetPerformer determines that the dialing sequence is completed when the global (inter-digits) *Dial timer* expires or when the user terminates dialing with the pound sign (#).

NOTE: The *Dial timer* is configured with the **GLOBAL** submenu of the **SETUP** command. Refer to the *Global Functions* chapter of the *Quick Configuration* fascicle of this document series.

To add a MAP entry with the SUPERMAP Map type:

1. Set the *Map type* to **SUPERMAP**
2. Define the *Egress hunt group pattern*
3. Specify which *Egress hunt group ports* will be used
4. Change the other **MAP** parameters from their default values, if desired.

SE/MAP example: with SUPERMAP Map type

```
BOSTON>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/PHONE/
PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/USER/VLAN,
def:BRIDGE) ? SIP
Define speed dial numbers for voice mapping table
MAP> Operation (ADD/MODIFY/DELETE,def:ADD) ? ADD
MAP> Map type (DIALSTRING/DIALIP/SUPERMAP,def:DIALSTRING) ? SUPERMAP
MAP> Egress hunt group pattern (SEQUENTIAL/ROTARY/NONE,def:NONE) ?
SEQUENTIAL
MAP> Egress hunt group ports (i.e. 101,102,203 or 101,103-106) (def:)
: 101,201,203,103,104
MAP> Strip prefix number of digits (def:I0 E0) :
MAP> Ingress/Egress prepend string (def:) :
MAP> Ingress/Egress append string (def:) :
MAP> Add another map entry (NO/YES,def:YES) ? NO

Saving map entry...
```

All of these parameters are common to the other MAP types, and are detailed in the section DIALSTRING Map Type on page 2.

2.7.5 Modifying a MAP Entry

You can modify a **MAP** entry that has already been defined. Refer to Figure 2-5.

To modify a MAP entry:

1. Enter the menu sequence: **SE** ↵ **MAP**
2. Set the *Operation* to **MODIFY**

3. At the *Map type* prompt:
   - Enter **SUPERMAP** to modify the **SUPERMAP** entry, ***or***
   - Enter **STANDARD** to modify a **DIALSTRING** or **DIALIP** entry.
4. If you select **STANDARD** for the *Map type*, specify the *Entry digits* of the **MAP** entry you want to modify

NOTE: The *Entry digits* string is not required if you are modifying the **SUPERMAP** entry.

5. The NetPerformer lists all parameters for this **MAP** entry with their current values, and then prompts you for the new values. Change the parameters to the new values desired, or press **<Enter>** to skip to the next parameter.
6. Enter **YES** at the *Modify another map entry* prompt if you would like to modify another existing **MAP** entry.

SE/MAP example: modifying a MAP entry

```
PHOENIX>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/PHONE/
PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/USER/VLAN,
def:BRIDGE) ? MAP
MAP> Operation (ADD/MODIFY/DELETE,def:ADD) ? MODIFY
MAP> Map type (def:STANDARD) ?
MAP> Entry digits (def:) ? 35434
MAP 35434> Map type.............................DIALSTRING
MAP 35434> Entry digits.........................35434
MAP 35434> Digits string length.................5
MAP 35434> Egress hunt group pattern............NONE
MAP 35434> Strip prefix number of digits........I0 E0
MAP 35434> Ingress\Egress prepend string........NONE
MAP 35434> Ingress\Egress append string.........NONE

MAP 35434> Map type (def:DIALSTRING) ?
MAP 35434> Entry digits (def:35434) ?
MAP 35434> Digits string length (5-40,def:5) ?
MAP 35434> Egress hunt group pattern (def:NONE) ? SEQUENTIAL
MAP 35434> Egress hunt group ports (def:) ? 102
MAP 35434> Strip prefix number of digits (def:I0 E0) ?
MAP 35434> Ingress/Egress prepend string (def:NONE) ?
MAP 35434> Ingress/Egress append string (def:NONE) ?
MAP> Modify another map entry (NO/YES,def:NO) ?
```

2.7.6 Deleting a MAP Entry

You can delete a **MAP** entry that has already been defined. Refer to Figure 2-5.

To delete a MAP entry:

1. Enter the menu sequence: **SE** ↵ **MAP**
2. Set the *Operation* to **DELETE**
3. At the *Map type* prompt:
   - Enter **SUPERMAP** to delete the **SUPERMAP** entry, ***or***
   - Enter **STANDARD** to delete a **DIALSTRING** or **DIALIP** entry.
4. If you select **STANDARD** for the *Map type*, specify the *Entry digits* of the **MAP** entry you want to delete

NOTE: The *Entry digits* string is not required if you are deleting the **SUPERMAP** entry.

Caution: The **MAP** entry will be deleted immediately, with no confirmation requested. **Enter the *Entry digits* with care.**

5. Enter **YES** at *Delete another map entry* if you would like to delete another **MAP** entry.

NOTE: You can delete all entries in the Voice Mapping Table simultaneously with the Erase Map File (**EMF**) command. Enter **EMF** at the console command prompt.

SE/MAP example: deleting a MAP entry

```
PHOENIX>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/PHONE/
PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/USER/VLAN,
def:BRIDGE) ? MAP
MAP> Operation (ADD/MODIFY/DELETE,def:ADD) ? DELETE
MAP> Map type (def:STANDARD) ?
MAP> Entry digits (def:) ? 35434
MAP> Delete another map entry (NO/YES,def:NO) ?
```

2.7.7 Ingress and Egress Dial Rule Definitions

- **Ingress dial rules** are for VoIP calls **initiated** by the NetPerformer unit
- **Egress dial rules** are for VoIP calls **received** by the NetPerformer unit.

Figure 2-6 shows the directionality of ingress and egress VoIP calls.

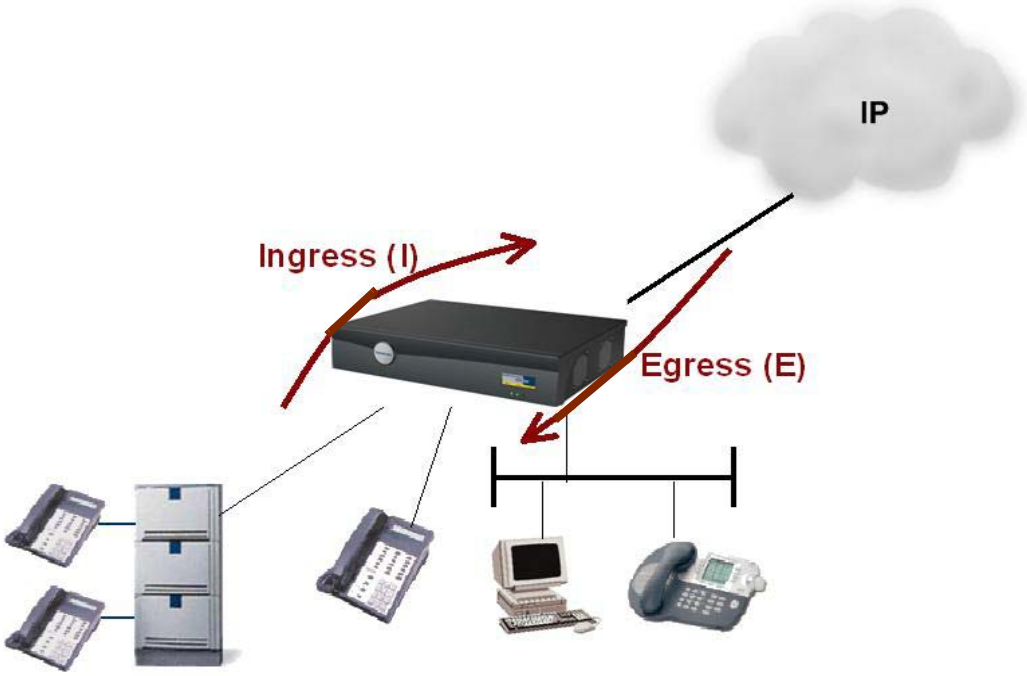

Figure 2-6: Ingress and Egress Calls

Ingress and egress dial rules are based on the following **MAP** parameters:

- *Entry digits:* Specifies the dialing string that the user must enter to activate call setup
- *Strip prefix number of digits:* The number of digits that are deleted from the beginning of the *Entry digits* before proceeding with call setup
- *Ingress/Egress prepend string:* The digits that are added at the beginning of the *Entry digits* before proceeding with call setup
- *Ingress/Egress append string:* The digits that are added at the end of the *Entry digits* before proceeding with call setup

Dial rules are applied on both inbound and outbound calls by parsing the ingress and egress rule definitions and applying them to the *Entry digits*.

The letters **I** (for ingress) and **E** (for egress) distinguish the two sides in the rule definition string. They can be concatenated, separated by a space or a slash. For example, valid values for *Strip prefix number of digits* are I3E4 and I3 E4, both of which remove 3 digits on the ingress side and 4 digits on the egress side.

Ingress Dial Rule Example

- *Entry digits*: **987******
- *Strip prefix number of digits*: **I3**

  If the call is in ingress, remove the first 3 digits of the dial string.
- *Ingress/Egress prepend string*: **I1234**

If the call is in ingress, add the digit string **1234** at the beginning of the dial string.

- *Ingress/Egress append string*: **I4567**

  If the call is in ingress, add the digit string **4567** at the end of the dial string.

With this definition, the dial string 987**654321** for a call in ingress results in 1234**654321**4567 before the NetPerformer proceeds with call setup.

Egress Dial Rule Example

- *Entry digits*: **1234**********
- *Strip prefix number of digits*: **E10**

  If the call is in egress, remove the first 10 digits of the received string.

- *Ingress/Egress prepend string*: **E9**

  If the call is in egress, add the digit **9** to the beginning of the received string.

- *Ingress/Egress append string*: **E8**

  If the call is in egress, add the digit **8** at the end of the received string.

With this definition, the dial string 1234654321**4567** for a call in egress results in 9**4567**8 before being forwarded to the voice ports defined with *Egress hunt group ports*.

NOTE: To allow these digits to be passed to an attached PBX or PSTN network, the *Fwd digits* parameter on the voice channel must be set to ALL.

Ingress/Egress Dial Rule Example

- *Entry digits*: **987******
- *Strip prefix number of digits*: **I2E3**

  If the call is in ingress, remove the first 2 digits. If it is in egress, remove the first 3 digits.

- *Ingress/Egress prepend string*: **I123E45**

  If the call is in ingress, prepend the digit string **123**. If it is in egress, prepend the digit string **45**.

- *Ingress/Egress append string*: **I456E9**

  If the call is in ingress, append the digit string **456**. If it is in egress, append the digit **9**.

With this definition, the dial string 98**7654321** for a call in ingress results in 123**7654321**456 before the NetPerformer proceeds with call setup. The dial string 987**654321** for a call in egress results in 45**6543219** before forwarding the digits to the PBX or PSTN.

2.8 Configuring the UA as a Gateway or Endpoint

The UA can be configured as an *Endpoint* or *Gateway* using the **USERAGENTTYPE** parameter in the Extended SIP Parameters set.

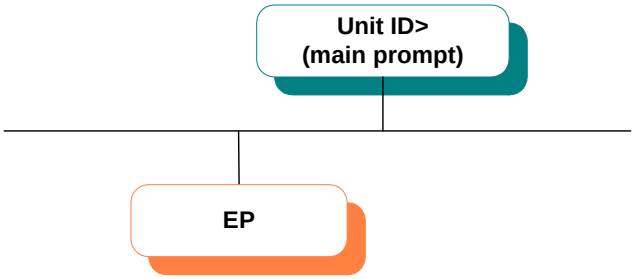

Figure 2-7: EP Path in the CLI Tree

To define the UA as an endpoint or gateway:

- Enter the following at the NetPerformer console main prompt:

  EP SIP USERAGENTTYPES *value*

  where *value* can be set to:

  - **ENDPOINT:** (default) If the UA receives an **INVITE** and there is no channel available to connect another call, the UA sends a **486 Busy** message. In this case, the proxy server will not attempt the place the call elsewhere.
  - **GATEWAY:** If the UA receives an **INVITE** and there is no channel available to connect another call, the UA sends a **503 Service Unavailable** message. In this case, the proxy server will attempt to place the call via another route, if one is available.

Codec Negotiation

3.1 About Codec Negotiation

Codec negotiation allows a NetPerformer unit to automatically change the codec that is loaded for a particular channel according to the codec list it receives in a SIP **INVITE** message. Codec negotiation is available on all SIP-enabled NetPerformer products that run V10.2.X.

With SIP, when a unit sends an **INVITE** message to the remote side, the remote channel must be using the same codec for the call to be accepted.

- Codec negotiation ensures that this is always the case, without requiring manual reconfiguration of the channel

  Only the remote side can negotiate the codec.

- With codec negotiation calls can be set up more easily, as they are not restricted to channels configured with the same codec as the originating channel
- The negotiation process is carried out rapidly, and does not interfere with the efficiency of the link.

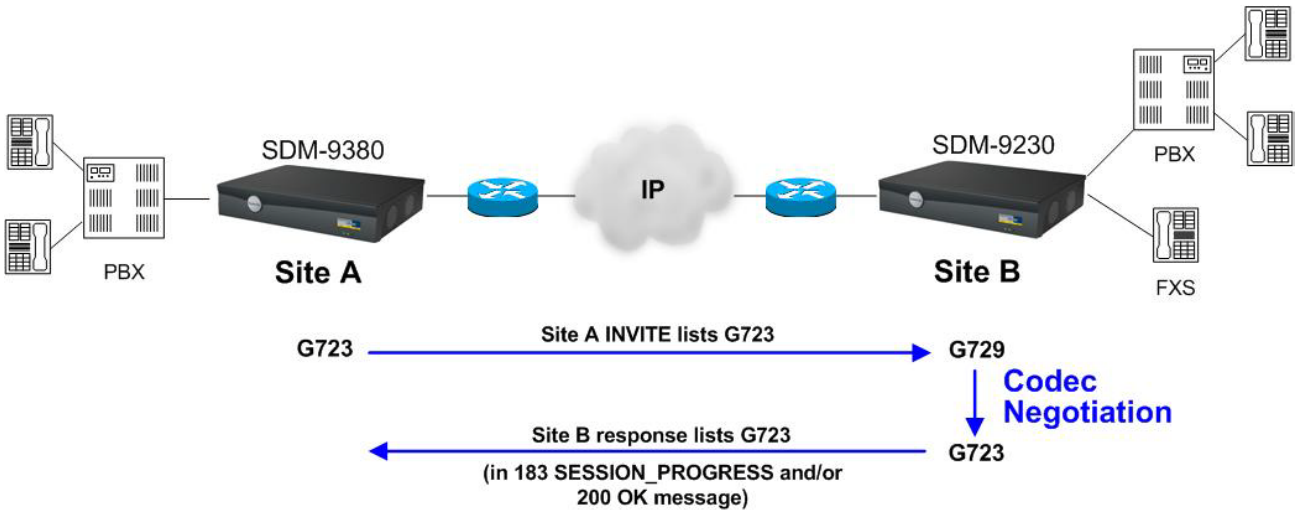

Figure 3-1: Codec Negotiation Example 1: INVITE Lists G7xx

For example, in an application using SIP VoIP like the one in Figure 3-1, Site A uses G723 and Site B uses G729. The **INVITE** message from Site A lists the G723 codec. The **INVITE** is received and accepted at Site B, and the receiving channel changes its current configuration to G723. Details of this transaction are provided in the following sections.

3.2 Negotiation Procedure

The following codec negotiation principles are common to all NetPerformer products running V10.2.X:

- An **INVITE** from the calling unit lists the codec that is currently running on the voice channel from which the call is being placed, as well as all codecs that are enabled in the Codec Negotiation Table of the calling unit
- The value of the voice channel *Protocol* parameter on the called unit is considered the *preferred codec* for that channel

  When the *Protocol* parameter is set to **PCM64K**, the G711 codec is used. The G711 law (alaw or µlaw) is determined from the digital link configuration. Refer to the *Digital Voice* fascicle of this document series for details.
- A *Codec Negotiation Table* can be configured on the called unit to provide alternatives to the preferred codec in case the **INVITE** from the calling unit does not list that codec
- To accept the call, the called unit must be able to match one of the codecs listed in the **INVITE** with either its preferred codec or a codec in its Codec Negotiation Table:
  - **If the preferred codec**, no change of codec is required on the DSP. The call will go up using the preferred codec of the called unit. **This is always the preferred course of action.**
  - If the preferred codec does not match, but **a match is found with one or more codecs listed in the called unit's Codec Negotiation Table**, then the first perfect match is loaded in the DSP, and the call will go up using that codec.

  If no match is found, the called unit sends a **415 Unsupported Media Type** message to the calling unit.
- The called unit lists its codec choice in the first message that can contain the Session Description Protocol (SDP). This message depends on the interface at the remote end:
  - **If the remote end is a PBX**, the audio path opens immediately, and the remote unit sends a **SIP 183 SESSION_PROGRESS** message to transport the dial tone from the PBX. The SDP is included with this message, as well as with the **SIP 200 OK** message.
  - **If the remote end is an FXS interface**, the remote unit first sends a ring (**SIP 180 Ringing** message), which cannot contain the SDP. In this case, the SDP (with the selected codec) is included with the **SIP 200 OK** message only, which the remote unit sends when the FXS interface goes off hook.

Codec negotiation is affected by the type of NetPerformer product involved in the negotiation process, as explained on "Effects of Product Type on the Negotiation Process" on page 3-5. See also "Other Factors Affecting Codec Selection" on page 3-8.

3.2.1 Negotiation Limitations

- A channel configured in ACELP-CN can negotiate toward G711 (PCM64K) only.
- ACELP-CN cannot be loaded through codec negotiation. If the called unit receives an **INVITE** with ACELP-CN, it must already be configured on the channel (using the *Protocol* parameter).

Refer also to "DSP Algorithm Limitations (Quadra File)" on page 3-8.

3.3 Effects of Product Type on the Negotiation Process

3.3.1 SDM-9220 and SDM-9230

For the SDM-9220 and SDM-9230:

- **The DSP loads all related algorithms at once**

  For example, if G723 is configured with the voice channel *Protocol* parameter, all algorithms related to G7xx are loaded.

  This does not affect which codecs are listed in the SDP. When the unit sends an INVITE it populates the SDP with the preferred codec (G723, in this example) along with all codecs listed in the *Codec Negotiation Table*.

- The *Codec Negotiation Table* can be configured to allow negotiation toward **all available codecs** (except ACELP-CN): G729 (including G729A), G723, G726-16K, G726-24K, G726-32K, G726-40K, G711 alaw and G711 µlaw.

  Configuration details are provided in "Configuring the NetPerformer for Codec Negotiation" on page 3-14.

3.3.2 SDM-9360, SDM-9380 and SDM-9585

For the SDM-9360, SDM-9380 and SDM-9585:

- **The DSP loads only one algorithm at a time**

  One exception to this rule is that when G723 is loaded, the **INVITE** will also list G711. However, if a channel is running G711, it cannot accept G723.

- The Codec Negotiation Table can be configured to allow negotiation toward **G711 alaw and G711 µlaw only.**

3.4 Example Scenarios

3.4.1 INVITE Lists G7XX

NOTE: This is the scenario shown in Figure 3-1.

- The channel on the SDM-9380 at Site A is configured with G723, and there are no codecs defined in the Codec Negotiation Table
- The Site A unit sends an **INVITE** that lists G723 to Site B
- The receiving channel on the SDM-9230 at Site B is running G729, and the Codec Negotiation Table includes G723
- The Site B unit sends a response (a **SIP 183 SESSION_PROGRESS** and/or **SIP 200 OK** message) that lists G723 as the codec choice, and it loads G723 on the channel.

NOTE: If the Site A unit is an SDM-9220 or SDM-9230, and the Site B unit is an SDM-9360, SDM-9380 or SDM-9585, **this scenario will not work**, since the SDM-9360, SDM-9380 and SDM-9585 **cannot switch from G729 to G723**.

3.4.2 INVITE Lists ACELP-CN Only

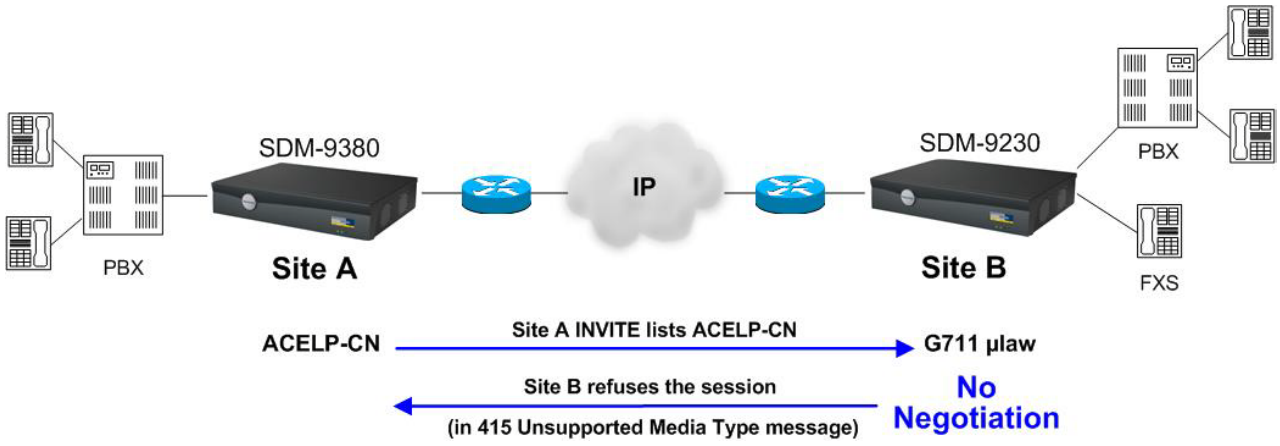

Figure 3-2: Codec Negotiation Example 2: INVITE Lists ACELP-CN Only

- The channel on the SDM-9380 at Site A is configured with ACELP-CN, and there are no codecs defined in the Codec Negotiation Table
- The Site A unit sends an **INVITE** message to Site B

- The receiving channel on the SDM-9230 at Site B is running G711 µlaw, and there are no codecs defined in the Codec Negotiation Table
- The Site B unit refuses the INVITE in its response (a **SIP 415 Unsupported Media Type** message).

  It does not load ACELP-CN, as this algorithm cannot be negotiated. Refer to "Negotiation Limitations" on page 3-4.

3.5 Other Factors Affecting Codec Selection

As we have seen, codec negotiation is affected by:

- The preferred codec on the called unit
- The content of the called unit's Codec Negotiation Table
- The type of NetPerformer product installed at the remote location
- Limitations on the type of codecs that can be negotiated (ACELP-CN).

The codec that will be negotiated and loaded on a particular channel is also determined from:

- The list of codecs in the calling unit's Codec Negotiation Table. The SDP list of the **INVITE** message contains both the configured *Protocol* **and the codecs configured in the Codec Negotiation Table.**

This means that the Codec Negotiation Table is used in two ways:

- **On the calling unit:** To build the SDP section of the **INVITE** message. The codecs that can be accepted for this SIP session are included with this message.
- **On the called unit:** If the preferred codec of a channel (the one set with the voice channel *Protocol* parameter) is **not** on the list received with an **INVITE** message, the called unit will accept the SIP session **if and only if at least one codec of the calling unit is listed in its Codec Negotiation Table.**

3.5.1 DSP Algorithm Limitations (Quadra File)

The number of voice channels you can configure to a particular voice *Algorithm group* is limited by the number of DSP channels that have already been allocated to another *Algorithm group* by the NetPerformer unit. This allocation is carried out dynamically by the unit when the *Protocol* parameter is defined, and varies according to DSP type.

DSP type	Low density DSP	Max. channels per DSP	Low density (DSP-120 or DSP-160)	Max. channels per DSP	High density DSP	Max. channels per DSP pair
	SDM-9360, SDM-9380, SDM-9585		SDM-9220, SDM-9220GW, SDM-9230, SDM-9230GW		SDM-9230 Rev. 3, SDM-9230GW	
	Qa 1.2.1 R01		Qb 1.2.1 R01		Qc 1.2.1 R01	
	30		30		120	

Table 3-1: Maximum number of channels available per DSP type

DSP type	Low density DSP	Max. channels per DSP	Low density (DSP-120 or DSP-160)	Max. channels per DSP	High density DSP	Max. channels per DSP pair
	G723:	4	G7XX:	5	G7XX:	10
	G726 16K to 40K:	4				
	G729: G729A:	3 5				
	ACELP-CN:	4	ACELP-CN:	5	ACELP-CN:	10
	TRANSPARENT, G711[a]:	5	TRANSPARENT, G711[1]:	5	TRANSPARENT, G711[1]:	10

Table 3-1: Maximum number of channels available per DSP type

a.G711 (PCM64K) and TRANSPARENT are also supported by all other algorithms. However, they do not support any other algorithms. See Example 3 on "Example 3: G711 (PCM64K)/TRANSPARENT Limitation" on page 3-10.

When you select a voice algorithm with the *Protocol* parameter, all channels on the DSP processor (or pair of processors in the case of the high density DSP) are allocated to the *Algorithm group* to which that *Protocol* belongs.

- You can continue configuring more voice channels with the same *Protocol* value, or other values belonging to the same *Algorithm group*, up to the *Max. number of channels* for that DSP type
- When mixing algorithm groups, the *Max. number of channels* can be configured only if you observe the limitations of the *Max. channels per DSP* (for the low-density DSP) or *Max. channels per DSP pair* (for the high-density DSP).

Example 1: Low-density DSP on the SDM-9230

- Set the *Protocol* parameter on voice channel 101 on an E1 interface card to **G726 16K**
- The SDM-9230 loads the first *Algorithm group* (G7XX) in the first DSP processor:
  - One DSP channel is used for voice channel 101
  - The other 4 channels on this DSP processor remain available for voice channel configuration. However, you can only select a *Protocol* value from:
    - The first algorithm group: **G723**, **G726 16K**, **G726 24K**, **G726 32K**, **G726 40K**, **G729**, **G729A** ***or***
    - **PCM64K (G711)** or **TRANSPARENT**, which are available when any algorithm group is loaded in a DSP.
- Set the *Protocol* parameter on all remaining voice channels on the E1 interface card to **ACELP-CN:**

- The SDM-9230 skips the 4 unused channels on the first DSP processor, as they are reserved for a G7XX algorithm
- DSP processors 2 to 6 can be fully loaded with ACELP-CN at 5 channels each, for a total of 25 channels
- Voice channels 127 to 130 cannot support ACELP-CN. If you try to configure them as ACELP-CN, the unit displays the following message at the console:

WARNING: **Maximum of 26 simultaneous calls, Not enough DSP channels available**

Workaround: If your application allows, set the *Protocol* parameter on the last four voice channels to a G7XX algorithm. This will provide the total allowable 30 channels using the low-density DSP.

Example 2: High-density DSP on the SDM-9230

NOTE: On the high-density DSP, each pair of DSP cores shares the same memory. **Therefore when a given codec is loaded, two DSP cores are allocated to it.**

- Set the *Protocol* parameter on voice channel 101 on an E1 interface card to **G726 16K**
- The SDM-9230 loads the first *Algorithm group* (G7XX) in the **first pair of DSP processors:**
  - One channel is used for voice port 101
  - The other 9 channels on this pair of DSP processors remain available **for G723**, **G726 16K**, **G726 24K**, **G726 32K**, **G726 40K**, **G729 or G729A only**
- You can then configure up to 50 E1 voice channels as ACELP-CN using the high-density DSP on this unit.

Example 3: G711 (PCM64K) / TRANSPARENT Limitation

Although G711 (**PCM64K**) and **TRANSPARENT** are supported by all other algorithms, they do not support any other algorithms. If you are mixing voice algorithms on a single digital interface, you should configure the highest numbered channels as **PCM64K** or **TRANSPARENT**. Otherwise, you may be unable to configure all channels of the digital interface for voice.

NOTE: G711 is configured using the value **PCM64K**.

- On an E1 interface card in an SDM-9230 with low-density DSP:
  - Set the *Protocol* parameter on voice channels 101-115 and 117-130 to **ACELP-CN**
  - Set the *Protocol* parameter on voice channel 116 to **PCM64K** or **TRANSPARENT**
- The SDM-9230 loads ACELP-CN in the first three DSP processors:
  - The first DSP processor handles voice channels 101-105
  - The second DSP processor handles voice channels 106-110
  - The third DSP processor handles voice channels 111-115
- The SDM-9230 then loads G7XX in the fourth DSP processor.
  - One DSP channel is used for voice channel 116
  - The other 4 channels on this DSP processor remain available for voice channel configuration. **However, you can only select G723, G726 16K, G726 24K, G726 32K, G726 40K, G729, G729A, PCM64K or TRANSPARENT as the *Protocol* value.** Since no other channels are configured to one of these algorithms, the SDM-9230 skips these 4 channels.
- The SDM-9230 loads G7XX in the fifth and sixth DSP processors:
  - The fifth DSP processor handles voice channels 117-121
  - The sixth DSP processor handles voice channels 122-126
  - **Thus there are no DSP channels available for voice channels 127 to 130.**

NOTE: If the G711 channel is configured on voice channel 130 instead of 116, all channels can be allocated on the 6 DSPs without problem, since the G7XX algorithm group supports G711.

3.5.2 Combined Effect of All Factors

Table 3-2 shows the result of all factors affecting codec negotiation in various application scenarios.

CALLING UNIT (SITE A)				CALLED UNIT (SITE B)				RESULT
Product type	**Protocol**	**Codec Nego. Table**	**SDP list (with INVITE)**	**Product type**	**Pre-ferred codec**	**Codec Nego. Table**	**Codec choice**	
SDM-9220 or SDM-9230	G711 alaw (PCM64K)	none	G711 alaw	SDM-9220 or SDM-9230	G729	G711 alaw	G711 alaw	Negotiation toward G711 alaw at Site B
SDM-9220 or SDM-9230	G729	G711 alaw	G729, G711 alaw	SDM-9220 or SDM-9230	G723	G711 alaw	G711 alaw	Negotiation toward G711 alaw at Site B Site A has to switch to G711 alaw
SDM-9220 or SDM-9230	G729	G711 alaw	G729, G711 alaw	SDM-9220 or SDM-9230	ACELP-CN	G711 alaw, G729	G711 alaw	Negotiation toward G711 alaw at Site B An ACELP-CN channel can negotiate toward G711 only
SDM-9220 or SDM-9230	G726-24K	G711 µlaw, G723	G726-24K, G711 µlaw, G723	SDM-9360, SDM-9380 or SDM-9585	G711 µlaw	G711 alaw	G711 µlaw	Site B accepts the offer of its pre-ferred codec from Site A Site A has to switch to G711 µlaw
SDM-9220 or SDM-9230	G726-24K	G711 µlaw, G723	G726-24K, G711 µlaw, G723	SDM-9360, SDM-9380 or SDM-9585	G711 alaw	none	Returns a 415 Unsuppor-ted Media Type mes-sage	Site B cannot accept the INVITE. **Cannot** negotiate toward G723 on this product

Table 3-2: Combined effect of factors affecting Codec Negotiation

CALLING UNIT (SITE A)				CALLED UNIT (SITE B)				RESULT
Product type	**Protocol**	**Codec Nego. Table**	**SDP list (with INVITE)**	**Product type**	**Pre-ferred codec**	**Codec Nego. Table**	**Codec choice**	
SDM-9220 or SDM-9230	G726-24K	G711 µlaw, G723	G726-24K, G711 µlaw, G723	SDM-9220 or SDM-9230	G711 alaw	G723	G723	Negotiation toward G723 at Site B **Can** negotiate toward G723 on this product Site A has to switch to G723
SDM-9360, SDM-9380 or SDM-9585	G723	none	G723	SDM-9220 or SDM-9230	G729	G723	G723	Negotiation toward G723 at Site B Scenario described in “INVITE Lists G7XX” on page 3-6
SDM-9220 or SDM-9230	G723	none	G723	SDM-9360, SDM-9380 or SDM-9585	G729	none	Returns a 415 Unsupported Media Type message	Cannot negotiate, as described in “INVITE Lists G7XX” on page 3-6

Table 3-2: Combined effect of factors affecting Codec Negotiation

3.6 Configuring the NetPerformer for Codec Negotiation

Configure the Codec Negotiation Table using the **SIP/CODEC NEGO** submenu of the **SETUP** command. No changes are required to the SIP session and voice channel definitions. Refer to the chapter "Configuring SIP VoIP" on page 2-1 and the *Digital Voice* fascicle of this document series.

NOTE: **By default, no codecs are included in the Codec Negotiation Table.**

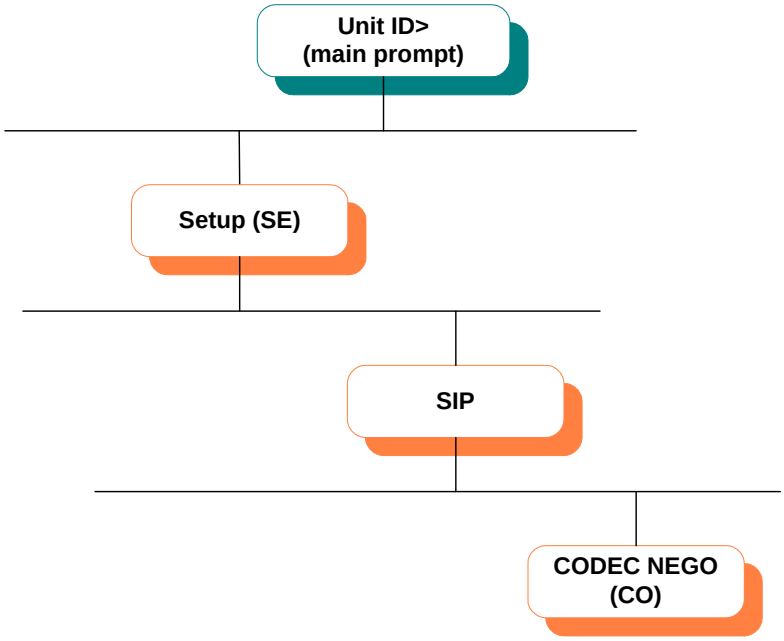

Figure 3-3: SETUP/SIP/CODEC NEGO Path on the CLI Tree

To add a codec to the Codec Negotiation Table:

1. At the NetPerformer command line prompt, enter the menu sequence: **SE** ↵ **SIP** ↵ **CODEC NEGO**
2. Each parameter that is listed refers to an individual codec. Set the parameter to **YES** to add this codec to the Codec Negotiation Table. **This will allow any channel on the unit to accept and load the specified codec, and include it with any INVITE message.** For example:
   - Set *G729* to **YES** to allow any channel on an SDM-9220 or SDM-9230 to accept an **INVITE** listing G729 and load the G729 codec

NOTE: G729A is included with the G729 codec.

- Set *G711 alaw* to **YES** to allow any channel on an SDM-9220, SDM-9230, SDM-9360, SDM-9380 or SDM-9585 to accept an **INVITE** listing G711 alaw and load the G711 alaw codec.

Caution: Refer to "Configuration Tips" on page 3-16 for important considerations when making changes to the codec negotiation parameters.

Table 3-3 on "Codec Negotiation parameters, SNMP variables and their availability on NetPerformer products" on page 3-16 identifies which codecs can be added to the Codec Negotiation Table on the various NetPerformer products, and provides the SNMP variable equivalents to the console parameters.

NOTE: On an SDM-9360, SDM-9380 or SDM-9585, only 2 parameters are available: *G711 alaw* and *G711 ulaw.*

SE/SIP/CODEC NEGO example: on SDM-9220 or SDM-9230

```
SDM-92XX>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/
PHONE/PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/USER/VLAN,
def:BRIDGE) ? SIP
SIP> (GLOBAL/TIMER/RETRIES/DIGEST/CODEC NEGO/ALL,def:GLOBAL) ?
CODEC NEGO
SIP Codec Negotiation> G729 (def:NO) ? YES
SIP Codec Negotiation> G723 (def:NO) ?
SIP Codec Negotiation> G726-16K (def:NO) ?
SIP Codec Negotiation> G726-24K (def:NO) ?
SIP Codec Negotiation> G726-32K (def:NO) ?
SIP Codec Negotiation> G726-40K (def:NO) ?
SIP Codec Negotiation> G711 alaw (def:NO) ?
SIP Codec Negotiation> G711 ulaw (def:NO) ?
```

SE/SIP/CODEC NEGO example: on SDM-9360, SDM-9380 or SDM-9585

```
SDM-93XX>SE
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/
PHONE/PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/SVC/USER/VLAN,
def:GLOBAL) ? SIP
SIP> (GLOBAL/TIMER/RETRIES/DIGEST/CODEC NEGO/ALL,def:GLOBAL) ?
CODEC NEGO
SIP Codec Negotiation> G711 alaw (def:NO) ? YES
SIP Codec Negotiation> G711 ulaw (def:NO) ?
```

Console Parameter	SNMP Variable	Available on
G729	npSipCodecNegoG729	SDM-9220, SDM-9230
G723	npSipCodecNegoG723	SDM-9220, SDM-9230
G726-16K	npSipCodecNegoG72616k	SDM-9220, SDM-9230
G726-24K	npSipCodecNegoG72624k	SDM-9220, SDM-9230
G726-32K	npSipCodecNegoG72632k	SDM-9220, SDM-9230
G726-40K	npSipCodecNegoG72640k	SDM-9220, SDM-9230
G711 alaw	npSipCodecNegoG711Alaw	SDM-9220, SDM-9230, SDM-9360, SDM-9380, SDM-9585
G711 ulaw	npSipCodecNegoG711Ulaw	SDM-9220, SDM-9230, SDM-9360, SDM-9380, SDM-9585

Table 3-3: Codec Negotiation parameters, SNMP variables and their availability on NetPerformer products

3.6.1 Configuration Tips

When deciding which codecs should be added to the Codec Negotiation Table, keep the following in mind:

- There may be different cost considerations and equipment requirements for running another codec in your application. Examine the implications of these factors before you make changes to the codec negotiation parameters on a unit that is up and running.
- Be particularly careful about how you set up codec negotiation in a satellite network. For example, the header size for G729 is relatively large, and could take up a lot of the available bandwidth.
- If you set *G711 alaw* or *G711 ulaw* to **YES**, make sure that any channel set to the G729 protocol has been configured with 2 packets per frame, using the *Packetization selection (Y/N)* parameter on the channel (in the **SE/SLOT/#/CHANNEL** submenu). Otherwise, a change to G711 will make the frames too big for transmission.

  Refer to "Voice Channel Parameters" on page 6-9 for examples.
- If you set *G711 alaw* or *G711 ulaw* to **YES**, and set the *Fax relay* parameter on the voice channel to **T.38**, a SIP **Invite** message will be sent in T.38 fax mode as well as G711 alaw and G711 µlaw. Likewise, if *Fax relay* is set to **T.38_SG3**, the T.38 Super G3 fax mode will be sent.

SIP Hairpin

4.1 About the SIP Hairpin function

The *SIP Hairpin* function provides a TDM local-switch service in cases where VoIP is **not** desired. SIP Hairpin has several applications:

- Permits locally switched voice calls on a NetPerformer installed with the SIP VoIP license, a function which is otherwise not available on this product

  On the NetPerformer in PowerCell mode, local calls can also be switched locally.
- If the Internet goes down, the call can be sent on the local PSTN
- Provides an alternate route if the called Gateway is busy or not responding
- Ideal for emergency dialing, for example to a 911 service where the 911 voice call has to be switched locally back to the PSTN. This function is typically performed using a single FXO card on the NetPerformer.

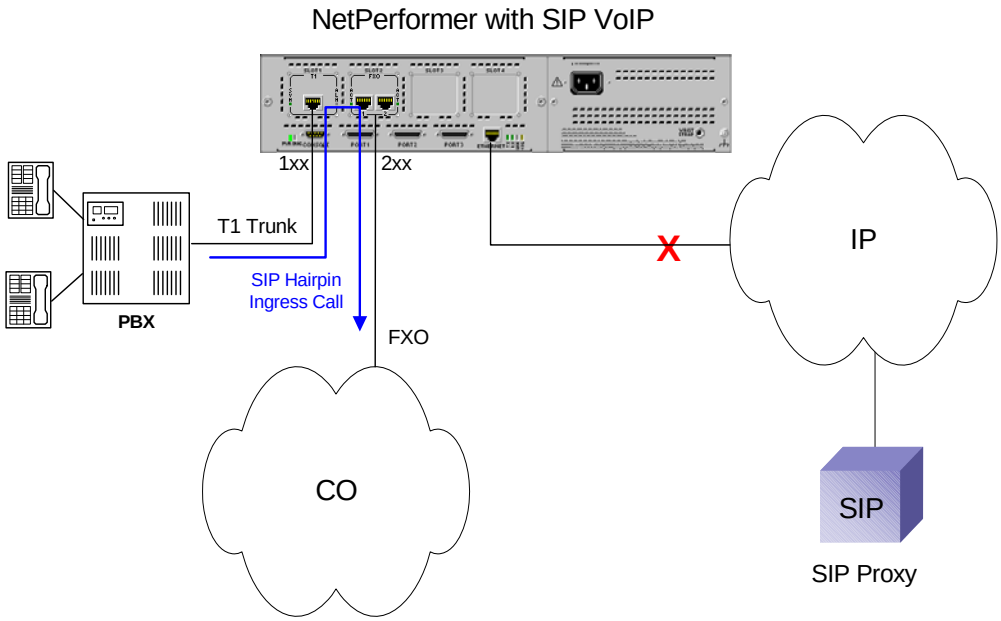

Figure 4-1: SIP Hairpin Scenario 1

4.2 How SIP Hairpin Works

The NetPerformer hairpin function allows you to enable TDM local-switch capability for specific voice calls, based on the dialed number defined in the MAP entries.

NOTE: The dialed number for a voice call can be received from a voice interface (ingress call) or from the IP network through a SIP **Invite** message (egress call). Refer to Figure 2-6:, Ingress and Egress Calls, on page 17.

- When a voice call dialed number commands the NetPerformer to switch the call locally, the Signaling Engine establishes the call by cross-connecting the proper TDM timeslots (voice channels).
- Under these conditions, no voice compression is performed on the voice packets. When voice samples are not compressed, voice quality is preserved at PCM-64 Kbps levels.

To switch voice calls, the SIP Hairpin function requires:

- **For ingress calls:** Based on the dialed number received from the voice interface, information is retrieved from the Voice Mapping Table entry (see next section).
- **For egress calls:** Switching information retrieved from the **Invite** message received from the SIP proxy server (see Hairpin Egress Calls on page 5).

  SIP hairpin egress calling procedure:

  - Based on the dialed number received for a voice interface, the NetPerformer sends an **Invite** message to the SIP proxy server.
  - The SIP proxy server analyzes the telephone number and dialing rules. It sends the **Invite** back to the calling gateway if this is a call to be switched locally by that gateway.

4.3 Hairpin Ingress Calls

The SIP Hairpin feature allows an ingress call (from the PBX) to be locally rerouted on the same Gateway by performing a TDM cross-connect function. For example, in Figure 4-1, the call arrives from the PBX on port **2xx** (slot 2). The called port, **1xx** (slot 1), is connected to the PSTN.

If a dialed number received from a voice interface matches a MAP entry that has its IP address configured to the source IP address of the gateway, the gateway considers the ingress call to be locally connected. The local called port is retrieved from the *Egress Hunt group ports* list in the MAP entry.

4.3.1 Benefits

SIP Hairpin ingress calls are particularly useful when the gateway has lost access to the IP network or the SIP proxy server.

4.3.2 Characteristics

- *Map type* is **DIALIP**
- For the call to be completed successfully, at least one of the *Egress hunt group ports* defined in the MAP entry is not busy
- Call setup is established internally, with no SIP signaling protocols required
- No voice compression, only TDM cross-connect
- No DSPs are allocated once the call is locally connected
- The NetPerformer is able to do SIP Voice Traffic Routing (VTR) and apply VoIP, Peer-to-Peer or Hairpin voice calls, depending on the situation. For example:

  If a call cannot be completed using the first MAP entry (e.g. the SIP registration is lost, SIP errors are encountered, or the remote gateway cannot process the call) the gateway will interrogate the MAP service to verify whether another MAP entry can be applied.

4.4 Hairpin Egress Calls

A SIP Hairpin egress call applies when the calling port **Invite** goes to the SIP proxy server and, based on the DNIS information stored in the SIP **Invite**, the SIP proxy server redirects the call back to the calling VoIP Gateway if the call has to be switched locally.

When it receives the SIP **Invite**, the gateway:

- Compares the remote IP address retrieved from the SDP media descriptor with the source IP address of the gateway.
- If the two match, the NetPerformer uses the list of *Egress Hunt group ports* provided in the MAP entry in order to locally loop back this call. It is therefore important that a MAP entry be configured to determine on which *Egress Hunt group ports* the egress call can be connected.

NOTE: The type of MAP entry is unimportant in this case. For an egress call the DNIS points to the MAP entry, which provides the list of hunt group ports.

4.4.1 Benefits

SIP Hairpin egress calls:

- Provide call security through SIP proxy server authorization
- Permit local calls with call detail records stored in the SIP proxy server database

Once the call has been torn down, the NetPerformer will not create a call detail record. The Voice Log feature used for call detail records on the NetPerformer in PowerCell mode is not supported with the NetPerformer in SIP VoIP mode.

4.4.2 Characteristics

- Call setup is established with a SIP proxy server
- The SIP proxy server reroutes the call back to the gateway that originated the call, if the dialed number is a local call for that gateway
- *Map type* is **DIALSTRING** mode

  This refers to the originating MAP entry. The MAP entry used in **EGRESS** mode can be of any type.
- For the call to be completed successfully, at least one of the *Egress hunt group ports* defined in the MAP entry is not busy
- No voice compression, only TDM cross-connect
- No DSPs allocated once the call is locally connected.

4.5 Configuring the NetPerformer for SIP Hairpin

No special parameters are required to configure a SIP Hairpin scenario, but you need to configure the MAP entries very carefully.

Caution: There is no parameter that enables or disables SIP Hairpin. If you **must not** have SIP Hairpin operating in your network you must configure the MAP entries carefully, especially if you have overloaded MAP entries. Also ensure that the other elements of your network are configured to properly handle the information sent out from the NetPerformer, in particular, the SIP proxy server.

Local calling on the NetPerformer SIP VoIP can be achieved in two ways:

- With a DIALIP MAP entry
- With overloaded MAP entries

  The term *overloaded MAP entries* refers to **multiple MAP entries that use the same dial digits string.**

  - Overloaded MAP entries offer more than one possible destination for a call, much like the NetPerformer Voice Traffic Routing feature.
  - They can be used in other dialing scenarios in the same application.

4.5.1 Using a DIALIP MAP Entry

Configuration

To configure a SIP Hairpin application *without* call detail records:

- Configure a MAP entry in **DIALIP** mode, and set its *IP address* to the destination address.

Tips:

- The *IP destination address* must be the *IP source address* of the gateway itself.
- For an example, refer to Scenario 2: Bypassing the SIP Proxy Server on page 10.

Call Setup

When doing local switching (hairpin), if the voice codec is G729 or some other DSP-intensive protocol, the NetPerformer:

- Disables the DSP
- Creates a TDM cross-connect scenario, and
- Initiates a pure 64 kbps PCM transfer.

The advantage of this method is the absence of compression, improved voice quality and no delays caused by echo cancellation. However, **no call detail records are generated**.

4.5.2 Using Overloaded MAP Entries

Configuration

To configure a SIP Hairpin application *with* call detail records:

> **NOTE:** The call detail records are managed by the SIP proxy server in this application.

1. Configure *overloaded MAP entries* with the *IP address* of the last MAP entry equivalent to the *source IP address* of the gateway. The last MAP entry can be of any type.
2. Configure either a **DIALSTRING** or **DIALIP** MAP entry to allow the NetPerformer to send an **Invite** to the SIP proxy server.

> **NOTE:** The **Invite** must be sent to the SIP proxy server in order to generate a call detail record.

   - If you configure a **DIALSTRING** entry, the MAP table will automatically use the *Proxy server address* as its destination.
   - If you configure a **DIALIP** entry, **you must set the destination *IP address* to the value of the *Proxy server address***.

> **NOTE:** You must order the overloaded map entries correctly to ensure that the ingress call terminates on the same unit. For an example, refer to Scenario 1: Using Overloaded MAP Entries, below.

Call Setup

- When the SIP proxy server receives the **Invite**, it determines that the destination IP address is equivalent to the source IP address (the **IPSRC** address of the NetPerformer interface used to reach the destination IP address). The SIP proxy server then sends the **Invite** back to the source unit.
- The local NetPerformer extracts the voice codec used, the destination IP address and the telephone number (or DNIS) from the looped **Invite**.
- The local NetPerformer discovers that this is a local call, since the IP address retrieved from the **Invite** is identical to the source IP address of the unit.

- The NetPerformer retrieves the specific local voice channel number from the *Egress hunt group ports* parameter of this MAP entry, and completes the call to that port.

NOTE: The extracted voice codec must match the codec configured on the voice channel.

- As soon as a SIP egress call is transmitted across the SIP proxy server and terminates on the NetPerformer, a call detail record (CDR) is logged on the SIP proxy server database.

4.6 Example Applications

4.6.1 Scenario 1: Using Overloaded MAP Entries

In the application shown in Figure 4-1 on "SIP Hairpin Scenario 1" on page 4-2:

- The IP source address of the NetPerformer SIP VoIP is **172.168.1.10**
- Overloaded MAP entries are used to perform the SIP Hairpin function.

Configuration

Here is how the overloaded MAP entries are set up:

DP/MAP example: with overloaded MAP entries

```
SDM-9230>DP
DISPLAY PARAMETERS
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/
PHONE/PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/USER/VLAN,
def:BRIDGE) ? MAP
MAP> Entry digits (def:) ? 514
MAP 514.1> Map type.............................DIALSTRING
MAP 514.1> Entry digits.........................514
MAP 514.1> Digits string length.................10
MAP 514.1> Egress hunt group pattern............NONE
MAP 514.1> Strip prefix number of digits........I0 E0
MAP 514.1> Ingress/Egress prepend string........NONE
MAP 514.1> Ingress/Egress append string.........NONE

MAP 514.2> Map type.............................DIALIP
MAP 514.2> Entry digits.........................514
MAP 514.2> Digits string length.................10
MAP 514.2> Egress hunt group pattern............SEQUENTIAL
MAP 514.2> Egress hunt group ports..............101
MAP 514.2> Strip prefix number of digits........I0 E0
MAP 514.2> Ingress/Egress prepend string........I1
MAP 514.2> Ingress/Egress append string.........NONE
MAP 514.2> Enter an IP address..................176.168.1.10
```

NOTE: In this example, the *Digits string length* is set to 10 to include both a 3-digit speed dial number and up to 7 extended digits. If less than 7 extended digits are entered, the dial string is considered complete when global *Dial timer* parameter expires.

Call Setup

The order of the overloaded **DIALSTRING** entries demonstrates the order in which the actions take place:

- The user dials the phone number **514-555-1212**.

  The NetPerformer detects a **DIALSTRING** *Map type*. It determines that the call is a real SIP call and sends the SIP signaling protocols to the SIP proxy server.

- If the voice connection cannot be established, the gateway interrogates the MAP service for another overloaded entry.

  In this example, the NetPerformer detects a **DIALIP** *Map type*, and evaluates the ingress MAP IP address configured in the MAP entry.

- The ingress MAP IP address is identical to the source IP address of the gateway.

- The NetPerformer applies the MAP Ingress rules (in this case it prepends 1) to specify a long distance call across the public network. It also retrieves the MAP *Egress Hunt group ports* to cross-reference the MAP entry with the calling port.

4.6.2 Scenario 2: Bypassing the SIP Proxy Server

In this application scenario, we want to reach the **MONTREAL** area, which is area code 514. The **MONTREAL** area can be reached through:

- The SIP proxy server
- The local FXO channel (201), using MAP dialing rules
- The intermediary **Unit 3**, using MAP dialing rules. In this case, the SIP proxy server is bypassed.

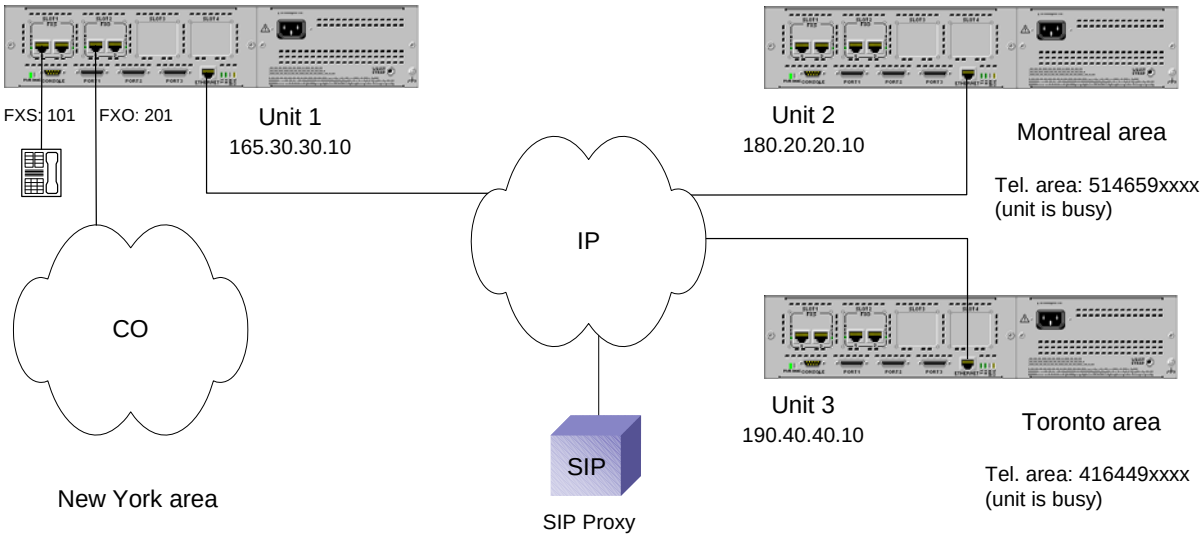

Figure 4-2: SIP Hairpin Scenario 2: Bypassing the SIP Proxy Server

Configuration

The MAP entries for this scenario are configured as follows:

DP/MAP example: bypassing the SIP proxy server

```
SDM-9230>DP
DISPLAY PARAMETERS
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/
PHONE/PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/USER/VLAN,
def:BRIDGE) ? MAP
MAP> Entry digits (def:) ? 514
MAP 514.1> Map type.............................DIALSTRING
MAP 514.1> Entry digits.........................514659
MAP 514.1> Digits string length.................10
MAP 514.1> Egress hunt group pattern............NONE
MAP 514.1> Strip prefix number of digits........I0 E0
MAP 514.1> Ingress/Egress prepend string........NONE
MAP 514.1> Ingress/Egress append string.........NONE

MAP 514.2> Map type.............................DIALIP
MAP 514.2> Entry digits.........................514659
MAP 514.2> Digits string length.................10
MAP 514.2> Egress hunt group pattern............SEQUENTIAL
MAP 514.2> Egress hunt group ports..............201
MAP 514.2> Strip prefix number of digits........I0 E0
MAP 514.2> Ingress/Egress prepend string........I1
MAP 514.2> Ingress/Egress append string.........NONE

MAP 514.2> Enter an IP address..................165.30.30.10
MAP 514.3> Map type.............................DIALIP
MAP 514.3> Entry digits.........................514659
MAP 514.3> Digits string length.................10
MAP 514.3> Egress hunt group pattern............NONE
MAP 514.3> Strip prefix number of digits........I0 E0
MAP 514.2> Ingress/Egress prepend string........I1
MAP 514.2> Ingress/Egress append string.........NONE
MAP 514.3> Enter an IP address..................190.40.40.10
```

Call Setup

In this scenario:

- The user dials **5146591122** on the FXS port (channel 101).

  The *Digits string length* for MAP entry #1 is set to **10**, which means the user can dial up to 10 digits. The first 6 digits comprise the speed dial number, and the last 4 digits are the extended digits.

- **Unit 1** sends its connection request to the SIP proxy server.
  - The SIP proxy server redirects the call to **Unit 2**.
  - **Unit 2** responds with a **486 BUSY HERE** message.

- When **Unit 1** receives the **486 BUSY HERE** message, it searches the MAP file for an overloaded MAP entry, and finds MAP entry #2.

  The *Prepend string* for MAP #2 is set to **I1**, which means that a dialing rule is applied to prepend the digit **1** to the dial string. As a result of this rule, the dial string **514659xxxx** is changed to **1514659xxxx** (for long distance calling).

- This time, **Unit 1** determines this is a local call, since:
  - The type of MAP entry is **DIALIP**, and
  - The IP address of the MAP entry is equivalent to the source IP address of **Unit 1**.
- **Unit 1** then makes a long distance call (using SIP Hairpin) from channel 101 via channel 201 and over the CO.
- If **Unit 1** channel 201 is busy, the unit looks up MAP entry #3:
  - This is a **DIALIP** MAP entry, with its IP address equivalent to the address of **Unit 3**.
  - A dialing rule is applied to prepend the digit **1** to the dial string, which changes **514659xxxx** to **1514659xxxx**.
- The connection request is sent directly to **Unit 3**, without passing through the SIP proxy server. As a result, the call is made with reduced long distance costs.

NOTE: No call detail records are available when bypassing the SIP proxy server.

4.6.3 Scenario 3: Dialing 911 using SIP Hairpin

In this application scenario, we want to dial **911** using SIP Hairpin, *and also* provide call detail records. The physical network is set up in the same way as for Scenario 2:

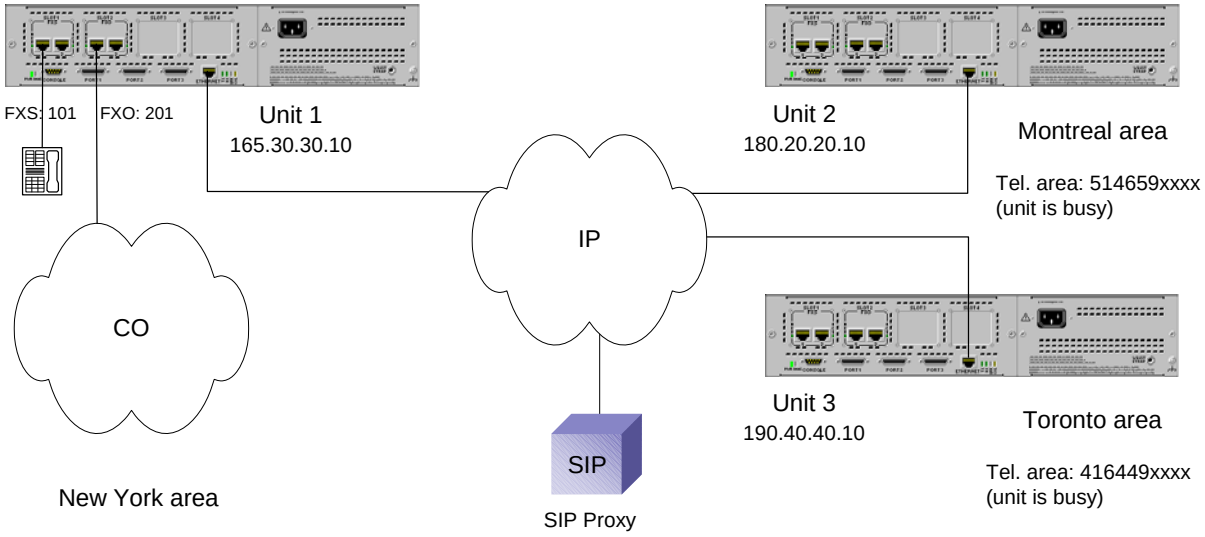

Figure 4-3: SIP Hairpin Scenario 3: for Dialing 911

Configuration

The MAP entry for this scenario with call detail records is configured as follows:

DP/MAP example: for dialing 911, with call detail records

```
SDM-9230>DP
DISPLAY PARAMETERS
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/
PHONE/PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/USER/VLAN,
def:BRIDGE) ? MAP
MAP> Entry digits (def:) ? 911
MAP 911.1> Map type.............................DIALSTRING
MAP 911.1> Entry digits........................911
MAP 911.1> Digits string length................3
MAP 911.1> Egress hunt group pattern...........SEQUENTIAL
MAP 911.1> Egress hunt group ports.............201
MAP 911.1> Strip prefix number of digits.......I0 E0
MAP 911.1> Ingress/Egress prepend string.......NONE
MAP 911.1> Ingress/Egress append string........NONE
```

Call Setup

In this scenario:

- The user dials **911** on the FXS port (channel 101).

- The connection request is sent to the SIP proxy server, which redirects the call to **Unit 1**.
- **Unit 1** determines that this is a local call, and connects to the CO via FXO channel 201.

NOTE: Since the *Egress hunt group ports* parameter is set to a channel number, the NetPerformer is able to redirect the call.

Alternate Scenario without Call Detail Records

It is also possible to dial 911 using SIP Hairpin, but **without redirecting the call via the SIP proxy server and with no call detail records**. The MAP entry for this scenario is configured as follows:

DP/MAP example: for dialing 911, without call detail records

```
SDM-9230>DP
DISPLAY PARAMETERS
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/
PHONE/PORT/
PU/PPPOE/PPPUSER/PVC/REDUNDANCY/SCHEDULE/SIP/SLOT/USER/VLAN,
def:BRIDGE) ? MAP
MAP> Entry digits (def:) ? 911
MAP 911.1> Map type.............................DIALIP
MAP 911.1> Entry digits.........................911
MAP 911.1> Digits string length.................3
MAP 911.1> Egress hunt group pattern............SEQUENTIAL
MAP 911.1> Egress hunt group ports..............201
MAP 911.1> Strip prefix number of digits........I0 E0
MAP 911.1> Ingress/Egress prepend string........NONE
MAP 911.1> Ingress/Egress append string.........NONE
MAP 911.1> Enter an IP address..................165.30.30.10
```

- In this case the connection request is considered a local call.
- The IP address in the MAP entry is equivalent to the source IP address of **Unit 1**.
- The call terminates on the CO, via FXO channel 201 on **Unit 1**.

SIP Redirect Server

5.1 About the SIP Redirect Server

The *SIP Redirect Server* directs calls between several sites and replaces the need for a carrier-grade call manager or telephony switch in small to medium-sized networks. In this application, one NetPerformer unit is configured to direct and manage calls between the other units in the network.

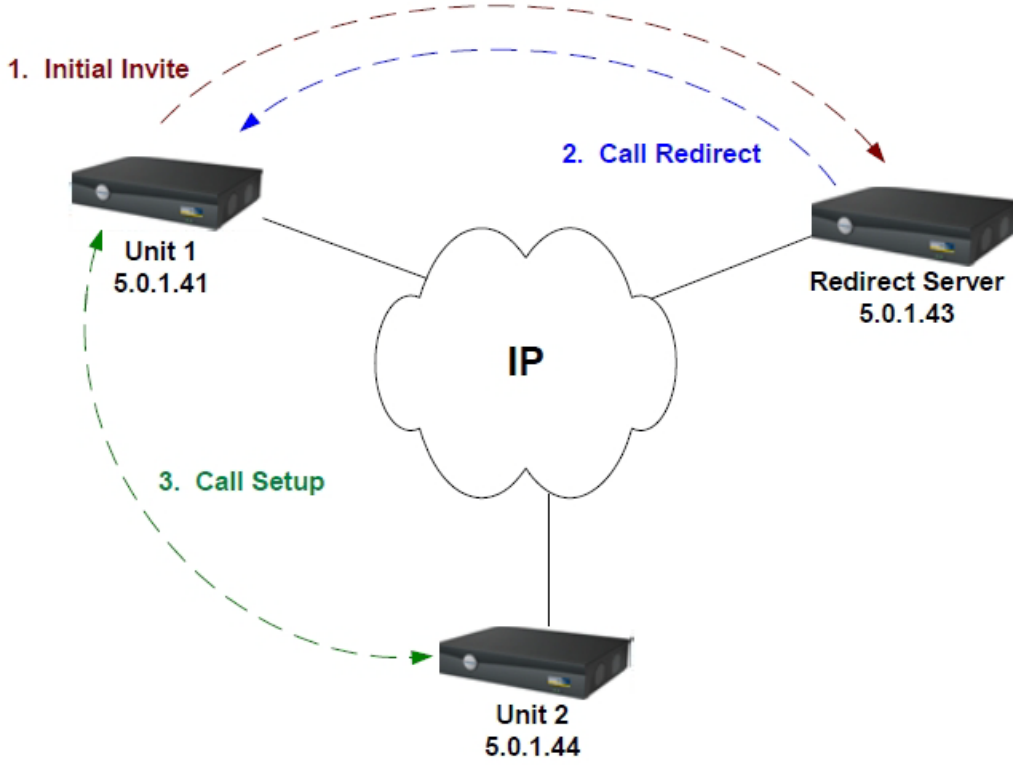

Figure 5-1: SIP Redirect Server Application

NOTE: Figure 5-1 shows an application within a single network. The addresses in a Redirect Server application can also be on different networks.

5.2 Call Negotiation

In the example presented in Figure 5-1 there are three stages in negotiating a call from Unit 1 to Unit 2:

1. **Initial Invite from Unit 1 to the Redirect Server:**

   Unit 1 calls the Redirect Server with a **REQUEST URI** message containing the *Speed dial number* of the location it wants to reach. In this example, the **REQUEST URI** message contains **12345@5.0.1.43**. Refer to the capture on page 6.

   - On Unit 1, the number **12345** matches the **SUPERMAP** map entry on the local unit.
   - This causes the call to be sent to the address of the SIP proxy server, which is configured with the address of the Redirect Server.
   - The call is sent to the Redirect Server as if it were the actual target of the call.

2. C**all Redirect between the Redirect Server and Unit 1:**

   The Redirect Server receives the invite and looks up the destination *Speed dial number* in its Voice Mapping Table (MAP file).

   - The Redirect Server discerns that the destination IP address is not its own, but that of Unit 2.
   - It sends a **302 MOVED TEMPORARILY** message back to Unit 1, containing the IP address of Unit 2 in the *Contact* field.
   - Unit 1 replies to the Redirect Server with an **ACK**.

NOTE: The Redirect Server shares the same internal resources as that used for regular calls. Once call redirection is complete, the Redirect Server releases these resources.

3. **Call Setup between the Unit 1 and Unit 2:**

   When Unit 1 receives the **302 MOVED TEMPORARILY** message from the Redirect Server, it sends an invite to Unit 2 containing the same *Speed dial number* as the original invite.

   - To complete the call connection, **Unit 2 must have a MAP entry that matches these digits**.
   - The actual voice traffic is transported between Unit 1 and Unit 2 only.

5.3 Traffic Volume Considerations

In a SIP Redirect Server application, voice calls and redirect call requests compete for the same resources. If too many SIP requests are received at the same time, the Redirect Server sends a **503 Service Unavailable** message to indicate that it is out of resources and cannot process the request.

To avoid these **Service Unavailable** messages, you should be aware of how many voice channels are available in your application. The maximum number of calls that can be redirected at one time depends on the number of free voice channels on the unit SIP stack.

TIP: Do not use the unit with the highest voice traffic load as your Redirect Server.

On the Redirect Server, the resources available for processing redirect requests are limited by the amount of memory allocated for voice channels. This memory is pre-allocated, and is not affected by the number of voice ports that are actually installed on the unit.

Table 5-1 indicates the resources available on NetPerformer units running in SIP VoIP mode.

NOTE: The *Number of Voice Channels Allocated in the SIP Stack* does ***not*** indicate the maximum number of calls that can be redirected. Rather, it is a measure of how many SIP calls can be processed simultaneously. In other words, once call redirection is completed, the NetPerformer Redirect Server is free to process another SIP redirect from somewhere else.

NetPerformer Model	Number of Voice Channels Allocated in the SIP Stack
SDM-9220	90
SDM-9230	90
SDM-9360	32
SDM-9380	96
SDM-9585	96

Table 5-1: Resources available for concurrent Call Redirects

If you expect a high volume of calls requiring redirection:

- Install an SDM-9230, SDM-9380 or SDM-9585 as your Redirect Server, as it can support up to 120 calls at one time.
- Consider using a standalone SIP proxy server for applications where a higher volume of calls may occur.

5.3.1 Examples

- On an SDM-9360 installed with 4 FXS interface cards, the maximum number of actual voice channels that can be used at one time is 8, leaving 24 channels available to process call redirects.
- If one E1 interface card is installed in an SDM-9360, only 2 voice channels are available to process call redirects.

5.4 Configuring the NetPerformer as a Redirect Server

In a Redirect Server application:

- The Redirect Server is not active by default. **To enable the Redirect Server, you must set the SIP Global *Redirect Server* parameter to ENABLE.** Refer to Enable SIP and Configure the Global SIP Properties on page 4.
- Each gateway requires a **SUPERMAP** entry. Refer to Setting up the Voice Mapping Table on page 10.
- On each gateway, you must set the SIP Global *Proxy server address* parameter to the address of the Redirect Server.
- Each gateway should have MAP entries that identify where each number it supports should egress, using the *Egress hunt group ports* parameter. Refer to "Egress hunt group ports" on page 8-5.

For example, Unit 2 in Figure 5-1 on "SIP Redirect Server Application" on page 5-2 requires a MAP entry for Speed Dial Number **12345** indicating that a call to this number should be forwarded to port **201**. Refer to the console capture on "Unit 2" on page 5-7.

Here is a capture of the configuration settings required for each of the three units in the example depicted in Figure 5-1:

5.4.1 Unit 1

```
UNIT_1>DP
DISPLAY PARAMETERS
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/
PHONE/
PORT/PU/PVC/SCHEDULE/SIP/SLOT/USER/VLAN/ALL,def:PORT) ? SIP
SIP> (GLOBAL/TIMER/RETRIES/ALL,def:GLOBAL) ?
SIP Global> Administrative status..............ENABLE
SIP Global> Proxy server address...............5.0.1.43
SIP Global> UDP Port...........................5060
SIP Global> Gateway ID.........................0
SIP Global> Server group.......................
SIP Global> Registration.......................DISABLE
SIP Global> ANI digits.........................
SIP Global> DTMF Payload.......................104
SIP Global> Redirect Server....................DISABLE

UNIT_1>DMF
DISPLAY MAP FILE
MAP VERSION: B.3
```

For incoming calls:

```
MAP 1> Map type................................DIALSTRING
MAP 1> Entry digits............................54321
MAP 1> Digits string length....................5
MAP 1> Egress hunt group pattern...............SEQUENTIAL
MAP 1> Egress hunt group ports.................101
MAP 1> Strip prefix number of digits...........I0 E0
```

```
MAP 1> Ingress/Egress prepend string.....NONE
MAP 1> Ingress/Egress append string.....NONE
```

For outgoing calls:

```
MAP 2> Map type.....SUPERMAP
MAP 2> Egress hunt group pattern.....NONE
MAP 2> Strip prefix number of digits.....I0 E0
MAP 2> Ingress/Egress prepend string.....NONE
MAP 2> Ingress/Egress append string.....NONE
```

5.4.2 Unit 2

```
UNIT_2>DP
DISPLAY PARAMETERS
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/
PHONE/
PORT/PU/PVC/SCHEDULE/SIP/SLOT/USER/VLAN/ALL,def:SIP) ? SIP
SIP> (GLOBAL/TIMER/RETRIES/ALL,def:GLOBAL) ?
SIP Global> Administrative status.....ENABLE
SIP Global> Proxy server address.....5.0.1.43
SIP Global> UDP Port.....5060
SIP Global> Gateway ID.....0
SIP Global> Server group.....
SIP Global> Registration.....DISABLE
SIP Global> ANI digits.....
SIP Global> DTMF Payload.....104
SIP Global> Redirect Server.....DISABLE

UNIT_2>DMF
DISPLAY MAP FILE
MAP VERSION: B.3
```

For incoming calls:

```
MAP 1> Map type.....DIALSTRING
MAP 1> Entry digits.....12345
MAP 1> Digits string length.....5
MAP 1> Egress hunt group pattern.....SEQUENTIAL
MAP 1> Egress hunt group ports.....201
MAP 1> Strip prefix number of digits.....I0 E0
MAP 1> Ingress/Egress prepend string.....NONE
MAP 1> Ingress/Egress append string.....NONE
```

For outgoing calls:

```
MAP 2> Map type.....SUPERMAP
MAP 2> Egress hunt group pattern.....NONE
MAP 2> Strip prefix number of digits.....I0 E0
MAP 2> Ingress/Egress prepend string.....NONE
MAP 2> Ingress/Egress append string.....NONE
```

5.4.3 Redirect Server

```
REDIRECT_SERVER>DP
DISPLAY PARAMETERS
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/FILTER/GLOBAL/IP/IPX/MAP/
PHONE/
PORT/PU/PVC/SCHEDULE/SIP/SLOT/USER/VLAN/ALL,def:GLOBAL) ? SIP
SIP> (GLOBAL/TIMER/RETRIES/ALL,def:GLOBAL) ?
SIP Global> Administrative status..............ENABLE
SIP Global> Proxy server address...............
SIP Global> UDP Port...........................5060
SIP Global> Gateway ID.........................0
SIP Global> Server group.......................
SIP Global> Registration.......................DISABLE
SIP Global> ANI digits.........................
SIP Global> DTMF Payload.......................104
SIP Global> Redirect Server....................ENABLE

REDIRECT_SERVER>DMF
DISPLAY MAP FILE
MAP VERSION: B.3
```

For redirecting calls to Unit 1:

```
MAP 1> Map type................................DIALIP
MAP 1> Entry digits............................54321
MAP 1> Digits string length....................5
MAP 1> Egress hunt group pattern...............NONE
MAP 1> Strip prefix number of digits...........I0 E0
MAP 1> Ingress/Egress prepend string...........NONE
MAP 1> Ingress/Egress append string............NONE
MAP 1> Enter an IP address.....................5.0.1.41
```

For redirecting calls to Unit 2:

```
MAP 2> Map type................................DIALIP
MAP 2> Entry digits............................12345
MAP 2> Digits string length....................5
MAP 2> Egress hunt group pattern...............NONE
MAP 2> Strip prefix number of digits...........I0 E0
MAP 2> Ingress/Egress prepend string...........NONE
MAP 2> Ingress/Egress append string............NONE
MAP 2> Enter an IP address.....................5.0.1.44
```

Monitoring VoIP Functions

6.1 About VoIP Functions

The following areas of the NetPerformer console command set provide information on the effects of codec negotiation in your network and the current configuration of parameters involved:

- For a display of channel status in real time, execute the Display Call States (**DCS**) command (see next section)

  Active Calls indicates the number of active calls on this slot, and *Total Active Calls* the number of active calls on the entire unit.

- To view the status of a SIP session, execute the **SIP** option of the Display States (**DS**) command (see "SIP Session Status" on page 6-4)
- To view the *Negotiated Codec Payload* of a particular voice channel, execute the **SLOT** option of the Display States (**DS**) command (see "Negotiated Codec Payload" on page 6-5)

  The value of this statistic indicates whether codec negotiation has taken place.

- To view SIP counters, execute the **SIP** option of the Display Counters (**DC**) command (see "SIP Counters" on page 6-7)
- To determine which codecs are included in the Codec Negotiation Table, use the **SIP/CODEC NEGO** option of the Display Parameters (**DP**) command (see "Codec Negotiation Table" on page 6-8)
- To view the current values of the *Protocol* and *Packetization selection (Y/N)* parameters on the voice channel, use the **SLOT/CHANNEL** option of the Display Parameters (**DP**) command (see "Voice Channel Parameters" on page 6-9)

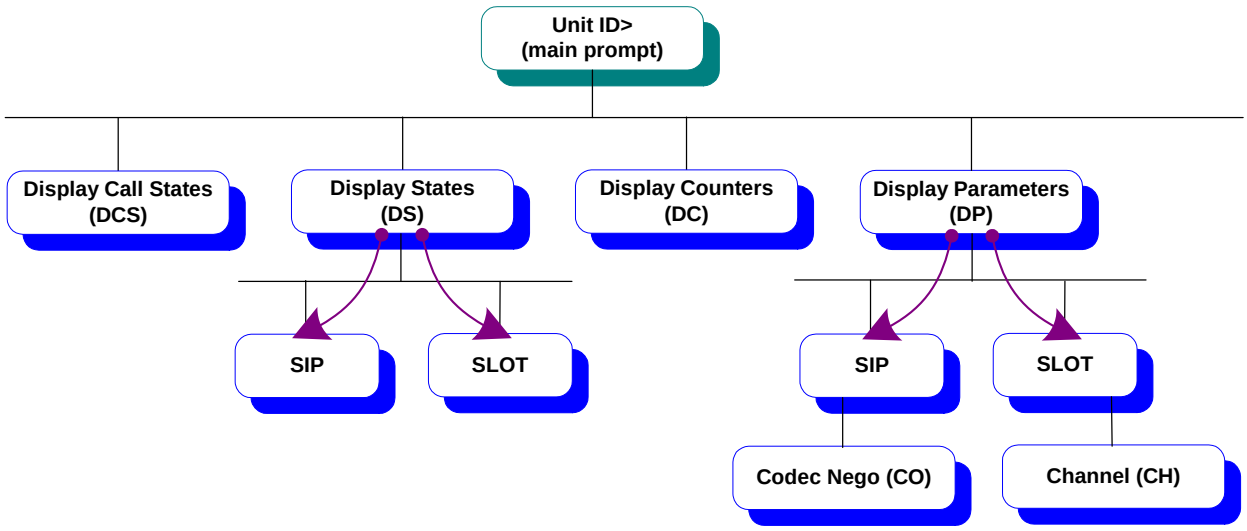

Figure 6-1: Statistics Commands in the CLI Tree for Voice over IP

6.2 Voice Channel Status

Refer to the *Digital Voice* fascicle of this document series for details concerning the **DCS** displays.

DCS example: on SDM-9220 or SDM-9230

```
SDM-92XX>DCS
DISPLAY CALL STATES
Use LEFT and RIGHT arrow keys to change slot.  Press any other key
to exit.
Active Calls:  1  Total Active Calls: 01

----------------------- SLOT 2 : FXS -----------------------------

 # Status  DNIS            Rate        | # Status  DNIS
Rate
01 CONNECT 22              G723  6.4Kx1|02 IDLE
-----------------------------------------------------------------




Use LEFT and RIGHT arrow keys to change slot.  Press any other key
to exit.
```

DCS example: on SDM-9360, SDM-9380 or SDM-9585

```
SDM-93XX>DCS
DISPLAY CALL STATES
Active Calls:  0  Total Active Calls: 00
------------------------- SLOT 1 : T1  -------------------------
 # Status  DNIS            Rate        | # Status  DNIS
Rate
01 IDLE                                |13 OFF
02 IDLE                                |14 OFF
03 IDLE                                |15 OFF
04 IDLE                                |16 OFF
05 OFF                                 |17 OFF
06 OFF                                 |18 OFF
07 OFF                                 |
08 OFF                                 |
09 OFF                                 |
10 OFF                                 |
11 OFF                                 |
12 OFF                                 |
-----------------------------------------------------------------




Use LEFT and RIGHT arrow keys to change slot.  Press any other key
to exit.
```

6.3 SIP Session Status

Refer to the appendix “DISPLAY Command Statistics” on page 9-1 for a detailed explanation of the **DS/SIP** statistics.

DS/SIP example

```
9360-2>DS
DISPLAY STATES
Item (GLOBAL/PORT/REDUNDANCY/SIP/SLOT,def:GLOBAL) ? SIP
SIP> Version.....................................SIP/2.0
SIP> Current operational state..................UP
SIP> Registration status........................Unregistered
SIP> Free SIP ports.............................32
```

6.4 Negotiated Codec Payload

The **DS/SLOT** display includes the *Negotiated Codec Payload*, which is set to an integer value if codec negotiation has taken place.

DS/SLOT example

```
9360>DS
DISPLAY STATES
Item (GLOBAL/PORT/PVC/REDUNDANCY/SIP/SLOT,def:GLOBAL) ? SLOT
SLOT> Slot number (1/2/ALL,def:1) ? 2
SLOT 2>
SLOT 2 - PORT 1>
PORT 200> State.............................IN SYNC
PORT 200> D-Channel state...................UP
PORT 200> Interface.........................BRI-TE

VOICE 201> State............................IDLE
VOICE 201> Protocol.........................G723
VOICE 201> Negotiated Codec Payload.........4
VOICE 201> Last error.......................SE CONNECTION
UNAVAIL->(403)
VOICE 201> Traffic Type.....................VOICE
```

The value of the *Negotiated Codec Payload* is an index that refers to a voice codec or traffic type. The index numbering system is based on that of the SDP media attributes field (**a=rtpmap**).

The following payload type values are used by the NetPerformer:

Value	Voice Codec/Traffic
0	G711-µlaw, Modem Passthru or Fax Passthru
2	G726-32K
4	G723
8	G711-alaw, Modem Passthru or Fax Passthru
18	G729 or G729A
100	ACELP-CN
101	G726-16K
102	G726-24K
103	G726-40K
104	DTMF digits (default)

Table 6-1: NetPerformer payload type values

Refer to the *Digital Voice* fascicle of this document series for details concerning the other statistics in the **DS/SLOT** display.

NOTE: Special considerations concerning Modem Passthru with SIP are included with the discussion of *Modem Passthru* in the *Digital Voice* fascicle of this document series. Fax Passthru is not configurable.

6.5 SIP Counters

The SIP counters provide details concerning the number of request messages, response messages and retries that have been sent or received on the unit.

Refer to page "DC/SIP" on page 9-3 for a detailed explanation of the **DC/SIP** statistics.

DC/SIP example

```
9360-2>DC
DISPLAY COUNTERS
Item (BOOTP/CHANNEL/CONFIG/DNS/IP/NAT/PORT/Q922/Q933/QOS/
REDUNDANCY/
SIP/SLOT/SNMP/TIMEP,def:BOOTP) ? SIP
SIP> Number of SIP request messages Rx.........0
SIP> Number of SIP request messages Tx.........14
SIP> Number of SIP response messages Rx.........0
SIP> Number of SIP response messages Tx.........0
SIP> Number of total transactions..............0
SIP> Number of INVITE requests Rx..............0
SIP> Number of INVITE requests Tx..............0
SIP> Number of ACK requests Rx.................0
SIP> Number of ACK requests Tx.................0
SIP> Number of BYE requests Rx.................0
SIP> Number of BYE requests Tx.................0
SIP> Number of CANCEL requests Rx..............0
SIP> Number of CANCEL requests Tx..............0
SIP> Number of REGISTER requests Rx............0
SIP> Number of REGISTER requests Tx............14
SIP> Number of 1xx class SIP responses Rx.......0
SIP> Number of 1xx class SIP responses Tx.......0
SIP> Number of 2xx class SIP responses Rx.......0
SIP> Number of 2xx class SIP responses Tx.......0
SIP> Number of 3xx class SIP responses Rx.......0
SIP> Number of 3xx class SIP responses Tx.......0
SIP> Number of 4xx class SIP responses Rx.......0
SIP> Number of 4xx class SIP responses Tx.......0
SIP> Number of 5xx class SIP responses Rx.......0
SIP> Number of 5xx class SIP responses Tx.......0
SIP> Number of 6xx class SIP responses Rx.......0
SIP> Number of 6xx class SIP responses Tx.......0
SIP> Number of INVITE retries..................0
SIP> Number of BYE retries.....................0
SIP> Number of CANCEL retries..................0
SIP> Number of REGISTER retries................12
SIP> Number of RESPONSE retries................0
```

6.6 Codec Negotiation Table

The **DP/SIP/CODEC NEGO** menu sequence provides a display of the current values of all parameters in the Codec Negotiation Table.

For parameter details consult "Configuring the NetPerformer for Codec Negotiation" on page 3-14 and the section "CODEC NEGO Parameters" on page 7-13.

DP/SIP/CODEC NEGO example: on SDM-9220 or SDM-9230

```
SDM-92XX>DP
DISPLAY PARAMETERS
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/GLOBAL/IP/IPX/MAP/PORT/PVC/
REDUNDANCY/
SIP/SLOT/USER/ALL,def:SLOT) ? SIP
SIP> (GLOBAL/TIMER/RETRIES/DIGEST/CODEC NEGO/ALL,def:GLOBAL) ?
CODEC NEGO
SIP Codec Negotiation> G729.....................NO
SIP Codec Negotiation> G723.....................YES
SIP Codec Negotiation> G726-16K.................NO
SIP Codec Negotiation> G726-24K.................NO
SIP Codec Negotiation> G726-32K.................NO
SIP Codec Negotiation> G726-40K.................NO
SIP Codec Negotiation> G711 alaw................YES
SIP Codec Negotiation> G711 ulaw................YES
```

DP/SIP/CODEC NEGO example: on SDM-9360, SDM-9380 or SDM-9585

```
SDM93XX>DP
DISPLAY PARAMETERS
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/GLOBAL/IP/IPX/MAP/PORT/PVC/
REDUNDANCY/
SIP/SLOT/USER/ALL,def:SLOT) ? SIP
SIP> (GLOBAL/TIMER/RETRIES/DIGEST/CODEC NEGO/ALL,def:GLOBAL) ?
CODEC NEGO
SIP Codec Negotiation> G711 alaw................YES
SIP Codec Negotiation> G711 ulaw................YES
```

NOTE: As mentioned on "SDM-9360, SDM-9380 and SDM-9585" on page 3-5, The Codec Negotiation Table can be configured to allow negotiation toward **G711 alaw and G711 µlaw only.** For examples of how negotiation is carried out, turn to "Example Scenarios" on page 3-6.

6.7 Voice Channel Parameters

If you intend to use codec negotiation you should view the current values of the *Protocol* and *Packetization selection (Y/N)* parameters on the voice channel, using **DP/SLOT/#/CHANNEL**. Refer to "Configuration Tips" on page 3-16.

DP/SLOT/#/CHANNEL example: G729 set to 2 packets per frame

```
SDM-93XX>DP
DISPLAY PARAMETERS
SETUP
Item (BRIDGE/CALLER ID/CLASS/CUSTOM/GLOBAL/IP/IPX/MAP/PORT/PVC/
REDUNDANCY/
SIP/SLOT/USER/ALL,def:GLOBAL) ? SLOT
SLOT> Slot number (1/2/4,def:1) ? 2
Item (LINK/CHANNEL,def:LINK) ? CHANNEL
SLOT> Port number (1-2/ALL,def:1) ?
VOICE 201> Protocol.............................G729
VOICE 201> DSP packets per frame                12345678
VOICE 201> Packetization selection (Y/N).......NYNNNNNN
...
```

SE/SIP Configuration Parameters

7.1 GLOBAL Parameters

Console	Values	Text-based Config
Administrative status	DISABLE, ENABLE Default value:ENABLE	[npsip] AdminStatus
Default dialstring dest. address	def:000.000.000.000 IP address or domain name, 0 - 64 alphanumeric characters	[npsip] DefaultDialstring-DestAddress
Default dialstring UDP port	1-65535,def:5060	[npsip] DefaultDialstringUdpPort
Force IP source address	IP address or domain name, 0 - 64 alphanumeric characters default: no value	[npsip] ForceIpSourceAddr
Header syntax form	SHORT FORM, FULL FORM Default value:FULL FORM	[npsip] HeaderSyntaxForm
REGISTER ANI digits/ Gateway ID	0-999999999,def:0	[npsip] RegisterAniDigits-GatewayID
DEFAULT ANI digits	MINIMUM LENGTH : 0 MAXIMUM LENGTH : 32 AVAILABLE CHARACTERS : 0/1/2/3/4/5/6/7/8/9/A/B/C/D/*/#	[npsip] DefaultAniDigits
Redirect server	DISABLE, ENABLE def: DISABLE	[npsip] RedirectServer
DTMF payload	104-127,def:104	[npsip] DtmfPayload
DTMF in SIP INFO packets	ALWAYS COMPATIBLE DTMFRELAY, DISABLED def: COMPATIBLE	[npsip] DtmfInInfo

Table 7-1: Global parameters

Console	Values	Text-based Config
Call accounting	NONE RADIUS INGRESS RADIUS EGRESS RADIUS ALWAYS def: NONE	[npsip] CallAccounting
Caller line identity restriction (CLIR)	NORMAL, ALWAYS def: NORMAL	[npsip] CallerLineIdentity-Restriction
Proxy rule	PRIMARY PROXY ONLY BACKUP LOAD BALANCING def: PRIMARY PROXY ONLY	[npsip] ProxyRule

Table 7-1: Global parameters

7.1.1 Administrative status

Console	SNMP	Text-based Config
Administrative status		[npsip] AdminStatus

Table 7-2: Administrative status parameters

Use the *Administrative status* parameter to **ENABLE** or **DISABLE** SIP operations on this NetPerformer unit. When set to **ENABLE**, the SIP client (UAC) and server (UAS) applications are activated.

Values: DISABLE, ENABLE

Default: ENABLE

7.1.2 UDP Port

Console	SNMP	Text-based Config
UDP Port	npSipPort	[npsip] Port

Table 7-3: UDP Port parameters

Defines the particular port that can be used by the SIP application for UDP transport.

Values: 1 - 65535

Default: 5060

7.1.3 Gateway ID

Console	SNMP	Text-based Config
Gateway ID	npsipGatewayID	[npsip] GatewayID

Table 7-4: Gateway ID parameters

Specifies the gateway ID number.

Values: 0 - 999999999

Default: 0

7.1.4 Server group

Console	SNMP	Text-based Config
Server group	npsipServerGroup	[npsip] ServerGroup

Table 7-5: Server group parameters

For use with a Clarent Command Center Database only:
Specifies the server group name. The name you select must match the *Server group* defined in the Clarent Command Center Database for this gateway.

Tip: The *Server group* is often set to the same value as the NetPerformer *Unit ID/ Location*.

Values: Maximum 32-character alphanumeric string

Default: no value

7.1.5 ANI digits

Console	SNMP	Text-based Config
ANI digits	npsipGlobalANIDigits	[npsip] GlobalANIDigits

Table 7-6: ANI digits parameters

Defines the digits that will be prefixed to any Channel ANI string.

Values: Maximum 32-character alphanumeric string, **0-9, A-D, *,** #

Default: no value

7.1.6 DTMF Payload

Console	SNMP	Text-based Config
DTMF Payload	npSipGlobalDTMFPay-load	[npsip] GlobalDTMFPay-load

Table 7-7: DTMF Payload parameters

Defines the SIP RTP payload format used to carry dual-tone multifrequency (DTMF), as defined in RFC-2833. This permits the exchange of the DTMF payload type during session initiation, which is required for functions such as calling card support.

Since SIP is unable to detect DTMF measurement separately, DTMF tones cannot be carried in the INFO packets in any other way.

NOTE: The *DTMF Payload* is required if the unit must interface with a Clarent Class 5 Call Manager (C5CM), for sending the pound sign (#) to return to C5CM functions.

Values: 96 - 127

Default: 104

7.1.7 DTMF in SIP INFO packets

Console	SNMP	Text-based Config
DTMF in SIP INFO packets	npSipGlobalDTMFInInfo	[npsip] GlobalDTMFInInfo

Table 7-8: DTMF in SIP INFO packets parameters

Permits sending the *DTMF payload* in the SIP INFO packets.This is required if the unit must interface with a Clarent Class 5 Call Manager (C5CM), to be able to send the INFO packets to the right location. In this application, the *Session name* (or *Subject*) field of the SIP **INVITE** contains **s=Clarent C5CM**.

DTMF in SIP INFO packets can be set to:

- **ALWAYS:** The NetPerformer always sends DTMF in SIP INFO packets, even if the equipment facing it is not a C5CM.

NOTE: The called unit must be able to accept DTMF in SIP INFO packets.

- **COMPATIBLE:** The NetPerformer sends DTMF in SIP INFO packets only if it detects that the equipment facing it is a C5CM. This value should be acceptable in most cases.
- **DISABLED:** The NetPerformer never sends DTMF in SIP INFO packets. However, if the telephone-event codec is present, DTMF in RTP (RFC-2833) will be generated.

Values: ALWAYS, COMPATIBLE, DISABLED

Default: COMPATIBLE

7.1.8 Redirect Server

Console	SNMP	Text-based Config
Redirect Server	npSipGlobalRedirect-Server	[npsip] GlobalRedirect-Server

Table 7-9: Redirect Server parameters

Enables or disables SIP redirect server functions on this unit. Refer to SIP Redirect Server on page 1.

Values: DISABLE, ENABLE

Default: DISABLE

7.1.9 Call Accounting

Console	SNMP	Text-based Config
Call Accounting	npSipCallAccounting	[npsip] CallAccounting

Table 7-10: Call Accounting parameters

Controls SIP call accounting functions on this unit, in tandem with RADIUS server software and a database of user profiles on a dedicated workstation in the network.

- **NONE:** The NetPerformer sends no accounting records to the RADIUS server. Use this setting to disable call accounting on the unit.
- **RADIUS INGRESS:** The NetPerformer sends accounting records only for calls that come in from the PSTN and go out through SIP. Use this setting to enable call accounting for ingress calls only.
- **RADIUS EGRESS:** The NetPerformer sends accounting records for calls that come in from SIP and go out to the PSTN. Use this setting to enable call accounting for egress calls only.
- **RADIUS ALWAYS:** The NetPerformer sends accounting records for calls that come in from SIP or from the PSTN. Use this setting to enable call accounting for both ingress and egress calls.

NOTE: The format of the billing information that is sent to the RADIUS server uses Cisco attributes. Refer to Call Accounting on page 10.

Values: NONE, RADIUS INGRESS, RADIUS EGRESS, RADIUS ALWAYS

Default: NONE

7.1.10 Call Authentication

Console	SNMP	Text-based Config
Call Authentication	npSipAuthenticateCalls	[npsip] AuthenticateCalls

Table 7-11: Call Authentication parameters

Controls SIP call authentication functions on this unit, in tandem with RADIUS server software and a database of user profiles on a dedicated workstation in the network.

- **NONE:** Disables call authentication on SIP calls
- **RADIUS EGRESS:** Enable call authentication on egress calls, that is, calls that come in from SIP and go out to the PSTN. Successful authentication is required before any such call can go through.

When the NetPerformer receives an **INVITE** and egress authentication is enabled, it creates a PIN from the **TO** field. If *Call Authentication* is set to **RADIUS EGRESS**, the *PIN Length* is requested at the console.

Values: NONE, RADIUS EGRESS

Default: NONE

7.1.11 PIN Length

Console	SNMP	Text-based Config
PIN Length	npSipPinLength	[npsip] PinLength

Table 7-12: PIN Length parameters

Sets the length of the PIN for call authentication on egress calls (*Call Authentication* parameter set to **RADIUS EGRESS**). The NetPerformer takes this number of digits from the end of the **TO** field in the **INVITE** message and uses them as the PIN.

NOTE: The PIN cannot be shorter than this length.

If a PIN is not required, set the *PIN Length* to **0**.

Values: 0 - 255

Default: 0

7.1.12 Caller Line Identity Restriction

Console	SNMP	Text-based Config
Caller Line Identity Restriction	npSipCallLineIdentity-Restriction	[npsip] SipCallLineIdentit-yRes-triction

Table 7-13: Caller Line Identity Restriction parameters

Determines whether the caller's personal identification will be displayed on the remote site telephone. If a call is restricted, the *P-Assert* setting (**P-Asserted-Identity**) is set to private (**Privacy: id**) when the call is forwarded from the unit.

- **NORMAL:** The unit detects the *P-Assert* setting in the ISDN/QSIG **SETUP** message, and forwards this value with the call. If the call is restricted, the *P-Assert* is set to private status. Otherwise, the call goes through with no identity restriction.
- **ALWAYS:** All calls forwarded from this unit are forced to private status, even if the original ISDN/QSIG **SETUP** message did not have a restricted setting. In other words, the NetPerformer configuration overrides the initial ISDN/QSIG call setup settings received on the PCM side, and the *P-Assert* is always set (**Privacy: id**) in the SIP **INVITE**.

NOTE: **The *Caller Line Identity Restriction* parameter affects only those calls that are received on the PCM side (ISDN-PRI) and sent out via SIP.** Calls going in the other direction, that is, ingressed from IP/SIP and egressed to PCM, are ***not*** affected by the NetPerformer CLIR setting.

Values: NORMAL, ALWAYS

Default: NORMAL

7.2 TIMER Parameters

Console	Values	Text-based Config
T1: round-trip time estimate (ms)	500-2000,def:500	[npsip] TimerT1-ms
T2: max. retransmit interval (ms)	1000-10000,def:4000	[npsip] TimerT2-ms
T4: wait time for ACK or response retrans. (ms)	1000-5000,def:5000	[npsip] TimerT4-ms
Timer B: INVITE transaction timeout (ms)	10000-32000,def:32000	[npsip] TimerB-ms

Table 7-14: TIMER parameters

7.2.1 Resend INVITE

Console	SNMP	Text-based Config
Resend INVITE	npSipUACfgTimerInvite	[npsip] UACfgTimerProv

Table 7-15: Resend INVITE parameters

Specifies the time, in milliseconds, that the UAC will wait between **INVITE** retries if no response is received. It will send a **CANCEL** after the maximum number of retries has been issued, as configured with the SIP Retries *INVITE* parameter.

Values: 1 - 1000

Default: 1

7.2.2 Receiving ACK

Console	SNMP	Text-based Config
Receiving ACK	npSipUACfgTimerAck	[npsip] UACfgTimerAck

Table 7-16: Receiving ACK parameters

Specifies the time, in milliseconds, that the UAC will wait to receive an **ACK** confirmation indicating that a session has been established.

Values: 1 - 1000

Default: 1

7.2.3 Disconnect (BYE or CANCEL)

Console	SNMP	Text-based Config
Disconnect (BYE or CANCEL)	npSipUACfgTimerDisconnect	[npsip] UACfgTimerDisconnect

Table 7-17: Disconnect parameters

Specifies the time, in milliseconds, that the UAC will wait to receive a **BYE** confirmation indicating that a session is disconnected.

Values: 1 - 1000

Default: 1

7.2.4 Registration duration

Console	SNMP	Text-based Config
Registration duration	npSipUACfgTimerReRegister	[npsip] UACfgTimerReRegister

Table 7-18: Registration duration parameters

Specifies the duration of time, in seconds, that the UAC would like its registration to remain valid. This is the maximum amount of time that the registration can last, after which a retry must be made. Three tries can be made to connect to the SIP registration server.

NOTE: The value of the *Registration duration* parameter is included in the *Expires* header of the **REGISTER** request.

Values: 1 - 100000000

Default: 20

7.3 AUTHENTICATION Parameters

Console	Values	Text-based Config
Authentication type	NONE RADIUS EGRESS SIP CHALLENGE def: NONE	[npsip] Authentication-Type
Radius PIN length	0-255,def:0	[npsip] RadiusPinLength
Challenge on INVITE	DISABLE, ENABLE def: DISABLE	[npsip] ChallengeOnInvite
Challenge on BYE	DISABLE, ENABLE def: DISABLE	[npsip] ChallengeOnBye
Challenge on OPTIONS	DISABLE, ENABLE def: DISABLE	[npsip] ChallengeOnOptions
Challenge username	MINIMUM LENGTH : 0 MAXIMUM LENGTH : 32 AVAILABLE CHARACTERS : ANY	[npsip] ChallengeUserName
Challenge password	MINIMUM LENGTH : 0 MAXIMUM LENGTH : 32 AVAILABLE CHARACTERS : ANY	[npsip] ChallengePassword

Table 7-19: AUTHENTICATION parameters

7.3.1 UserName

Console	SNMP	Text-based Config
UserName	npsipDigestUsername	[npsip] DigestUsername

Table 7-20: UserName parameters

Specifies the Digest username for authentication of the SIP session. SIP digest is used to carry out the authentication exchange between client (UAC) and server (UAS). The *Authorization* header includes the value of *UserName* in a request to the server (UAS).

Values: Maximum 32-character alphanumeric string (upper and lowercase)

Default: no value

7.3.2 UserPassword

Console	SNMP	Text-based Config
UserPassword	*not available*	[npsip] DigestUserPass-word

Table 7-21: UserPassword parameters

Specifies the Digest password for authentication of the SIP session. The value of *UserPassword* is encrypted and included in the *Authorization* header in a response field along with the encrypted username.

Values: Maximum 32-character alphanumeric string

Default: no value

7.4 CODEC NEGO Parameters

Caution: Refer to Configuration Tips on page 16 for important considerations when making changes to the codec negotiation parameters.

Console	Values	Text-based Config
G729	NO,YES def: NO	[npsip] NegotiateG729
G723	NO,YES def: NO	[npsip] NegotiateG723
G726-16K	NO,YES def: NO	[npsip] NegotiateG726-16k
G726-24K	NO,YES def: NO	[npsip] NegotiateG726-24k
G726-32K	NO,YES def: NO	[npsip] NegotiateG726-32k
G726-40K	NO,YES def: NO	[npsip] NegotiateG726-40k
G711 alaw	NO,YES def: NO	[npsip] NegotiateG711-alaw
G711 ulaw	NO,YES def: NO	[npsip] NegotiateG711-ulaw

Table 7-22: CODEC NEGO parameters

7.4.1 G729

Console	SNMP	Text-based Config
G729	npSipCodecNegoG729	[npsip] CodecNegoG729

Table 7-23: G729 parameters

For SDM-9220 or SDM-9230 only.
Controls the addition of the G729 codec to the Codec Negotiation Table.

NOTE: G729A is included with the G729 codec.

- **YES:** Any voice channel on this unit can accept and load the G729 codec through codec negotiation. Also, an **INVITE** from this unit will include G729 in the media attributes of the SDP message body.
- **NO:** Negotiation toward G729 is not permitted on any voice channel on this unit.

Values: NO, YES

Default: NO

7.4.2 G723

Console	SNMP	Text-based Config
G723	npSipCodecNegoG723	[npsip] CodecNegoG723

Table 7-24: G723 parameters

For SDM-9220 or SDM-9230 only.
Controls the addition of the G723 codec to the Codec Negotiation Table.

- **YES:** Any voice channel on this unit can accept and load the G723 codec through codec negotiation. Also, an **INVITE** from this unit will include G723 in the media attributes of the SDP message body.
- **NO:** Negotiation toward G723 is not permitted on any voice channel on this unit.

Values: NO, YES

Default: NO

7.4.3 G726-16K

Console	SNMP	Text-based Config
G726-16K	npSipCodecNegoG72616k	[npsip] CodecNegoG72616k

Table 7-25: G726-16K parameters

For SDM-9220 or SDM-9230 only.
Controls the addition of the G726-16K codec to the Codec Negotiation Table.

- **YES:** Any voice channel on this unit can accept and load the G726-16K codec through codec negotiation. Also, an **INVITE** from this unit will include G726-16K in the media attributes of the SDP message body.
- **NO:** Negotiation toward G726-16K is not permitted on any voice channel on this unit.

Values: NO, YES

Default: NO

7.4.4 G726-24K

Console	SNMP	Text-based Config
G726-24K	npSipCodecNegoG72624k	[npsip] CodecNegoG72624k

Table 7-26: G726-24K parameters

For SDM-9220 or SDM-9230 only.
Controls the addition of the G726-24K codec to the Codec Negotiation Table.

- **YES:** Any voice channel on this unit can accept and load the G726-24K codec through codec negotiation. Also, an **INVITE** from this unit will include G726-24K in the media attributes of the SDP message body.
- **NO:** Negotiation toward G726-24K is not permitted on any voice channel on this unit.

Values: NO, YES

Default: NO

7.4.5 G726-32K

Console	SNMP	Text-based Config
G726-32K	npSipCodecNegoG72632k	[npsip] CodecNegoG72632k

Table 7-27: G726-32K parameters

For SDM-9220 or SDM-9230 only.
Controls the addition of the G726-32K codec to the Codec Negotiation Table.

- **YES:** Any voice channel on this unit can accept and load the G726-32K codec through codec negotiation. Also, an **INVITE** from this unit will include G726-32K in the media attributes of the SDP message body.
- **NO:** Negotiation toward G726-32K is not permitted on any voice channel on this unit.

Values: NO, YES

Default: NO

7.4.6 G726-40K

Console	SNMP	Text-based Config
G726-40K	npSipCodecNegoG72640k	[npsip] CodecNegoG72640k

Table 7-28: G726-40K parameters

For SDM-9220 or SDM-9230 only.

Controls the addition of the G726-40K codec to the Codec Negotiation Table.

- **YES:** Any voice channel on this unit can accept and load the G726-40K codec through codec negotiation. Also, an **INVITE** from this unit will include G726-40K in the media attributes of the SDP message body.
- **NO:** Negotiation toward G726-40K is not permitted on any voice channel on this unit.

Values: NO, YES

Default: NO

7.4.7 G711 alaw

Console	SNMP	Text-based Config
G711 alaw	npSipCodecNegoG711A-law	[npsip] CodecNegoG711Alaw

Table 7-29: G711 parameters

Controls the addition of the G711 alaw codec to the Codec Negotiation Table.

- **YES:** Any voice channel on this unit can accept and load the G711 alaw codec through codec negotiation. Also, an **INVITE** from this unit will include G711 alaw in the media attributes of the SDP message body.
- **NO:** Negotiation toward G711 alaw is not permitted on any voice channel on this unit.

Values: NO, YES

Default: NO

7.4.8 G711 ulaw

Console	SNMP	Text-based Config
G711 ulaw	npSipCodecNegoG711U-law	[npsip] CodecNegoG711Ulaw

Table 7-30: G711 ulaw parameters

Controls the addition of the G711 µlaw codec to the Codec Negotiation Table.

- **YES:** Any voice channel on this unit can accept and load the G711 µlaw codec through codec negotiation. Also, an **INVITE** from this unit will include G711 µlaw in the media attributes of the SDP message body.
- **NO:** Negotiation toward G711 µlaw is not permitted on any voice channel on this unit.

Values: NO, YES

Default: NO

7.5 PROXY Parameters

Console	Values	Text-based Config
SIP Proxy entry number	1-2,def:1	[npsipProxy #]
Enable registration	NO YES Def: NO	[npsipProxy #] EnableRegistration
Proxy server address	MINIMUM LENGTH : 0 MAXIMUM LENGTH : 64 AVAILABLE CHARACTERS : A/B/C/D/E/F/G/H/I/J/K/L/M/N/O/P/Q/R/S/T/U/V/W/X/Y/Z/0/1/2 /3/4/5/6/7/8/9/-/!/&/*/(/)/_/-/+/=/>/'/</|/?/$/%/;/./:/,/	[npsipProxy #] Proxy-ServerAddr
Proxy server UDP port	1-65535,def:5060	[npsipProxy #] Proxy-ServerUdpPort
REGISTER expires (s)	20-100000000,def:20	[npsipProxy #] Register-Expires-s
Proxy authentication username	MINIMUM LENGTH : 0 MAXIMUM LENGTH : 32 AVAILABLE CHARACTERS : ANY	[npsipProxy #] ProxyAuthUsername
Proxy authentication password	MINIMUM LENGTH : 0 MAXIMUM LENGTH : 32 AVAILABLE CHARACTERS : ANY	[npsipProxy #] ProxyAuthPassword

Table 7-31: Proxy parameters

7.5.1 SIP Proxy entry number

Console	SNMP	Text-based Config
SIP Proxy entry number	npsipProxyEntry, npsipProxyIndex	[npsipProxy #]

Table 7-32: SIP Proxy entry number parameters

Enter the number of the SIP Proxy unit you want to configure on the console command line. For SNMP, select the *npsipProxyEntry* table and look under the *npsipProxyIndex* for the desired PVC.

Once you select a SIP Proxy unit, the **SIP PROXY** number is displayed thereafter at the

beginning of each line from the console.

Values: 1 - 2

Default: 1

7.5.2 Enable registration

Console	SNMP	Text-based Config
Enable registration		[npsipProxy #] EnableRegistration

Table 7-33: Enable registration parameters

Enables or disables registration of this SIP proxy unit with the registration server.

- **ENABLE:** Permits SIP registration on the NetPerformer.

  This setting is required if the unit must interface with a Clarent Class 5 Call Manager (C5CM).

- **DISABLE:** SIP registration cannot take place. An **INVITE** message from this unit will not be forwarded via a registration server to the called party.

Values: DISABLE, ENABLE

Default: DISABLE

7.5.3 Proxy server address

Console	SNMP	Text-based Config
Proxy server address		[npsipProxy #] Proxy-ServerAddr

Table 7-34: Proxy server address parameters

Specifies the address of this proxy server. The value can be:

- An IP address: 4-byte value in dotted decimal notation, with a maximum value of 255 for each byte
- A host name, for example:

  ```
  SIP Global> Proxy server address (def: ) ? sip-proxy.acme.com.
  ```

NOTE: To accept a host name, a *DNS server address* must be configured on the unit. For details, refer to the *LAN Connection and IP Networks* fascicle of this document series.

If you leave the *Proxy server address* at its default value (**0.0.0.0**) it is considered not

defined, and **calls cannot be routed via this proxy server**. You can, however, place calls from this unit directly to another NetPerformer unit with SIP VoIP **using the DIALIP Map type**. Refer to "Setting up the Voice Mapping Table" on page 2-10).

Values: 0.0.0.0 - 255.255.255.255, or maximum 16-character alpha-numeric string

Default: 0.0.0.0

7.5.4 Proxy server UDP Port

Console	SNMP	Text-based Config
Proxy server UDP port		[npsipProxy #] Proxy-ServerUdpPort

Table 7-35: Proxy server UDP Port parameters

Defines the particular port that can be used by this SIP proxy unit for UDP transport.

Values: 1 - 65535

Default: 5060

7.5.5 REGISTER expires (s)

Console	SNMP	Text-based Config
REGISTER expires (s)		[npsipProxy #] Register-Expires-s

Table 7-36: Register expires parameters

Values:

Default:

7.5.6 Proxy authentication username

Console	SNMP	Text-based Config
Proxy authentication username		[npsipProxy #] ProxyAu-thUsername

Table 7-37: Proxy authentication parameters

Specifies the username for authentication of the SIP session on this SIP proxy unit.

Values: Maximum 32-character alphanumeric string (upper and low-ercase)

Default: no value

7.5.7 Proxy authentication password

Console	SNMP	Text-based Config
Proxy authentication password		[npsipProxy #] ProxyAuthPassword

Table 7-38: Proxy authentication password parameters

Specifies the password for authentication of the SIP session on this SIP proxy unit.

Values: Maximum 32-character alphanumeric string

Default: no value

SE/MAP Configuration Parameters

8.1 DIALSTRING Map Type

Many of the parameters detailed in this section are also listed when the MAP entry is configured to another *Map type*.

8.1.1 Operation

Console	SNMP	Text-based Config
Operation	*not available*	*not applicable*

Table 8-1: Operation parameters

Specifies the type of operation you would like to execute at the console:

- **ADD:** To add a new MAP entry to the Voice Mapping Table
- **MODIFY:** To change an existing MAP entry
- **DELETE:** To delete a MAP entry from the Voice Mapping Table.

Values: ADD, MODIFY, DELETE

Default: ADD

8.1.2 Map type

Console	SNMP	Text-based Config
Map type	*not available*	[map] OutputType

Table 8-2: Map type parameters

Specifies the way the called party will be accessed:

- **DIALSTRING:** The user enters a specific digits string.
  - For an Ingress call, the call request is sent via the SIP proxy server using the *Proxy server address* specified in the SIP global parameters (see "GLOBAL Parameters" on page 7-2).
  - A **DIALSTRING** Map entry can also be used to egress a call that comes in from SIP and goes out to the PSTN.
- **DIALIP:** The user enters a specific digits string, and the call request is sent to a specific IP address.
- **SUPERMAP:** The user does not need to enter a digits string.
  - Select this value when no specific destination can be defined using either **DIALSTRING** or **DIALIP** Map entries, and where all other destinations should be attempted to set up the call.
  - All digits strings defined in the Voice Mapping Table are attempted on the *Egress hunt group ports* specified in the MAP entry, until an available destination is found

- The SIP *Proxy server address* is also required (see "Proxy server address" on page 7-18).

Values: DIALSTRING, DIALIP, SUPERMAP

Default: DIALSTRING

8.1.3 Entry digits

Console	SNMP	Text-based Config
Entry digits	*not available*	[map] MappingEntry

Table 8-3: Entry parameters

NOTE: *For DIALSTRING and DIALIP Map type only.*
Specifies the digits string that the user must enter to activate call setup using this MAP entry.

Values: Maximum 19-digit numeric string: 0 - 9

Default: no value

8.1.4 Digits string length

Console	SNMP	Text-based Config
Digits string length	*not available*	[map] MaxCharacters

Table 8-4: Digits string length parameters

For DIALSTRING and DIALIP Map type only.
The maximum number of digits that can be dialed by the user. This includes the speed dial number and extended digits, but not the *Ingress/Egress prepend string* or *Ingress/Egress append string*.

Example:

- A Map entry has the *Entry digits* defined as **1234** and the *Digits string length* defined as **6**
- The user dials **1234**
- The NetPerformer waits for 2 more digits (e.g. **56**). If the user dials them, call setup continues immediately.

  The effect of entering the last two numbers is the same as entering the pound sign (#).
- The *Dial timer* expires if no more digits are entered. Call setup continues, using this Map entry.

Values: Minimum: length of the Entry digits value
Maximum: 40

Default: Automatically generated based on the Map type and Entry digits values

8.1.5 Egress hunt group pattern

Console	SNMP	Text-based Config
Egress hunt group pattern	*not available*	[map] HuntMode

Table 8-5: Egress hunt group pattern parameters

Specifies the type of hunt process to use when placing an egress call. The *Egress hunt group pattern* can be set to:

- **SEQUENTIAL:** Carries out an ascending sequential search of all voice channels specified by the *Egress hunt group ports* parameter, always beginning with the first port defined in the sequence.
- **ROTARY:** Carries out an ascending sequential search of the *Egress hunt group ports*, beginning with the port after the last port investigated in the previous hunt.
- **NONE:** No hunt process will be used. This setting is suitable for outgoing calls only. Incoming calls will fail with the alarm message **SIP not available**.

  The hunt process continues until either:

  - An available port is found, in which case the NetPerformer proceeds with call connection, ***or***
  - The first port of the hunt process is reached again, in which case the NetPerformer produces a busy signal.

Values: SEQUENTIAL, ROTARY, NONE

Default: NONE

8.1.6 Egress hunt group ports

Console	SNMP	Text-based Config
Egress hunt group ports	*not available*	[map] HuntGroup

Table 8-6: Egress hunt group ports parameters

Specifies the voice channels that will be searched during the hunt process on an egress call (*Egress hunt group pattern* set to **SEQUENTIAL** or **ROTARY**). This may be a series of port numbers, e.g. **101,102,203**, a range of port numbers, e.g. **315-322**, or both, e.g. 1**01,203-306**

Values: Series and/or range of port numbers

Default: no value

8.1.7 Strip prefix number of digits

Console	SNMP	Text-based Config
Strip prefix number of digits	*not available*	[map] StripPrefixNumber

Table 8-7: Strip prefix number of digits parameters

Defines the number of digits that are deleted from the beginning of the *Entry digits* before proceeding with call setup.

- Use the letter **I** (for ingress) to identify the number of digits deleted on ingress calls
- Use the letter **E** (for egress) to identify the number of digits deleted on egress calls.
- The **I** and **E** values can be concatenated, separated by a space or a slash in the rule definition string.

Examples of valid values for *Strip prefix number of digits* are **I3E4** and **I3 E4**, both of which remove 3 digits on the ingress side and 4 digits on the egress side. For further information, refer to "Ingress and Egress Dial Rule Definitions" on page 2-16.

Values: Maximum 10-character string: 0 - 9, I, E, / (slash), space

Default: I0 E0

8.1.8 Ingress/Egress prepend string

Console	SNMP	Text-based Config
Ingress/Egress prepend string	*not available*	[map] PrependString

Table 8-8: Ingress/Egress prepend string parameters

Defines the digits that are added at the beginning of the *Entry digits* before proceeding

with call setup.

- Use the letter **I** (for ingress) to identify the number of digits added on ingress calls
- Use the letter **E** (for egress) to identify the number of digits added on egress calls
- Use the **,** (comma) to add a dial delay to the digits string
- The **I** and **E** values can be concatenated, separated by a space or a slash in the rule definition string
- Enter **NONE** if no prepend string is required.

Examples of valid values for *Ingress/Egress prepend string* are **I1E604** and **I1 E604**, both of which add the dial digit **1** on the ingress side and the dial digits **604** on the egress side. For further information, refer to "Ingress and Egress Dial Rule Definitions" on page 2-16.

Values: Maximum 10-character string: 0 - 9, I, E, space, , (comma), / (slash), NONE

Default: no value

8.1.9 Ingress/Egress append string

Console	SNMP	Text-based Config
Ingress/Egress append string	*not available*	[map] AppendString

Table 8-9: Ingress/Egress append string parameters

Defines the digits that are added at the end of the *Entry digits* before proceeding with call setup.

- Use the letter **I** (for ingress) to identify the number of digits added on ingress calls
- Use the letter **E** (for egress) to identify the number of digits added on egress calls
- Use the **,** (comma) to add a dial delay to the digits string
- Use the **!** (exclamation mark) to allow user-dialed digits to be added to the append string. During call setup the **!** is replaced by the digits dialed by the user.
- The **I** and **E** values can be concatenated, separated by a space or a slash in the rule definition string.
- Enter **NONE** if no append string is required.

Examples of valid values for *Ingress/Egress prepend string* are **I50E8** and **I50 E8**, both of which add the dial digits **50** on the ingress side and the dial digit **8** on the egress side. For further information, refer to "Ingress and Egress Dial Rule Definitions" on page 2-16.

Values: Maximum 10-character string: 0 - 9, I, E, space, (comma), / (slash), ! (exclamation mark), NONE

Default: no value

8.1.10 Add another map entry

Console	SNMP	Text-based Config
Add another map entry	*not available*	*not applicable*

Table 8-10: Add another map entry parameters

Determines whether parameter prompts for another MAP entry will be provided at the console. If you select **NO**, the NetPerformer will save the MAP entry you have just defined, and display the message **Saving map entry...** at the console.

Values: NO, YES

Default: NO

8.2 DIALIP Map Type

DIALIP parameters that are common to other *Map types* are listed under "DIALSTRING Map Type" on page 8-2.

8.2.1 Enter an IP address

Console	SNMP	Text-based Config
Enter an IP address	*not available*	[map] IpAddress

Table 8-11: Enter an IP address parameters

For DIALIP Map type only.
Defines the IP address to which the call attempt (**INVITE** message) will be directed when the user enters the *Entry digits* for this MAP entry.

Values: 0.0.0.0 - 255.255.255.255

Default: 0.0.0.0

8.3 SUPERMAP Map Type

All **SUPERMAP** parameters are common to other *Map types*, and are listed under "DIALSTRING Map Type" on page 8-2 and "DIALIP Map Type" on page 8-8, above.

DISPLAY Command Statistics

9.1 DS/SIP

9.1.1 Version

Console	SNMP
Version	sipStatsVersion

Displays the SIP version supported by this NetPerformer unit. The value reflects the SIP version information contained in SIP messages generated by this NetPerformer, e.g. SIP/2.0.

9.1.2 Current operational state

Console	SNMP
Current operational state	sipStatsCurrentOperational

Displays the current operational state of the SIP application:

- **UP:** The application is operating normally, and is processing SIP requests and responses
- **DISABLE:** The application is currently unable to process SIP messages

9.1.3 Registration status

Console	SNMP
Registration status	sipStatsRegistration

Displays the current registration status of the UA:

- **Unregistered:** The unit is not registered with a registration server.
- **Registered:** The unit is currently registered with a registration server.

9.2 DC/SIP

9.2.1 Number of SIP request messages Rx

Console	SNMP
Number of SIP request messages Rx	sipSummaryInRequests

The total number of SIP request messages that have been received by this NetPerformer unit.

Request messages are initiated by the SIP client application, or User Agent Client (UAC).

9.2.2 Number of SIP request messages Tx

Console	SNMP
Number of SIP request messages Tx	sipSummaryOutRequests

The total number of SIP request messages that have been sent by this NetPerformer unit.

9.2.3 Number of SIP response messages Rx

Console	SNMP
Number of SIP response messages Rx	sipSummaryInResponses

The total number of SIP response messages that have been received by this NetPerformer unit.

Responses are generated by the SIP server application, or User Agent Server (UAS).

9.2.4 Number of SIP response messages Tx

Console	SNMP
Number of SIP response messages Tx	sipSummaryOutResponses

The total number of SIP response messages that have been sent by this NetPerformer unit.

9.2.5 Number of total transactions

Console	SNMP
Number of total transactions	sipSummaryTotalTransactions

The total number of transactions that have occurred on this NetPerformer unit.

9.2.6 Number of INVITE requests Rx

Console	SNMP
Number of INVITE requests Rx	sipStatsInviteIns

The number of SIP **INVITE** request messages that have been received by this NetPerformer unit.

INVITE messages are used to set up a SIP session. During message exchange, the calling party acts like a SIP client (UAC), and the called party acts like a SIP server (UAS). **INVITE**, **200 OK** and **ACK** messages must be exchanged between the UAC and UAS to complete session initiation.

9.2.7 Number of INVITE requests Tx

Console	SNMP
Number of INVITE requests Tx	sipStatsInviteOuts

The number of SIP **INVITE** request messages that have been sent by this NetPerformer unit.

9.2.8 Number of ACK requests Rx

Console	SNMP
Number of ACK requests Rx	sipStatsAcksIns

The number of SIP **ACK** request messages that have been received by this NetPerformer unit.

During session setup, the calling party (UAC) sends an **ACK** to confirm it can support the type of session that was proposed by the called party (UAS) in the **180 Ringing** or **200 OK** message.

9.2.9 Number of ACK requests Tx

Console	SNMP
Number of ACK requests Tx	sipStatsAcksOuts

The number of SIP **ACK** request messages that have been sent by this NetPerformer unit.

9.2.10 Number of BYE requests Rx

Console	SNMP
Number of BYE requests Rx	sipStatsByeIns

The number of SIP **BYE** request messages that have been received by this NetPerformer unit.

BYE messages are used to tear down a SIP session. During message exchange, the calling

party acts like a SIP server (UAS), and the called party acts like a SIP client (UAC).

9.2.11 Number of BYE requests Tx

Console	SNMP
Number of BYE requests Tx	sipStatsByeOuts

The number of SIP **BYE** request messages that have been sent by this NetPerformer unit.

9.2.12 Number of CANCEL requests Rx

Console	SNMP
Number of CANCEL requests Rx	sipStatsCancelIns

The number of SIP **CANCEL** request messages that have been received by this NetPerformer unit.

CANCEL messages are used to terminate pending searches or call attempts. The UAC will issue a **CANCEL** to stop a call attempt that it initiated earlier.

9.2.13 Number of CANCEL requests Tx

Console	SNMP
Number of CANCEL requests Tx	sipStatsCancelOuts

The number of SIP **CANCEL** request messages that have been sent by this NetPerformer unit.

9.2.14 Number of REGISTER requests Rx

Console	SNMP
Number of REGISTER requests Rx	sipStatsRegisterIns

The number of SIP **REGISTER** request messages that have been received by this NetPerformer unit.

REGISTER messages provide the current IP address of the UA to the SIP network. They also list all Universal Resource Locators (URLs) for which the UA can receive calls.

9.2.15 Number of REGISTER requests Tx

Console	SNMP
Number of REGISTER requests Tx	sipStatsRegisterOuts

The number of SIP **REGISTER** request messages that have been sent by this NetPerformer unit.

9.2.16 Number of 1xx class SIP responses Rx

Console	SNMP
Number of 1xx class SIP responses Rx	sipStatsInfoClassIns

The number of SIP response messages received by this unit that belong to the 1xx *Informational* (or *Provisional*) response class.

An *Informational* response indicates how the call is progressing. The first informational response confirms receipt of the **INVITE**, e.g. **100 Trying**, **180 Ringing**.

9.2.17 Number of 1xx class SIP responses Tx

Console	SNMP
Number of 1xx class SIP responses Tx	sipStatsInfoClassOuts

The number of SIP response messages sent by this unit that belong to the 1xx *Informational or Provisional* response class.

9.2.18 Number of 2xx class SIP responses Rx

Console	SNMP
Number of 2xx class SIP responses Rx	sipStatsSuccessClassIns

The number of SIP response messages received by this unit that belong to the 2xx *Success* response class.

A *Success* response indicates that the request has succeeded, e.g. **200 OK**.

9.2.19 Number of 2xx class SIP responses Tx

Console	SNMP
Number of 2xx class SIP responses Tx	sipStatsSuccessClassOuts

The number of SIP response messages sent by this unit that belong to the 2xx *Success* response class.

9.2.20 Number of 3xx class SIP responses Rx

Console	SNMP
Number of 3xx class SIP responses Rx	sipStatsRedirClassIns

The number of SIP response messages received by this unit that belong to the 3xx *Redirection* response class.

A *Redirection* response is sent by a SIP Redirect server in response to an **INVITE**, e.g. **301 Moved Permanently**, **302 Moved Temporarily**. It includes the possible locations where the UAC can retry its request.

9.2.21 Number of 3xx class SIP responses Tx

Console	SNMP
Number of 3xx class SIP responses Tx	sipStatsRedirClassOuts

The number of SIP response messages sent by this unit that belong to the 3xx *Redirection* response class.

9.2.22 Number of 4xx class SIP responses Rx

Console	SNMP
Number of 4xx class SIP responses Rx	sipStatsReqFailClassIns

The number of SIP response messages received by this unit that belong to the 4xx *Client error* response class.

A *Client error* response indicates that the request has failed due to an error on the part of the UAC. Examples are:

- **400 Bad Request:** Required headers are probably missing
- **401 Unauthorized:** Authentication information is required by the UAS
- **404 Not Found:** The end user is not signed on
- **415 Unsupported Media Type:** The codec could not be negotiated.

9.2.23 Number of 4xx class SIP responses Tx

Console	SNMP
Number of 4xx class SIP responses Tx	sipStatsReqFailClassOuts

The number of SIP response messages sent by this unit that belong to the 4xx *Client error* response class.

9.2.24 Number of 5xx class SIP responses Rx

Console	SNMP
Number of 5xx class SIP responses Rx	sipStatsServerFailClassIns

The number of SIP response messages received by this unit that belong to the 5xx *Server error* response class.

A *Server error* response indicates that the request has failed due to an error on the part of the UAS. The request itself is error-free, e.g. **501 Not Implemented** (the request contains an unknown method), **500 Server Internal Error**, **503 Service Unavailable**.

9.2.25 Number of 5xx class SIP responses Tx

Console	SNMP
Number of 5xx class SIP responses Tx	sipStatsServerFailClassOuts

The number of SIP response messages sent by this unit that belong to the 5xx *Server error* response class.

9.2.26 Number of 6xx class SIP responses Rx

Console	SNMP
Number of 6xx class SIP responses Rx	sipStatsGlobalFailClassIns

The number of SIP response messages received by this unit that belong to the 6xx *Global error* response class.

A *Global error* response indicates that the request has failed and will fail on any other server, as well. e.g. **600 Busy Everywhere**, **603 Decline**, **606 Not Acceptable**.

9.2.27 Number of 6xx class SIP responses Tx

Console	SNMP
Number of 6xx class SIP responses Tx	sipStatsGlobalFailClassOuts

The number of SIP response messages sent by this unit that belong to the 6xx *Global error* response class.

9.2.28 Number of INVITE retries

Console	SNMP
Number of INVITE retries	sipStatsRetryInvites

The number of times that this NetPerformer unit has retried sending an **INVITE** request message.

9.2.29 Number of BYE retries

Console	SNMP
Number of BYE retries	sipStatsRetryByes

The number of times that this NetPerformer unit has retried sending an **BYE** request message.

9.2.30 Number of CANCEL retries

Console	SNMP
Number of CANCEL retries	sipStatsRetryCancels

The number of times that this NetPerformer unit has retried sending an **CANCEL** request message.

9.2.31 Number of REGISTER retries

Console	SNMP
Number of REGISTER retries	sipStatsRetryRegisters

The number of times that this NetPerformer unit has retried sending an **REGISTER** request message.

9.2.32 Number of RESPONSE retries

Console	SNMP
Number of RESPONSE retries	sipStatsRetryResponses

The number of times that this NetPerformer unit has retried sending a **200 OK** or **ERROR** response message while expecting an **ACK** in return.

Index

A

Add another map entry prompt 8-7
Administrative status parameter 7-3
ANI digits parameter 7-4
Authentication 1-9
AUTHENTICATION parameters 2-7
Authentication parameters 7-11

B

Billing signals 1-9

C

Call accounting 1-9
Call Accounting parameter 7-6
Call authentication 1-9
Call Authentication parameter 7-7
Call Manager 1-19
Call negotiation, using Redirect server 5-3
Caller Line Identity Restriction 7-8
Clarent Connect 1-19
Clarent Gateway 1-19
Clearmode 1-14
CLIR 1-15, 7-8
CODEC NEGO parameters 3-14, 7-13
Codec Negotiation 3-1
  codec selection 3-3, 3-8
  configuration 3-14
  configuration tips 3-16
  display of negotiated codec payload 6-5
  effect of all factors 3-12
  effects of product type 3-5
  examples 3-6
  limitations 3-4
  procedure 3-3
  viewing the table 6-8
Command Center 1-18
Configuration 2-3
  AUTHENTICATION parameters 2-7
  Codec Negotiation 3-14
  DIALIP Map Type 2-12
  DIALSTRING Map Type 2-11
  Gateway versus Endpoint 2-19
  GLOBAL parameters 2-4
  Ingress/Egress dial rules 2-16
  MAP parameters 2-10, 2-11, 2-14
  PROXY parameters 2-8
  SE/MAP parameters 8-1
  SE/SIP parameters 7-1
  SIP Hairpin 4-6
  SIP Redirect Server 5-6
  SUPERMAP Map Type 2-13
  TIMER parameters 2-6
Connection
  multipoint, without proxy server 1-5
  point-to-point 1-3
  SIP proxy server 1-4
Current operational state statistic 9-2

D

Database 1-18
DC/SIP command 6-7
DCS command 6-3
Dial rules 2-16
DIALIP Map Type 2-12
  for SIP Hairpin 4-6
  parameters 8-8
DIALSTRING Map Type 2-11
  parameters 8-2
Digit transport, out-of-band 1-15
Digits string length parameter 8-3
Disconnect (BYE or CANCEL) parameter 7-10
Display commands 6-1
  statistics 9-1
DP/SIP/CODEC NEGO command 6-8
DP/SLOT/#/CHANNEL command 6-9
DS/SIP command 6-4, 9-2
DS/SLOT command 6-5
DSP algorithm limitations 3-8
DTMF in INFO packets parameter 7-5
DTMF Payload parameter 7-4

E

Egress dial rules 2-16
Egress hunt group pattern parameter 8-4
Egress hunt group ports parameter 8-5
Enable registration parameter 7-18
Enter an IP address prompt 8-8
Entry digits parameter 8-3

F

Fax relay 3-16

G

G711 alaw parameter 7-16
G711 ulaw parameter 7-16
G723 parameter 7-14
G726-16K parameter 7-14
G726-24K parameter 7-15
G726-32K parameter 7-15
G726-40K parameter 7-15
G729 parameter 7-13
Gateway 1-5
  defining the UA as 2-19
Gateway ID parameter 7-4
GLOBAL parameters 2-4, 7-2

I

Ingress dial rules 2-16
Ingress/Egress append string parameter 8-6
Ingress/Egress prepend string parameter 8-5

L

Limitations
  DSP algorithm 3-8

M

MAP entry
  adding 2-11
  deleting 2-15
  modifying 2-14
  parameters 2-10
MAP Type
  DIALIP 2-12
  DIALSTRING 2-11
  SUPERMAP 2-13
Map type parameter 8-2
Monitoring
  Codec Negotiation Table 6-8
  messages and retries 6-7
    DC/SIP command 9-3
  negotiated codec payload 6-5
  SIP session 6-4, 9-1
  voice channel 6-3, 6-9
  VoIP functions 6-1
Multipoint connection without proxy server 1-5

N

Negotiated codec payload, viewing 6-5
Network management, for Clarent network 1-21
Number of 1xx class SIP responses Rx 9-6
Number of 1xx class SIP responses Tx 9-6
Number of 2xx class SIP responses Rx 9-6
Number of 2xx class SIP responses Tx 9-6
Number of 3xx class SIP responses Rx 9-7
Number of 3xx class SIP responses Tx 9-7
Number of 4xx class SIP responses Rx 9-7
Number of 4xx class SIP responses Tx 9-7
Number of 5xx class SIP responses Rx 9-8
Number of 5xx class SIP responses Tx 9-8
Number of 6xx class SIP responses Rx 9-8
Number of 6xx class SIP responses Tx 9-8
Number of ACK requests Rx 9-4
Number of ACK requests Tx 9-4
Number of BYE requests Rx 9-4
Number of BYE requests Tx 9-5
Number of BYE retries 9-9
Number of CANCEL requests Rx 9-5
Number of CANCEL requests Tx 9-5
Number of CANCEL retries 9-9
Number of INVITE requests Rx 9-4
Number of INVITE requests Tx 9-4
Number of INVITE retries 9-8
Number of REGISTER requests Rx 9-5
Number of REGISTER requests Tx 9-6
Number of REGISTER retries 9-9
Number of RESPONSE retries 9-9
Number of SIP request messages Rx 9-3
Number of SIP request messages Tx 9-3
Number of SIP response messages Rx 9-3
Number of SIP response messages Tx 9-3
Number of total transactions 9-3

O

Operation parameter 8-2
Out-of-band digit transport 1-15
Overloaded MAP entries 4-7
  example 4-9

P

Packetization selection, viewing 6-9
Parameter list
  Add another map entry 8-7
  Administrative status 7-3
  ANI digits 7-4
  Call Accounting 7-6
  Call Authentication 7-7
  Caller Line Identity Restriction 7-8
  Digits string length 8-3
  Disconnect (BYE or CANCEL) 7-10
  DTMF in INFO packets 7-5
  DTMF Payload 7-4
  Egress hunt group pattern 8-4
  Egress hunt group ports 8-5
  Enable registration 7-18
  Enter an IP address 8-8
  Entry digits 8-3
  G711 alaw 7-16
  G711 ulaw 7-16

G723 7-14
G726-16K 7-14
G726-24K 7-15
G726-32K 7-15
G726-40K 7-15
G729 7-13
Gateway ID 7-4
Ingress/Egress append string 8-6
Ingress/Egress prepend string 8-5
Map type 8-2
Operation 8-2
PIN Length 7-7
Proxy authentication password 7-20
Proxy authentication username 7-19
Proxy server address 7-18
Proxy server UDP Port 7-19
PVC number, Frame Relay 7-17
Receiving ACK 7-9
Redirect Server 7-6
REGISTER expires 7-19
Registration duration 7-10
Resend INVITE 7-9
Server group 7-4
SIP Proxy entry number 7-17
Strip prefix number of digits 8-5
UDP Port 7-3
UserName 7-11
UserPassword 7-12
Parameters
Authentication 7-11
CODEC NEGO 3-14, 7-13
DIALIP Map Type 2-12, 8-8
DIALSTRING Map Type 2-11, 8-2
Extended SIP 2-19
Ingress/Egress dial rules 2-16
MAP entry, adding 2-11
MAP entry, deleting 2-15
MAP entry, modifying 2-14
PROXY 7-17
SE/MAP 8-1
SE/SIP 7-1
SIP Authentication 2-7
SIP Global 2-4, 7-2
SIP Proxy 2-8
SIP Timer 2-6, 7-9
SUPERMAP Map Type 2-13, 8-8
Voice Mapping Table 2-10
PIN Length parameter 7-7
Point-to-point connection 1-3
Protocol, viewing 6-9
Proxy authentication password 7-20
Proxy authentication username 7-19
PROXY parameters 2-8, 7-17
Proxy server address parameter 7-18
Proxy server UDP Port parameter 7-19

R

RADIUS 1-9
Receiving ACK parameter 7-9
Redirect server 5-1
see also SIP Redirect Server
Redirect Server parameter 7-6
REGISTER expires 7-19
Registration 1-8
Registration duration parameter 7-10
Registration status statistic 9-2
Request messages, statistics 6-7, 9-3
Resend INVITE parameter 7-9
Response messages, statistics 6-7, 9-3
Retries, statistics 6-7, 9-3

S

Server group parameter 7-4
SIP billing 1-9
SIP characteristics, defining 2-3
SIP connection types 1-3
SIP counters 6-7, 9-3
SIP Hairpin 4-1
bypassing the proxy server 4-10
configuration 4-6
DIALIP MAP entry 4-6
egress calls 4-5
example applications 4-9
for dialing 911 4-13
how it works 4-3
ingress calls 4-4
overloaded MAP entries 4-7
overloaded MAP entries, example 4-9
SIP protocol 1-3
SIP Proxy entry number 7-17
SIP proxy server
bypassing, with SIP Hairpin 4-10
connection 1-4
SIP Redirect Server 5-1
call negotiation 5-3
configuration 5-6
example 5-6
traffic volume considerations 5-4
SIP registration 1-8
configuring 2-8
SIP session, status of 6-4, 9-1
SIP VoIP mode
characteristics 1-2
configuring 2-1
enabling 2-4
monitoring 6-1
network management 1-21
other network components 1-17
Statistics 6-1
Statistics list

Current operational state 9-2
Number of 1xx class SIP responses Rx 9-6
Number of 1xx class SIP responses Tx 9-6
Number of 2xx class SIP responses Rx 9-6
Number of 2xx class SIP responses Tx 9-6
Number of 3xx class SIP responses Rx 9-7
Number of 3xx class SIP responses Tx 9-7
Number of 4xx class SIP responses Rx 9-7
Number of 4xx class SIP responses Tx 9-7
Number of 5xx class SIP responses Rx 9-8
Number of 5xx class SIP responses Tx 9-8
Number of 6xx class SIP responses Rx 9-8
Number of 6xx class SIP responses Tx 9-8
Number of ACK requests Rx 9-4
Number of ACK requests Tx 9-4
Number of BYE requests Rx 9-4
Number of BYE requests Tx 9-5
Number of BYE retries 9-9
Number of CANCEL requests Rx 9-5
Number of CANCEL requests Tx 9-5
Number of CANCEL retries 9-9
Number of INVITE requests Rx 9-4
Number of INVITE requests Tx 9-4
Number of INVITE retries 9-8
Number of REGISTER requests Rx 9-5
Number of REGISTER requests Tx 9-6
Number of REGISTER retries 9-9
Number of RESPONSE retries 9-9
Number of SIP request messages Rx 9-3
Number of SIP request messages Tx 9-3
Number of SIP response messages Rx 9-3
Number of SIP response messages Tx 9-3
Number of total transactions 9-3
Registration status 9-2
Version 9-2
Strip prefix number of digits parameter 8-5
Super G3 fax 3-16
SUPERMAP Map Type 2-13
parameters 8-8

T

T.38 mode 3-16
TIMER parameters 2-6, 7-9

U

UA 1-3
gateway versus endpoint 2-19
UDP Port parameter 7-3
USERAGENTTYPES parameter 2-19
UserName parameter 7-11
UserPassword parameter 7-12

V

Version statistic 9-2
Voice channel, status of 6-3, 6-9
VoIP gateway 1-5

W

Wildcard
in Ingress/Egress append string 8-6
in SUPERMAP entry 2-13

REACH FURTHER. OFFER MORE.

Contact Memotec:

tel.: +1-514-738-4781
e-mail: MemotecSupport@memotec.com

7755 Henri Bourassa Blvd. West
Montreal, Quebec | Canada H4S 1P7 www.memotec.com

MEMOTEC
redefining network efficiency