



**NORTEL**

**Secure Router 2330/4134 as Communication Server 1000  
Survivable SIP Branch Solution**

# Quick Start Configuration Guide

Release: 10.2

Document Revision: 01.03

[www.nortel.com](http://www.nortel.com)

---

**NN-SR-0001**

**Secure Router 2330/4134 as Communication Server 1000 Survivable SIP Branch Solution**  
**Release: 10.2**  
**Publication: NN-SR-0001**  
**Document release date: 23 November 2009**

**Copyright © 2009 Nortel Networks. All Rights Reserved.**

**While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.**

**Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.**

**All other trademarks are the property of their respective owners.**

---

# Contents

---

<b>CONTENTS</b>	<b>3</b>
<b>NEW IN THIS RELEASE</b>	<b>4</b>
NAVIGATION	4
CS 1000 AND SECURE ROUTER 2330/4134	4
FEATURE BACKGROUND	4
<i>Communication Server 1000</i>	4
<i>Secure Router 4134</i>	6
<i>Secure Router 2330</i>	7
FEATURE DESCRIPTION	7
<i>Multiservice Branch Router</i>	7
<i>Survivable SIP PSTN Gateway</i>	8
<b>INTRODUCTION</b>	<b>10</b>
NAVIGATION	10
<b>SR 2330/4134 INTEROPERABILITY WITH CS 1000</b>	<b>11</b>
SR 2330/4134, CS 1000 COMPONENTS	11
SSM OPERATION	12
SIP GATEWAY OPERATION	13
<b>CS 1000 CONFIGURATION</b>	<b>16</b>
SLG CONFIGURATION	16
<i>Steps</i>	16
SSG CONFIGURATION	26
<i>Steps</i>	26
NRS/SPS CONFIGURATION	29
<i>Steps</i>	29
SIP CLIENTS CONFIGURATION	34
CS 1000 PATCHES	34
<b>SR 2330/4134 CONFIGURATION</b>	<b>35</b>
<i>Steps</i>	35
<i>NTML Examples</i>	40
Example of Normal mode NTML (normal_cs1k.ntm)	40
Example of Backup mode NTML (backup_cs1k.ntm)	40

---

## New in this release

---

The following section details what's new in *Secure Router 2330/4134 as Communication Server 1000 Survivable SIP Branch Solution (NN-SR-0001)* for Release 10.2.

### Features

The following sections detail the Secure Router 2330/4134 based CS 1000 branch solution and its features.

### Navigation

- ["CS 1000 and Secure Router 2330/4134" \(page 4\)](#)
- ["Feature background" \(page 4\)](#)
- ["Feature description" \(page 7\)](#)

## CS 1000 and Secure Router 2330/4134

In a centralized CS 1000 call server architecture, the remote branches make use of the call processing resources available at a central location, generally located at the corporate headquarters. The survivable branch solution based on Secure Router 4134 (SR 4134) and Secure Router 2330 (SR 2330) provides business continuity to the branch office in the event of a WAN connection outage to corporate headquarters. With this solution, employees at the branch office can continue to use SIP phones to place and receive intra-site calls and calls over the PSTN, including 911 calls.

## Feature Background

### Communication Server 1000

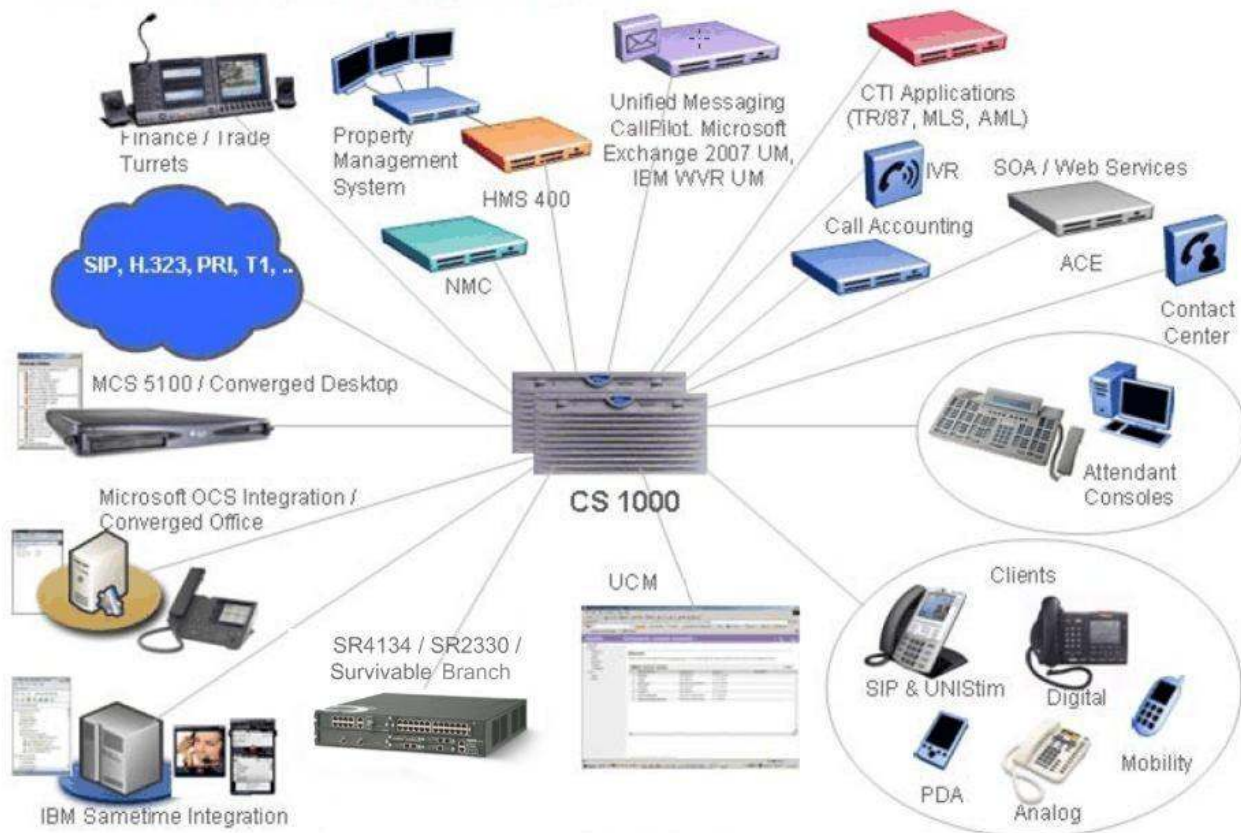
**Nortel Communication Server 1000** is a server-based, full-featured IP PBX and the cornerstone of Nortel Enterprise Unified Communication deployments. It provides the benefits of a converged network plus advanced applications and over 750 world-class telephony features. Fully distributed over IP LAN & WAN infrastructure with built-in reliability and survivability, Communication Server 1000 supports business-critical applications, including unified messaging, customer contact center, IVR, wireless VoIP and IP phones.

Key Features:

- Feature rich with over 750 call processing and telephony features
- Highly scalable with support for up to 22,500 IP users off of one Call Server, multiple Call Servers networked together can support unlimited scalability

- World class reliability and redundancy mechanisms - highly reliability architectural elements that maximize network uptime with extensive redundancy mechanisms to ensure network uptime including survivability options such as Campus and Geographic redundancy to support network failover
- Extensive desktop portfolio includes; Wireless, Soft-phones, IP, Digital and Analog set support, to meet diverse end-user requirements
- Supports business-critical applications, including IP Contact Center, CallPilot unified messaging, and integrated services such as conferencing, one-number-follow-me Personal Call Director, recorded announcement, network-wide attendant and messaging
- Telephony integration with desktop application providers such as Microsoft and IBM

## CS 1000: The Big Picture



For more details please refer Nortel CS 1000 Product Webpage

[http://products.nortel.com/go/product\\_content.jsp?segId=0&catId=null&parId=0&prod\\_id=51121&locale=en-US](http://products.nortel.com/go/product_content.jsp?segId=0&catId=null&parId=0&prod_id=51121&locale=en-US)

## Secure Router 4134

The **Nortel Secure Router 4134** is a modular, multi-service platform that integrates multiple networking functions, including routing, WAN, Ethernet switching, security and Voice over IP (VoIP) into a single device. The platform's design ensures the consistently high throughput required by voice, data or unified communications applications. The first device of its kind to feature embedded Microsoft intelligence to simplify deployment of unified communications, the Secure Router 4134 can reduce the number of devices needed at the branch or regional site, generating substantial operational and capital cost savings for your business.

### Key Features:

- Highly modular, high-performance platform - A wide range of LAN, WAN and multiservice options to support converged branch, regional or headquarters environments
- All-in-one voice, data and unified communications solution for enterprises – Nortel SCS Server hosted on 4134 provides complete unified communications and data networking solution for enterprise sites of up to 250 users by combining voice — call server, conferencing, collaboration applications and PSTN gateway — with data and security in an integrated, easy-to-manage platform.
- Only device of its kind to integrate Microsoft OCS services - Ideal for enterprises considering deploying Microsoft OCS services in their remote branch sites
- Voice media gateway services - Enables connection to the Public Switched Telephone Network (PSTN) or to traditional telephony devices
- Survivable voice services - Allows continued voice calling when the primary IP connection is lost.
- Robust routing services - Full IPv4 and IPv6, BGP-4 and multicast implementation for enterprise deployments
- Integrated Ethernet switching - High-density L2/L3 Gigabit, Fast Ethernet, as well as Power over Ethernet. Up to 58 Gigabit or 72 Fast Ethernet ports supported.
- Wide range of WAN connectivity - Low and high-speed WAN options include serial, T1/E1, DS3/T3, Channelized DS3/T3, HSSI and ISDN
- Integrated security - Stateful firewall and high-speed VPN encryption ensured the integrity of both voice and data traffic
- High-reliability / resiliency - Hot-swappable modules, redundant power and port/platform resiliency features deliver maximum uptime
- Unified Communications-ready platform - Superior small packet handling and low latency ensures the quality of multimedia applications. Integrated VoIP and Microsoft capabilities deliver on the promise of the unified communications branch.

For more details please refer Nortel SR 4134 Product Webpage

[http://products.nortel.com/go/product\\_content.jsp?segId=0&catId=null&parId=0&prod\\_id=62360&locale=en-US](http://products.nortel.com/go/product_content.jsp?segId=0&catId=null&parId=0&prod_id=62360&locale=en-US)

## Secure Router 2330

The **Nortel Secure Router 2330** is a cost reduced 1RU version of 4134 with almost same feature set and lower capacity.

For more details please refer Nortel SR 2330 Product Webpage

[http://products.nortel.com/go/product\\_content.jsp?segId=0&catId=null&parId=0&prod\\_id=69360&locale=en-US](http://products.nortel.com/go/product_content.jsp?segId=0&catId=null&parId=0&prod_id=69360&locale=en-US)

## Feature Description

The Secure Routers 4134 and 2330 combines high performance, robust routing, flexible WAN and voice media gateway connectivity and is targeted at enterprise branch and remote site environments. A rich suite of routing services and advanced WAN functionality makes these Secure Routers ideal for high-speed Internet access, private line WAN connectivity, IP Telephony and multimedia, IPSec VPN, stateful firewall and data applications. The SR 2330/4134 survivable branch solution for Nortel CS 1000 provides business continuity to the branch office in the event of a WAN connection outage to corporate headquarters.

### Multiservice Branch Router

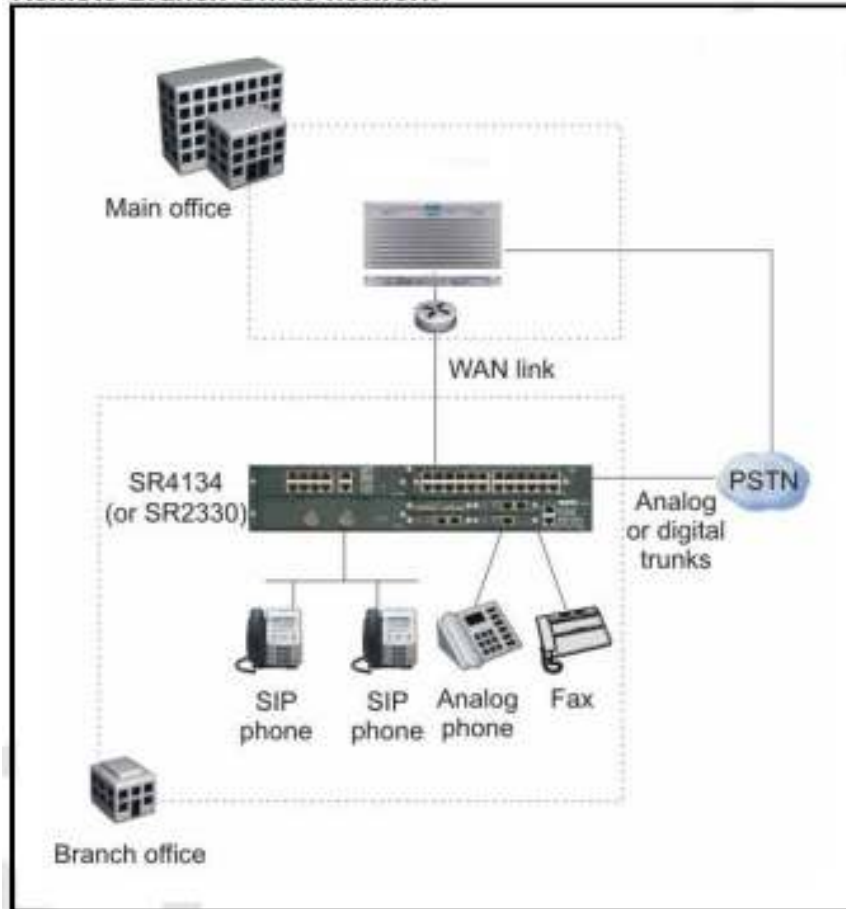
Figure 1 shows a survivable branch office deployment with CS 1000 Call Server located at the corporate main office or data center and Secure Router as branch office multi service router providing data routing, security and survivable SIP-PSTN gateway.

Data routing services include a full IPv4 and IPv6 protocol set, including BGP-4 and multicast capabilities. A full-function IPv6 implementation also enables deployment into environments that require extended IP addressing with the same routing services.

Powerful, fully-integrated security features include VPN and firewalls for increased reliability and user confidence. Capabilities include stateful packet firewall, detection and prevention of more than 60 Distributed Denial of Service (DDoS) attacks, VPN hardware acceleration for hub and spoke deployment over IPSec and VPN tunnels, and IPSec VPN data-encryption services with AES, 3DES, DES, SHA-1, MD-5 and Diffie-Hellman support.

The SR also offers a set of integrated voice interfaces that allow connection to the public switched telephone network (PSTN) as well as support of conventional TDM-based telephony devices. T1/E1, FXS and FXO interfaces are all available for flexible telephony connection with support for up to 128 simultaneous voice channels.

**Figure 1**  
**Remote Branch Office network**



## Survivable SIP PSTN Gateway

Figure 2 shows a survivable branch office deployment with CS 1000 Call Server located at the corporate main office or data center and Secure Router providing survivable SIP-PSTN gateway functionality complementing the existing data infrastructure.

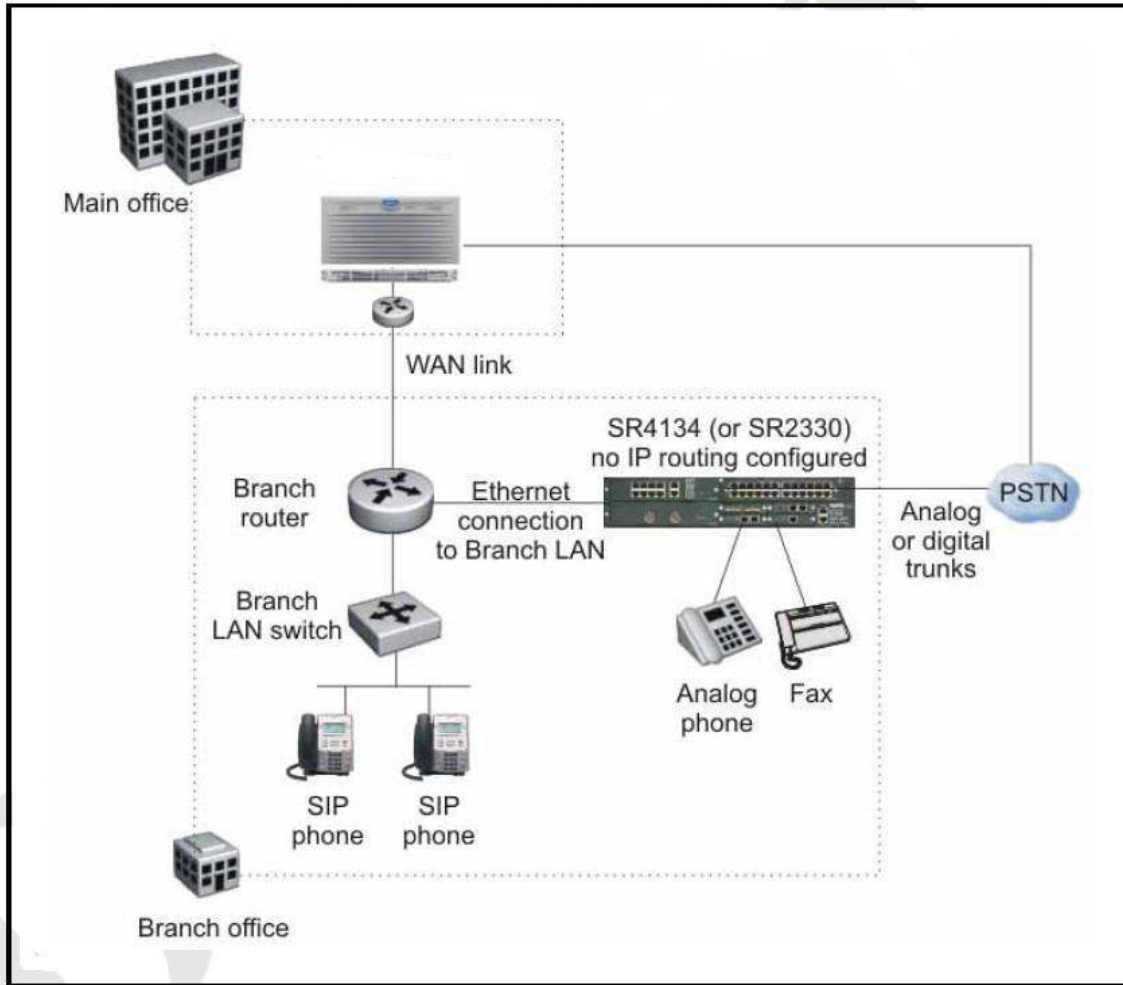
The SR 2330/4134 supports a variety of PSTN interfaces like T1/E1, BRI U, BRI S/T, FXS/DID and FXO/CAMA for connectivity to PSTN and legacy PBXs and telephony devices. Also supports a rich set of PSTN protocols including ISDN PRI, BRI, QSIG, T1 CAS, E1 R2 and analog signaling.

The Secure Router also includes a SIP Registrar and B2BUA based SIP Proxy which can function as a backup SIP Server supporting up-to 300 SIP end-points including Nortel and 3rd-party SIP phones Nortel 1120E/1140E, Nortel 1535 Video phone, LG Nortel 6800/8800, Polycom 330, SMC 3456, IP Dialog and Xlite. It can provide phone and call routing services to the branch office when main office call server connectivity is lost and is already tested with Nortel Call Servers and 3rd party Servers - CS 1000, CS 2100, CS 2000, A2E, SCS,



Microsoft OCS and Broadsoft/Sylantro. Other main features include Call Admission Control, PSTN fallback and memory based load control.

**Figure 2**  
**SR with existing LAN infrastructure in Remote Branch Office network**



---

# Introduction

---

This document describes the quick start configuration of Nortel Secure Router 2330/4134 (Release 10.2) as survivable branch SIP-PSTN gateway for Nortel Communication Server 1000 (Release 6.0). For more information and detailed configuration guides on SR 2330, SR 4134 and CS 1000 go to the Nortel website:

[www.nortel.com/support](http://www.nortel.com/support)

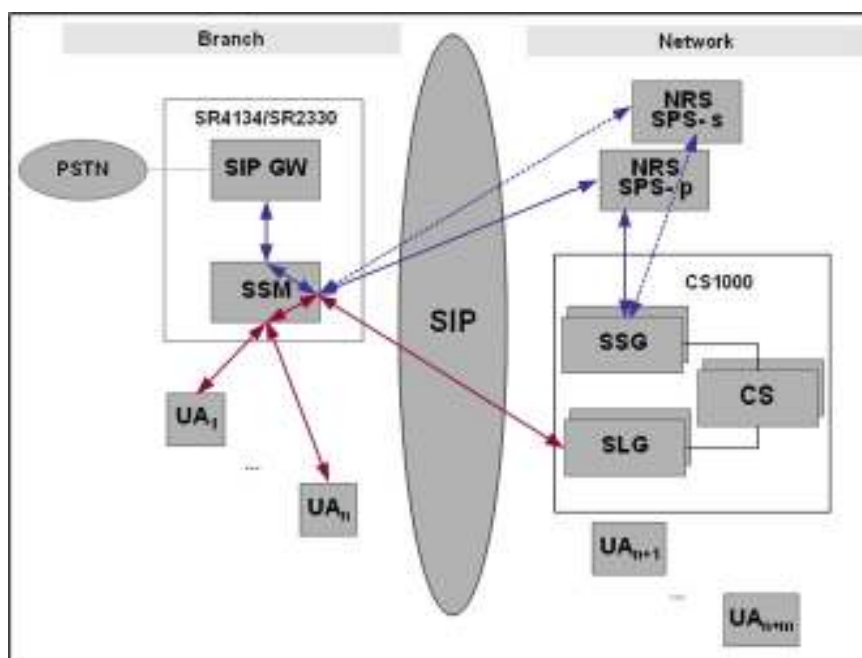
## Navigation

- "SR 2330/4134 interoperability with CS 1000 (page 11)
- "CS 1000 Configuration" (page 16)
- "SR 2330/4134 Configuration" (page 35)

## SR 2330/4134 interoperability with CS 1000

### SR 2330/4134, CS 1000 components

The following diagram shows the main components of Secure Router 2330/4134 and Communication Server 1000.



SR has two modules SIP Gateway (SIP GW) and SIP Survivability Module (SSM) that together interworks with CS 1000 to provide SIP survivable gateway functionality at the branch. SSM is a software-only subsystem on the Secure Router through which SIP calls are routed to the CS 1000. This module includes SIP B2BUA based proxy and SIP Registrar. SIP GW is software and hardware subsystem on the Secure Router that provides PSTN connectivity. The User Agents (UA) are SIP endpoints.

For detailed information about SSM operation please refer to Secure Router Release 10.2 guide NN47263-510 Configuration — SIP Survivability.

For detailed information on SIP GW please refer to Secure Router Release 10.2 guide NN47263-508 Configuration — SIP Media Gateway.

The main CS 1000 components are Call Server (CS), SIP Signaling Gateway (SSG), SIP Line Gateway (SLG), SIP Proxy Server (SPS) and Network Routing Service (NRS). SSG handles SIP trunking and SLG takes care of SIP endpoints or SIP Lines.

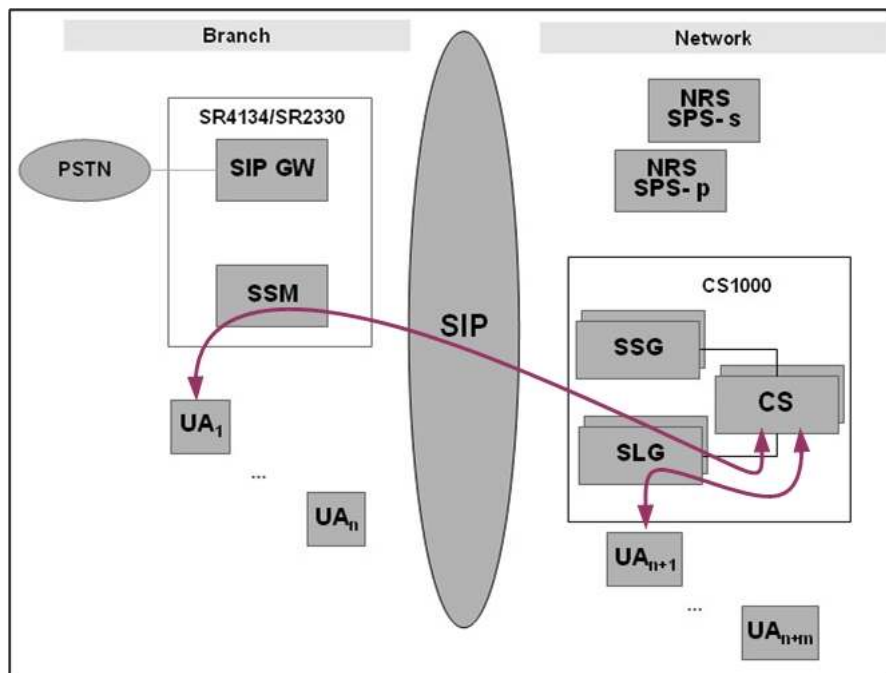
For detailed information on CS 1000 components and operation please refer to Communication Server 1000 Release 6.0 user guides.

## SSM Operation

The SSM operates in two modes - Normal (Connected) and Survivable (Isolated). In normal mode, the SSM functions as an outbound proxy and proxies all SIP messages initiated from the SIP phones (UA) and the SIP GW to the SLG located in the head office. SSM acts as a B2BUA i.e. changes the Contact Header of SIP endpoint requests. Also the SIP endpoint registrations to the SLG are “cached” locally. In survivable mode, the SSM supports SIP server functionality to provide basic call features to the SIP endpoints at the branch, and also supports local registrar functionality to store registrations.

SSM monitors the reachability of SLG by sending OPTIONS messages. If SLG is not reachable or the link connected to SLG is down, SSM switches to the Survivable mode. The SSM will continue to monitor the reachability of SLG as long as the link is up. Once it is reachable, SSM will switch back to Normal mode.

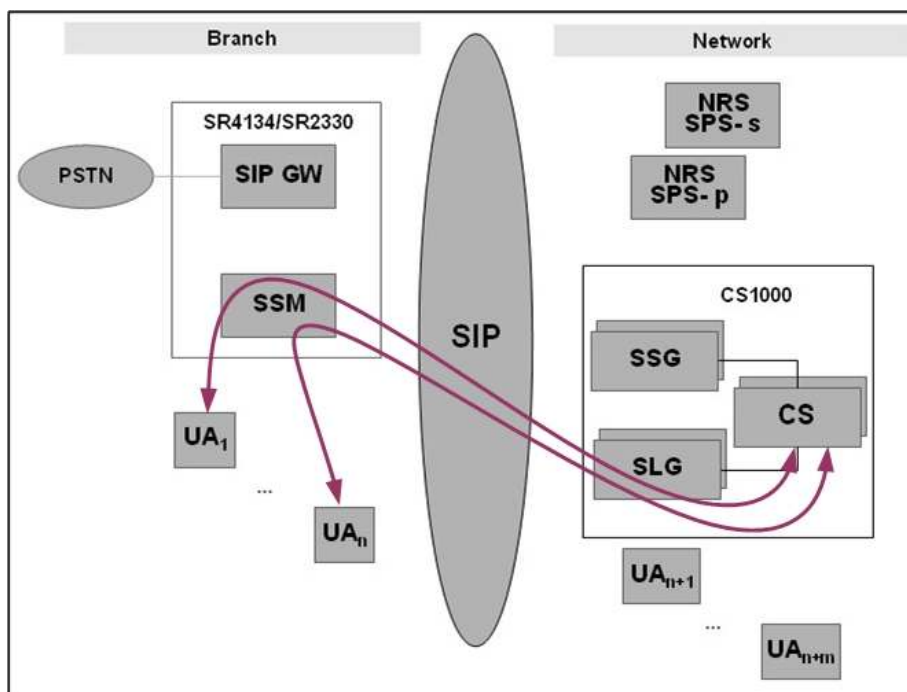
SIP endpoints that have registered during Survivable mode will be registered with the SLG after the Normal mode is established and next registration is attempted. SSM forces SIP endpoints to register frequently (Default time 30 sec) in Survivable mode so that the endpoints are registered to SLG as soon as SSM switches to Normal mode.



The above diagram shows the call flow of a SIP endpoint in branch, calling a SIP endpoint connected to CS 1000 in Normal (Connected) mode. SSM proxies the calls to the SLG received from the SIP endpoint. SSM also modifies the contact header in the INVITE messages to point to the SSM bind IP address before forwarding the INVITE to the SLG to

ensure that incoming calls are routed through the SSM. The same call flow holds good for the call originated by the SIP endpoint connected to CS 1000. When the call arrives at SSM, it will look for a mapped contact in its registration “cache” and routes the call to the UA. If SSM does not find the mapped contact then it forwards the call to the configured default gateway.

The following diagram shows the call flow between two SIP endpoints in branch in Normal (Connected) mode.

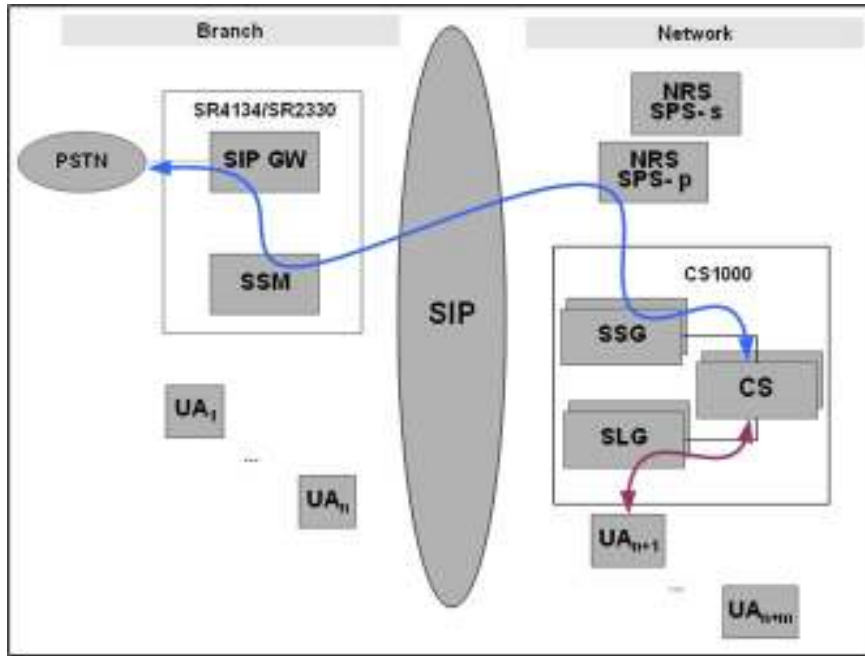


## SIP Gateway Operation

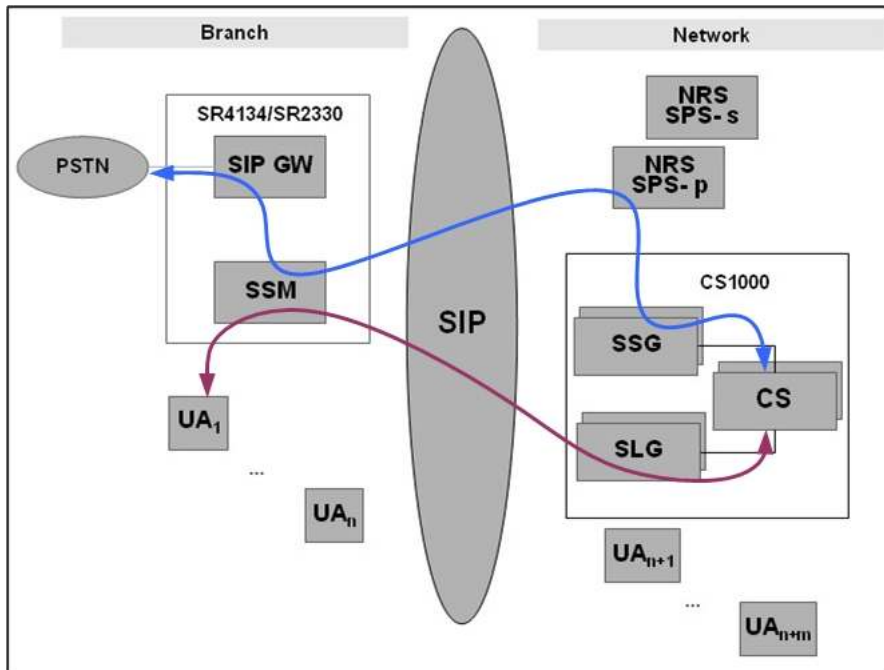
SIP GW interconnects SIP voice over IP networks with the PSTN. It also provides direct connections for analog phones, faxes and modems. In branch office deployment for CS 1000, SIP GW registers with the currently active NRS/SPS to enable newly active SPS to route calls to SIP GW. This is different than a user registration. SIP GW will monitor the reachability of NRS/SPS to know that current active NRS/SPS. SIP GW does this by sending OPTIONS messages to both primary and secondary NRS/SPS. If current active SPS is not reachable, then gateway will switch to the other SPS as the currently active SPS.

The following diagram shows the call flow between a branch PSTN interface/device and SIP endpoint connected to CS 1000. The SIP GW will route PSTN calls to an active SPS server with Req-Uri having IP address of the active NRS/SPS via SSM. The SSM will then replace the IP address with CS 1000 domain in 'From', 'To' and Req-Uri headers. If none of the NRS SPSs is available, then SIP GW will send calls to SSM with Req-Uri having host as domain configured for SLG in SSM e.g. nortel.com. This routing happens on the basis of entries defined in Normal mode NTML dial plan. Normal mode dial plan defines routes for both primary SPS and secondary SPS. SSM will choose the route from NTML depending upon destination set in SIP messages by SIP GW.

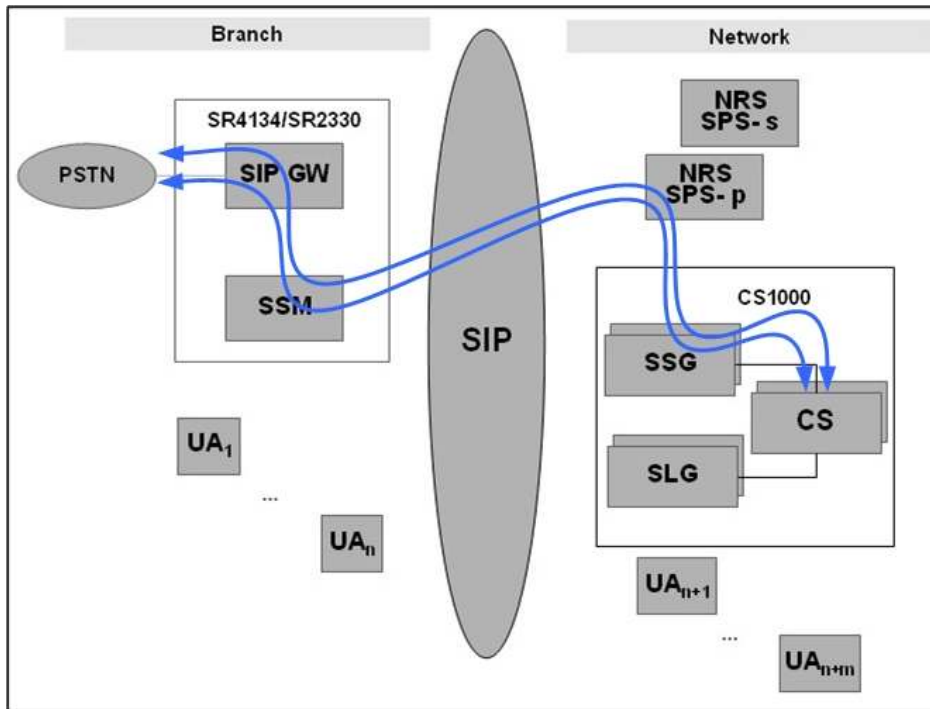
SSM will receive the incoming calls from SPS that are destined for PSTN. For such calls SSM will not be able to find a mapped contact in its registration cache and hence routes the call to configured default gateway which is SIP GW.



The following diagram shows the call flow between a branch PSTN interface/device and branch SIP endpoint.

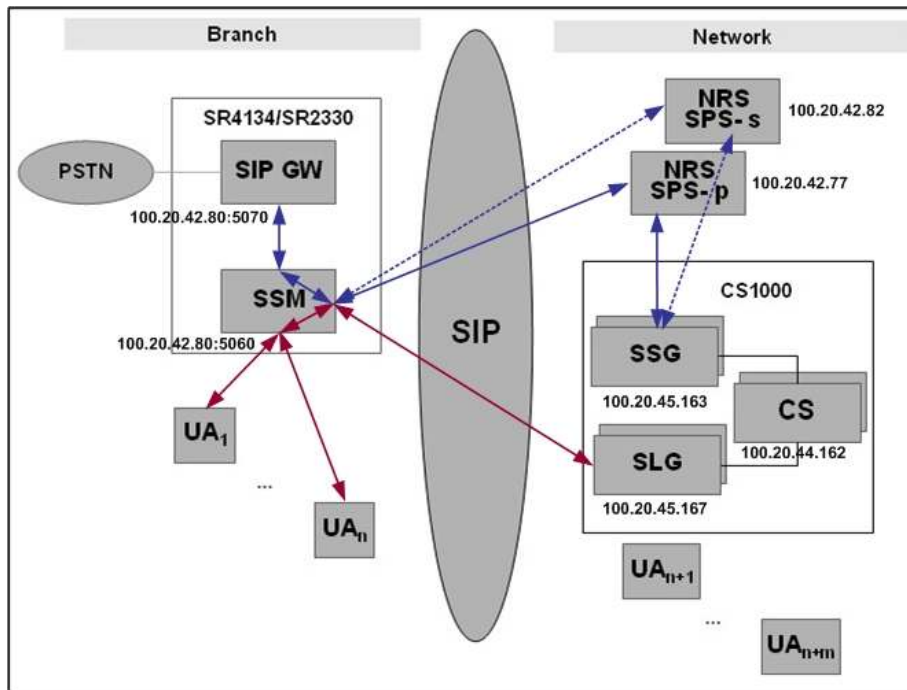


The following diagram shows the call flow between branch PSTN interfaces/devices.



# CS 1000 Configuration

This section describes the configuration steps needed on CS 1000 components like SLG, SSG and SPS for SR 2330/4134 based branch solution. There is no SR 2330/4134 specific configuration required on CS 1000. Please refer to CS 1000 user guides for the detailed configuration steps. The following diagram complete with IP addresses will be used as reference for the configuration chapters.



## SLG Configuration

Please refer to CS 1000 NN43001-508 SIP Line Fundamentals document for detailed information on SLG configuration. There is no Secure Router specific configuration need to be done on SLG.

### Steps

1. SIP Line (SIPL) feature depends on the following packages to be enabled in keycode.



Package Mnemonic	Package Number	Package Description	Package Type (New or Existing or Dependency)	Applicable Market
SLS_Package	417	SIP Line Service	New	Global
FFC	139	Flexible Feature Codes	Existing	Global
SIP_LINE_NT_PKG	415	Nortel SIP Line Package	Existing	
SIP_LINE_3P_PKG	416	3rdParty SIP Line Package	Existing	

2. Deploy SIP Line software application on the Linux server

The screenshot shows the 'UCM DEPLOYMENT MANAGER' interface. On the left is a navigation menu with 'Deployment Targets' selected. The main area displays details for a target deployment on host 'ws2' (IBM X306M), which is currently 'Undeployed'. The 'Software Applications' section shows a list of packages to be deployed, with 'SIPL' (SIP Line) checked. The 'Software versions' dropdown is set to '6.31.02'. Buttons for 'Deploy', 'Upgrade', and 'Undeploy' are visible.

Figure SIPL 1 – SIP Line application deployment

### 3. SIPL node configuration

#### + Nodes: Servers, Media Cards

Managing: 100.20.44.162 Username: admin  
System » IP Network » IP Telephony Nodes

#### Node Details (ID: 4101 - SIP Line)

Node ID:  \* (0-9999)

Call Server IP Address:  \*

**Telephony LAN (TLAN)**

Node IP Address:  \*

Subnet Mask:  \*

**Embedded LAN (ELAN)**

Gateway IP address:  \*

Subnet Mask:  \*

**IP Telephony Node Properties**

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN

**Applications (click to edit configuration)**

- [SIP Line](#)

\* Required Value. Save Cancel

#### Associated Signaling Servers & Cards

Select to add    Print | Refresh

<input type="checkbox"/>	Hostname	Type	Deployed Applications	ELAN IP	TLAN IP	Role
<input type="checkbox"/>	campus4-sipline	Signaling Server	SIP Line	100.20.44.165	100.20.45.166	Leader

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list.

Figure SIPL 2 – SIPL node details

Managing: 100.20.44.162 Username: admin  
System » IP Network » IP Telephony Nodes

#### Node ID: 4101 - SIP Line Configuration Details

General | SIP Line Gateway Settings | SIP Line Gateway Service

SIP Line Gateway Application:  Enable gateway service on this Node

**General**

SIP Domain name:  \*

SLG endpoint name:

SLG Group ID:

SLG Local Sip Port:  (1 - 65535)

SLG Local Tls Port:  (1 - 65535)

**Virtual Trunk Network Health Monitor**

Monitor IP Addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

**SIP Line Gateway Settings**

Security Policy:

Number of Byte Re-negotiation:

Options:  Client Authentication  
 x509 Certificate Authentication Enabled

\* Required Value. Save Cancel

Note: Changes made on this page will NOT be transmitted until the Node is also saved.

Figure SIPL 3 – General SIPL node configuration

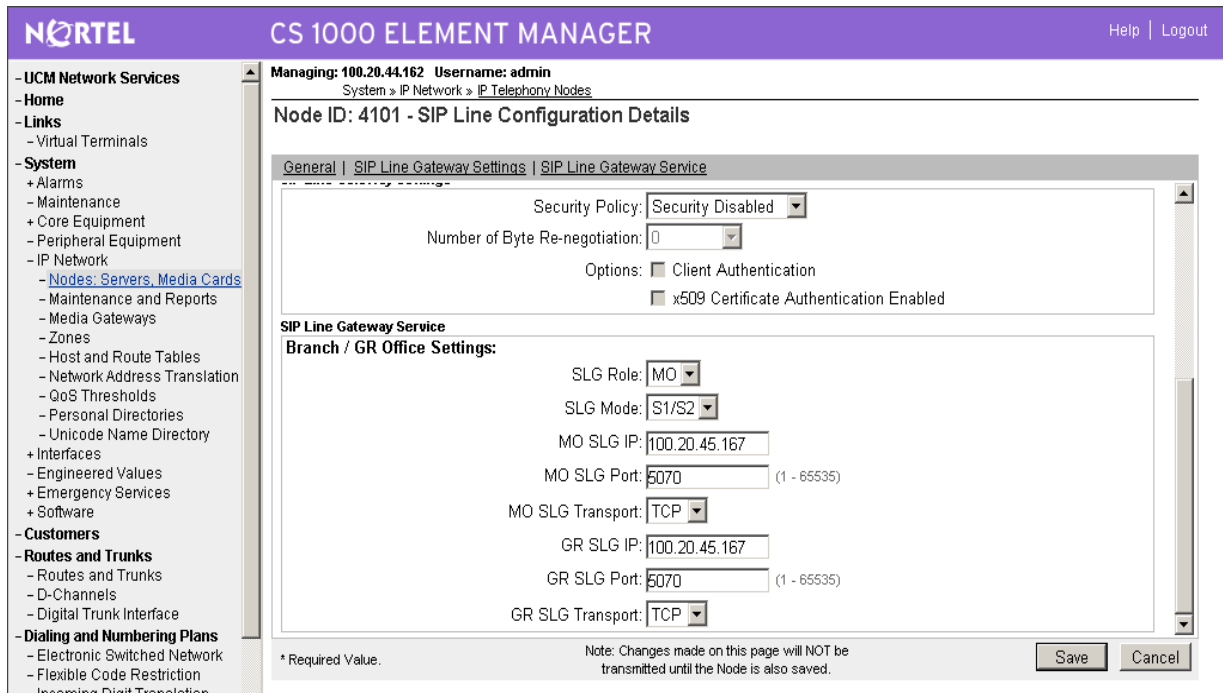


Figure SIPL 4 – SIP Line Gateway Service configuration

4. The SIP Line service must be enabled on a customer level

+ Customer --> Cus Number --> SIP Line Service

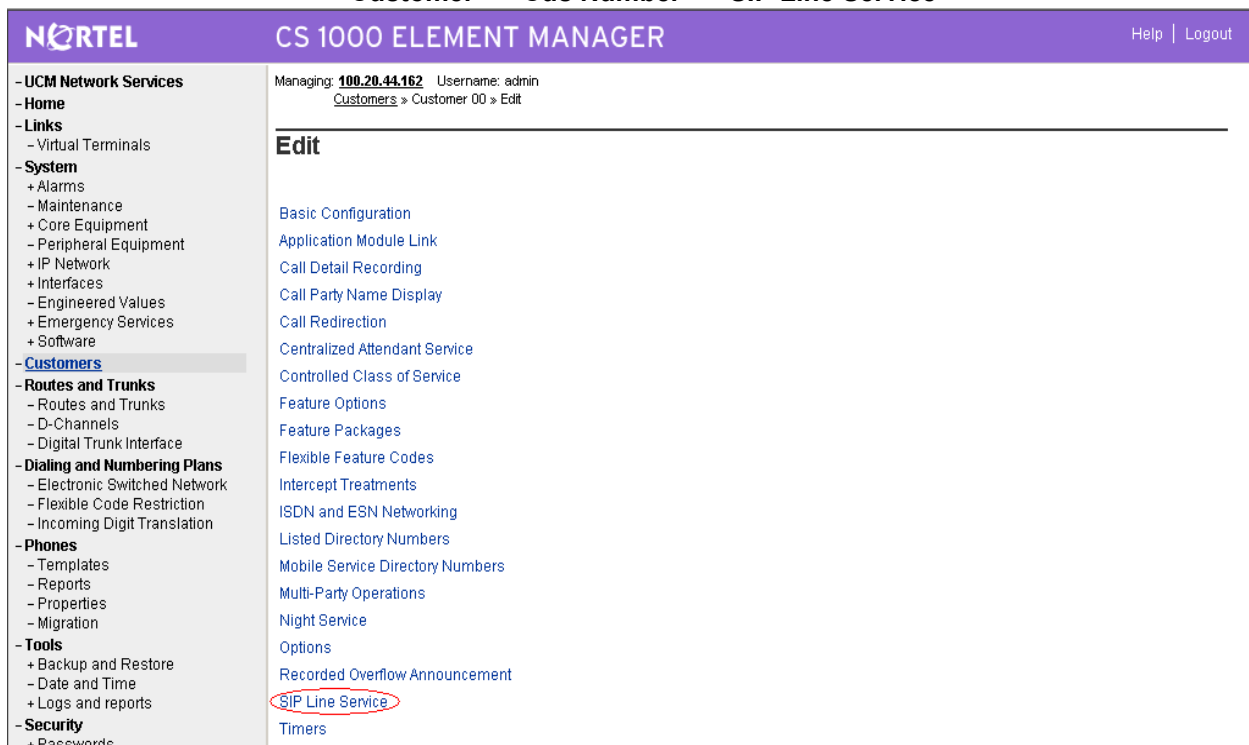


Figure SIPL 5 - SIP Line service inside Customer edit page

**NORTEL** CS 1000 ELEMENT MANAGER Help | Logout

Managing: **100.20.44.162** Username: admin  
 Customers > Customer 00 > Edit > SIP Line Service

### SIP Line Service

SIP Line Service

Root domain:  \*

User agent DN prefix:

Optional features:  Nortel Multimedia

\*Required Value Save Cancel

Figure SIPL 6 - SIP Line service enable page

## 5. Password length configuration for SIP clients

### + Customer -->CUS# -->Flexible Feature Codes

**NORTEL** CS 1000 ELEMENT MANAGER Help | Logout

Managing: **100.20.44.162** Username: admin  
 Customers > Customer 00 > Edit > Flexible Feature Codes

### Flexible Feature Codes

Controlled class of service restricted service:

Station control password length:   
The active password length is changed only if new configuration data is dumped, and a complete data load and program load takes place

Station control password:  Use for set based administration user level access  
 Use default station control password for IP phones

Mobile extension activation code:

Indicator:  Provide end of dialing indicator

End of dial indicator string length:

End of dial indicating string:  (0-9,\*,#)

Auto dial delay:  (Seconds)

Tone:  Provide confirmation tone

[Flexible Feature Code Entries](#)

Save Cancel

Figure SIPL 7 - Password length configuration

## 6. Enable ISDN for trunking

### + Customer --> CUS# --> Features Packages

**CS 1000 ELEMENT MANAGER** Help | Logout

- UCM Network Services
  - Home
  - Links
  - System
    - + Alarms
    - Maintenance
    - + Core Equipment
    - Peripheral Equipment
    - IP Network
      - Nodes: Servers, Media Cards
      - Maintenance and Reports
      - Media Gateways
      - Zones
      - Host and Route Tables
      - Network Address Translation
      - QoS Thresholds
      - Personal Directories
      - Unicode Name Directory
    - + Interfaces
      - Engineered Values
      - + Emergency Services
      - + Software
  - Customers
  - Routes and Trunks
    - Routes and Trunks
    - D-Channels
    - Digital Trunk Interface
  - Dialing and Numbering Plans
    - Electronic Switched Network
    - Flexible Code Restriction
    - Incoming Digit Translation
  - Phones
    - Templates

**+ Customer --> CUS# --> Features Packages**

- + main frequency Compensated Signaling Package: 120
- + International Supplementary Features Package: 131
- + Enhanced Night Service Package: 133
- Integrated Services Digital Network Package: 145
  - + Dial Access Prefix on CLID table entry option
    - Integrated Services Digital Network:
    - Virtual Private Network Identifier: 101 (1 - 16383)
    - Private Network Identifier: 1 (1 - 16383)
      - Node DN: [ ]
    - Multi-location Business Group: 0 (0 - 65535)
    - Business Sub Group Consult-only: 65535 (0 - 65535)
      - Prefix 1: [ ]
      - Prefix 2: [ ]
    - Home Number Plan Area code: [ ] (200 - 999)
    - Prefix for Central Office: [ ] (100 - 9999)
    - Home location code: 32 (100 - 99999999)
    - Local steering code: 52
    - Calling Number Type: CLID feature displays the set's Prime DN
    - Redirection Count for ISDN calls: 5
    - CLID information for incoming/outgoing calls: No manipulation is done
    - Public Service Telephone Networks:

Figure SIPL 8 – Enable ISDN feature

## 7. AML and VAS configuration

### + System --> Interfaces --> Application Module Link (must over 32)

**CS 1000 ELEMENT MANAGER** Help | Logout

Managing: 100.20.44.162 Username: admin  
System » Interfaces » Application Module Link » New Application Module Link

**New Application Module Link**

Port number: 33 \* (16 - 127)  
AML over ELAN

Description: SIPL

Link control system parameters

Maximum octets: 512 (per HDLC frame)

Save Cancel

Figure SIPL 9 – AML configuration

+ System --> Interfaces --> Value Added Server --> Add --> Application Module Link

**NORTEL CS 1000 ELEMENT MANAGER** Help | Logout

Managing: **100.20.44.162** Username: admin  
System > Interfaces > Value Added Server > Add Value Added Server > Ethernet Link

### Ethernet Link

Value Added Server ID:  \* (16 - 127)

Ethernet LAN Link:  ELAN port configured in ADAN

Application Security:

Interval:  Time interval for checking the link for overload in five second increments

Message Count Threshold:  \* (10 - 9999)

Figure SIPL 10 – AML configuration

8. D-channel/Route/Trunk for SIPL service

+ Routes and Trunks --> D-Channel

**NORTEL CS 1000 ELEMENT MANAGER** Help | Logout

Managing: **100.20.44.162** Username: admin  
Routes and Trunks > D-Channels > D-Channels 80 Property Configuration

### D-Channels 80 Property Configuration

**- Basic Configuration**

Input Description	Input Value
Action Device And Number (ADAN) (TYPE)	DCH
D channel Card Type (CTYP)	DCIP
Designator (DES)	SIPLine
Recovery to Primary (RCVP)	<input type="checkbox"/>
PRI loop number for Backup D-channel (BCHL)	<input type="text"/>
User (USR)	Integrated Services Signaling Link Dedicated (ISLD)
Interface type for D-channel (IFC)	Meridian Meridian1 (SL1)
Country (CNTY)	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number (DCHL)	<input type="text"/>
Primary Rate Interface (PRI)	<input type="text"/> <input type="button" value="more PRI"/>
Secondary PRI2 loops (PRI2)	<input type="text"/>
Meridian 1 node type (SIDE)	Slave to the controller (USR)
Release ID of the switch at the far end (RLS)	25
Central Office switch type (CO_TYPE)	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum (ISLM)	4000 <span style="color: green;">Range: 1 - 4000</span>
Signaling Server Resource Capacity (SSRC)	1800 <span style="color: green;">Range: 0 - 4000</span>

Copyright © 2002-2009 Nortel Networks. All rights reserved.

Figure SIPL 11 – D-Channel configuration for SIPL service

+ Routes and Trunks --> Routes and Trunks --> CUS# --> Add route

Managing: 100.20.44.162 Username: admin  
Routes and Trunks > Routes and Trunks > Customer 0, Route 80 Property Configuration

### Customer 0, Route 80 Property Configuration

**- Basic Configuration**

Route data block (RDB) (TYPE)

Customer number (CUST)

Route number (ROUT)

Designator field for trunk (DES)

Trunk type (TKTP)

Incoming and outgoing trunk (ICOG)

Access code for the trunk route (ACOD)

Trunk type M911P (M911P)

The route is for a virtual trunk route (VTRK)

- Zone for codec selection and bandwidth management (ZONE)  Range: 0 - 255

- Node ID of signaling server of this route (NODE)  Range: 0 - 9999

- Protocol ID for the route (PCID)

Integrated services digital network option (ISDN)

- Mode of operation (MODE)

- D channel number (DCH)  Range: 0 - 254

- Interface type for route (IFC)

Private network identifier (PNI)

Network calling name allowed (NCNA)

Network call redirection (NCRD)

- Trunk route optimization (TRO)

- Recognition of DT12 ABCD FALT signal for ISL (FALT)

- Channel type (CHTY)

- Call type for outgoing direct dialed TIE route (CTYP)

- Insert ESN access code (INAC)

- Integrated service access route (ISAR)

- Display of access prefix on CLID (DAPC)

- Mobile extension route (MBXR)

Copyright © 2002-2009 Nortel Networks. All rights reserved.

Figure SIPL 12a – Route configuration for SIPL service

Integrated services digital network option (ISDN)

- Mode of operation (MODE)

- D channel number (DCH)  Range: 0 - 254

- Interface type for route (IFC)

- Private network identifier (PNI)  Range: 0 - 32700

- Network calling name allowed (NCNA)

- Network call redirection (NCRD)

- Trunk route optimization (TRO)

- Recognition of DT12 ABCD FALT signal for ISL (FALT)

- Channel type (CHTY)

- Call type for outgoing direct dialed TIE route (CTYP)

- Insert ESN access code (INAC)

- Integrated service access route (ISAR)

- Display of access prefix on CLID (DAPC)

- Mobile extension route (MBXR)

**+ Basic Route Options**

**+ Network Options**

**+ General Options**

**+ Advanced Configurations**

Figure SIPL 12b – Route configuration for SIPL service

+ Routes and Trunks --> Routes and Trunks --> CUS# --> Route# --> Add Trunks

**NORTEL** CS 1000 ELEMENT MANAGER Help | Logout

Routes and Trunks > Routes and Trunks > Customer 0, Route 80, Trunk 1 Property Configuration

### Customer 0, Route 80, Trunk 1 Property Configuration

**- Basic Configuration**

Input Description	Input Value
Trunk data block (TYPE)	IPTI
Terminal Number (TN)	100 0 07 00
Designator field for trunk (DES)	SIPL
Extended Trunk (XTRK)	VTRK
Route number, Member number (RTMB)	80 1 *
Level 3 Signaling (SIGL)	<input type="text"/>
Card Density (CDEN)	8D
Start arrangement Incoming (STR)	Immediate (IMM)
Start arrangement Outgoing (STRO)	Immediate (IMM)
Trunk Group Access Restriction (TGAR)	0
Channel ID for this trunk. (CHID)	1
Increase or decrease the member numbers (INC)	Increase channel and member number (YES)
Class of Service (CLS)	Edit

**+ Advanced Trunk Configurations**

Figure SIPL 13 – Trunk configuration for SIPL service


9. SIPL phone configuration

+ Phones --> Add --> choice UEXT-SIPL phone --> preview

**NORTEL** CS 1000 ELEMENT MANAGER Help | Logout

Managing: **EM on campus4(100.20.44.162)**  
Phones > Phone Details

### Phone Details



System: EM on campus4  
Phone Type: UEXT-SIPL  
Sync Status: TRN

[General Properties](#) | [Features](#) | [Keys](#) |

#### General Properties

Customer Number:  \*

Terminal Number:

Designation:  \*

Zone:  \*

SIP User Name:  \*

Copyright © 2002-2009 Nortel Networks. All rights reserved.

Figure SIPL 14a – SIPL phone configuration



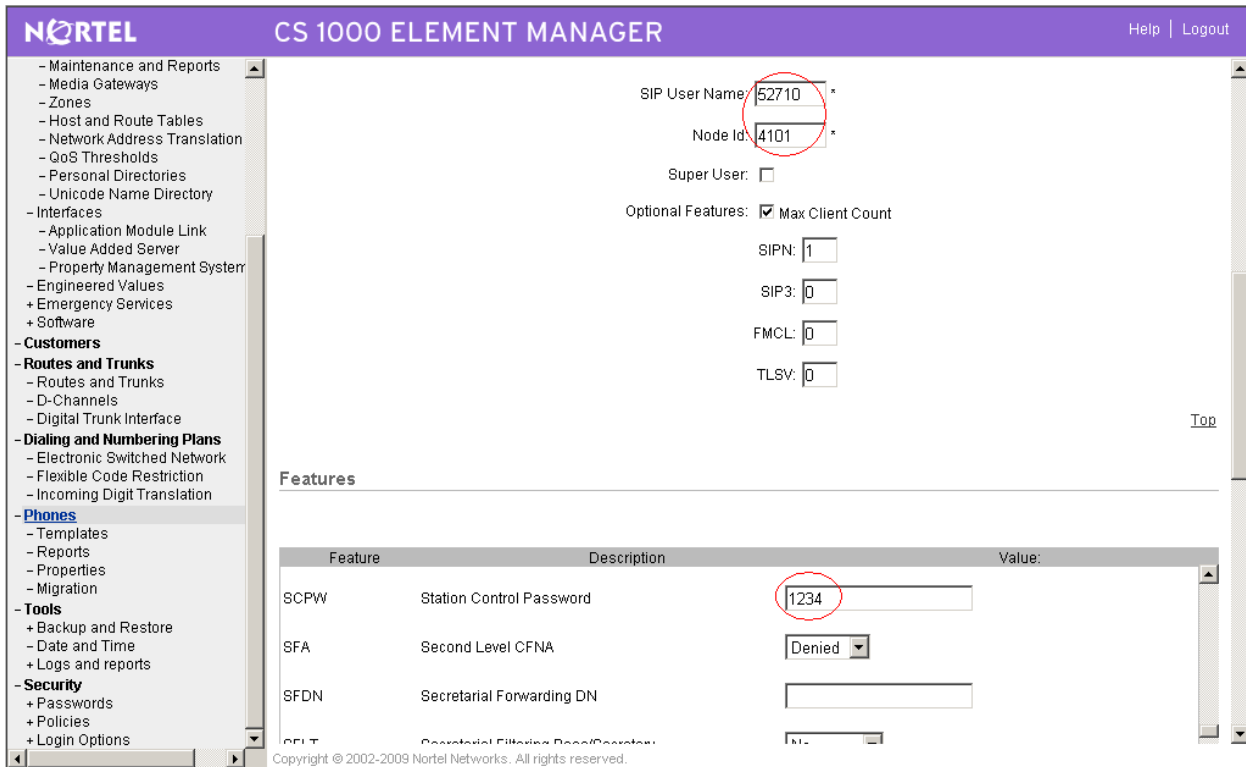


Figure SIPL 14b – SIPL phone configuration

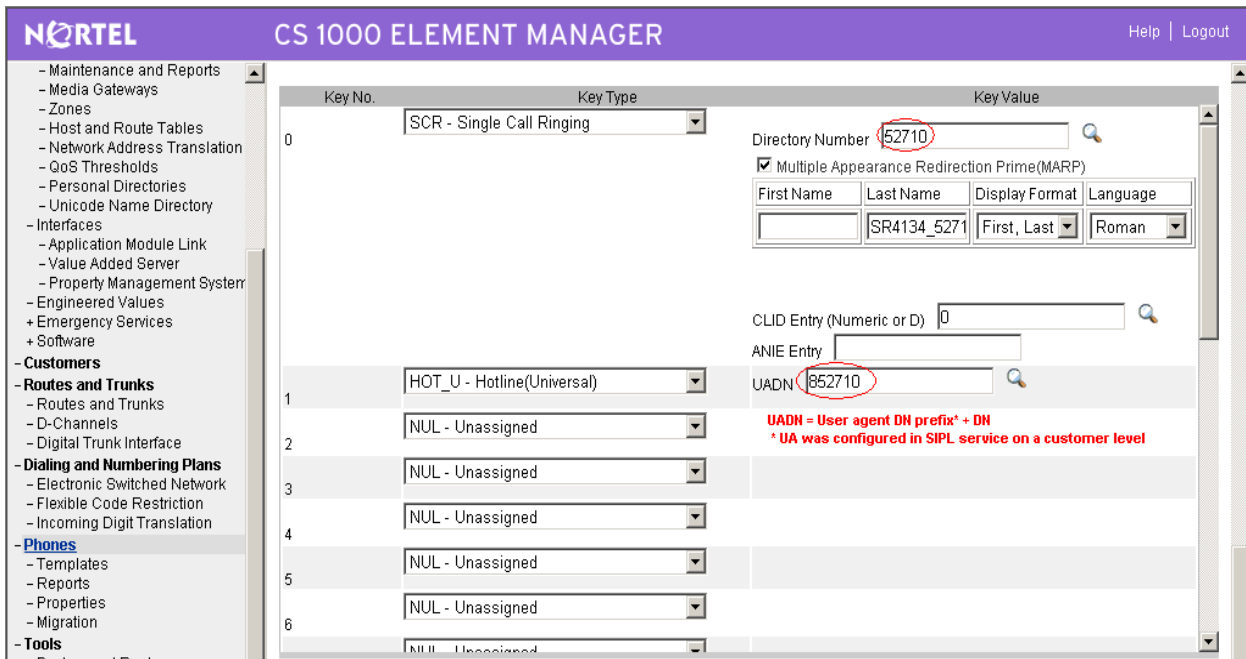


Figure SIPL 14c – SIPL phone configuration

## SSG Configuration

Please refer to CS 1000 document for detailed information on SSG configuration. SIPL needs a SSG server to route an external call to NRS (Network Routing Service). SIPGW and H323GW endpoints will be configured in SSG to register on specific NRS server.

### Steps

- 1) Deploy Signaling Server software application on the Linux server

The screenshot displays the Nortel UCM Deployment Manager interface. The top header shows the Nortel logo and the title 'UCM DEPLOYMENT MANAGER'. The left sidebar contains navigation links: «UCM Network Services, Deployment Targets, Software Loads, and Backups. The main content area is titled 'Managing: DEPLOYMENT MANAGER' and shows details for a 'Target Deployment' on host 'ws2' (Type: IBM X306M). The server status is 'Undeployed', and the current operation status is 'None'. A table of software applications is visible, with 'SS' (Signaling Server) selected.

Deployment package	Description
<input type="checkbox"/> EM	Element Manager
<input type="checkbox"/> NRS	Network Routing Service
<input type="checkbox"/> NRS+SS	Signaling Server and Network Routing Service
<input type="checkbox"/> SIPL	SIP Line
<input checked="" type="checkbox"/> SS	Signaling Server
<input type="checkbox"/> SubM	Subscriber Manager

Figure SSG 1 – SSG application deployment

- 2) SSG node configuration:

**+ Nodes: Servers, Media Cards**

**NORTEL** CS 1000 ELEMENT MANAGER Help | Logout

Managing: 100.20.44.162 Username: admin  
System » IP Network » IP Telephony Nodes

### Node Details (ID: 4100 - LTPS, Gateway ( SIPGw, H323Gw ))

Node ID:  \* (0-9999)

Call Server IP Address:  \*

**Telephony LAN (TLAN)**  
Node IP Address:  \*  
Subnet Mask:  \*

**Embedded LAN (ELAN)**  
Gateway IP address:  \*  
Subnet Mask:  \*

**IP Telephony Node Properties**

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN

**Applications (click to edit configuration)**

- Terminal Proxy Server (TPS)
- Gateway (SIPGw & H323Gw)
- Personal Directories (PD)

\* Required Value. Save Cancel

### Associated Signaling Servers & Cards

Select to add    Print | Refresh

<input type="checkbox"/>	Hostname	Type	Deployed Applications	ELAN IP	TLAN IP	Role
<input type="checkbox"/>	campus4	Signaling Server	LTPS, Gateway, PD	100.20.44.162	100.20.45.162	Leader

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list.

Figure SSG 2 – SSG node details

**NORTEL** CS 1000 ELEMENT MANAGER Help | Logout

Managing: 100.20.44.162 Username: admin  
System » IP Network » IP Telephony Nodes

### Node ID: 4100 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services | H.323 Gateway Settings

Vtrk Gateway Application:  Enable gateway service on this Node

**General**

Vtrk Gateway Application:

SIP Domain name:  \*

Local SIP Port:  \* (1 - 65535)

Gateway endpoint name:  \*

Gateway password:  \*

H.323 ID:  \*

Enable failsafe NRS:

**Virtual Trunk Network Health Monitor**

Monitor IP Addresses (listed below)  
Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

**SIP Gateway Settings**

TLS Security:

\* Required Value. Save Cancel

Note: Changes made on this page will NOT be transmitted until the Node is also saved.

Figure SSG 3 – SIPGw and H323Gw endpoints configuration

## 3) Specify a NRS server for SIPGw endpoint:

**NORTEL CS 1000 ELEMENT MANAGER** Help | Logout

Managing: 100.20.44.162 Username: admin  
System » IP Network » IP Telephony Nodes

Node ID: 4100 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services | H.323 Gateway Settings

**SIP Gateway Settings**

TLS Security: Security Disabled

Port: 5061 (1 - 65535)

Number of Byte Re-negotiation: 0

Options:  Client Authentication  
 X509 certificate authority

**Proxy Or Redirect Server:**

Primary TLAN IP Address: 100.20.42.77 Secondary TLAN IP Address: 100.20.42.82

Port: 5060 (1 - 65535) Port: 5060 (1 - 65535)

Transport protocol: TCP Transport protocol: TCP

Options:  Support registration  Support registration  
 Primary CDS Proxy  Secondary CDS Proxy

CLID Presentation:

\* Required Value. Note: Changes made on this page will NOT be transmitted until the Node is also saved. Save Cancel

Figure SSG 4 – Specify a NRS server for SIPGw endpoint

## 4) Specify a GateKeeper server (NRS) for H323Gw endpoint:

**NORTEL CS 1000 ELEMENT MANAGER** Help | Logout

Managing: 100.20.44.162 Username: admin  
System » IP Network » IP Telephony Nodes

Node ID: 4100 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services | H.323 Gateway Settings

Auto Number	Auto Number Use	Insert Number
<input type="checkbox"/> 77002	Auto Number is DN	

**H.323 Gateway Settings**

Primary gatekeeper (TLAN) IP Address: 100.20.42.77

Alternate gatekeeper (TLAN) IP Address: 100.20.42.82

Primary Network Connect Server (TLAN) IP Address: 100.20.42.77

Primary Network Connect Server Port number: 16500 (1 - 65535)

Alternate Network Connect Server (TLAN) IP Address: 100.20.42.82

Alternate Network Connect Server Port number: 16500 (1 - 65535)

Primary Network Connect Server timeout: 10 (1 - 30)

\* Required Value. Note: Changes made on this page will NOT be transmitted until the Node is also saved. Save Cancel

Figure SSG 5 – Specify a GateKeeper server(NRS) for H323Gw endpoint

# NRS/SPS Configuration

Please refer to CS 1000 NN43001-130 Network Routing Service Fundamentals document for detailed information on NRS/SPS configuration. The Network Routing Service (NRS) provides routing services to both SIP and H.323-compliant devices. The NRS allows customers to manage a single network dialing plan for SIP, H.323, and mixed SIP/H.323 networks. Therefore SIPGw and H323Gw endpoints of SSG and Secure Router endpoint have to register on NRS server.

## Steps

- 1) Deploy NRS software application on the Linux server

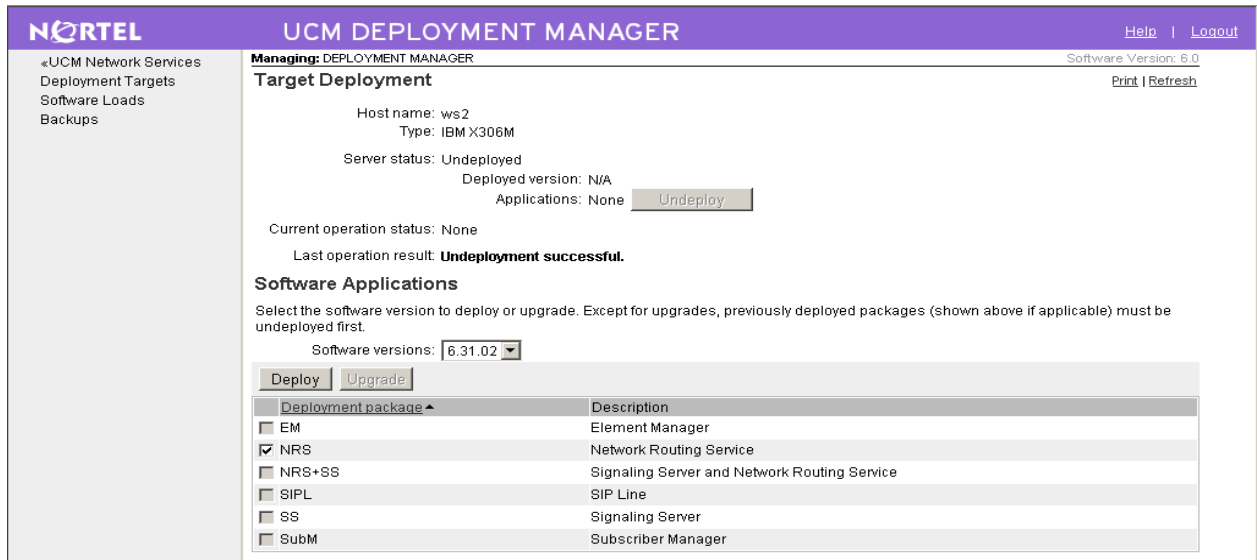


Figure NRS 1 – NRS application deployment

## 2) NRS server configuration

The screenshot displays the 'NRS Server' configuration page in the Nortel Network Routing Service Manager. The interface includes a sidebar with navigation options like 'System', 'Numbering Plans', and 'Tools'. The main content area shows the 'Service Status' section with buttons for 'Enable', 'Graceful disable', and 'Restart'. Below this is a table listing three services: SIP Proxy Server (SPS), Gatekeeper (GK), and Network Connection Server (NCS), all of which are currently 'In service'. The 'Server Configuration' section is expanded to show 'NRS Setting' with fields for Host name (sps-client), Primary TLAN IP address (100.20.42.77), Secondary TLAN IP address (100.20.42.82), and other parameters like Control priority, Server mate communication port, Realm name, and Server role. There is also a section for 'H.323 Gatekeeper Settings' with a 'Location request (LRQ) response timeout' set to 3.

Figure NRS 2 – NRS server configuration

## 3) SSG endpoint configuration

The screenshot shows the 'Edit Gateway Endpoint' configuration page in the Nortel Network Routing Service Manager. The page title is 'Edit Gateway Endpoint ( nortel.com / udp / cdp )'. The 'Managing' section indicates the system is on a 'Standby database' at IP 100.20.44.95. The configuration form includes fields for 'End point name' (set to 'campus4'), 'Description' (set to 'CAMPUS 4 SSL'), and 'Trust Node' (checked). Other fields include 'Tandem gateway endpoint name' (set to 'Not Applicable'), 'Endpoint authentication enabled' (set to 'Authentication off'), and several 'E.164' dialing access code fields (country, area, international, national, and local) which are currently empty. A 'Save' button and a 'Cancel' button are located at the bottom right of the form.

Figure NRS 2a – SSG endpoint configuration

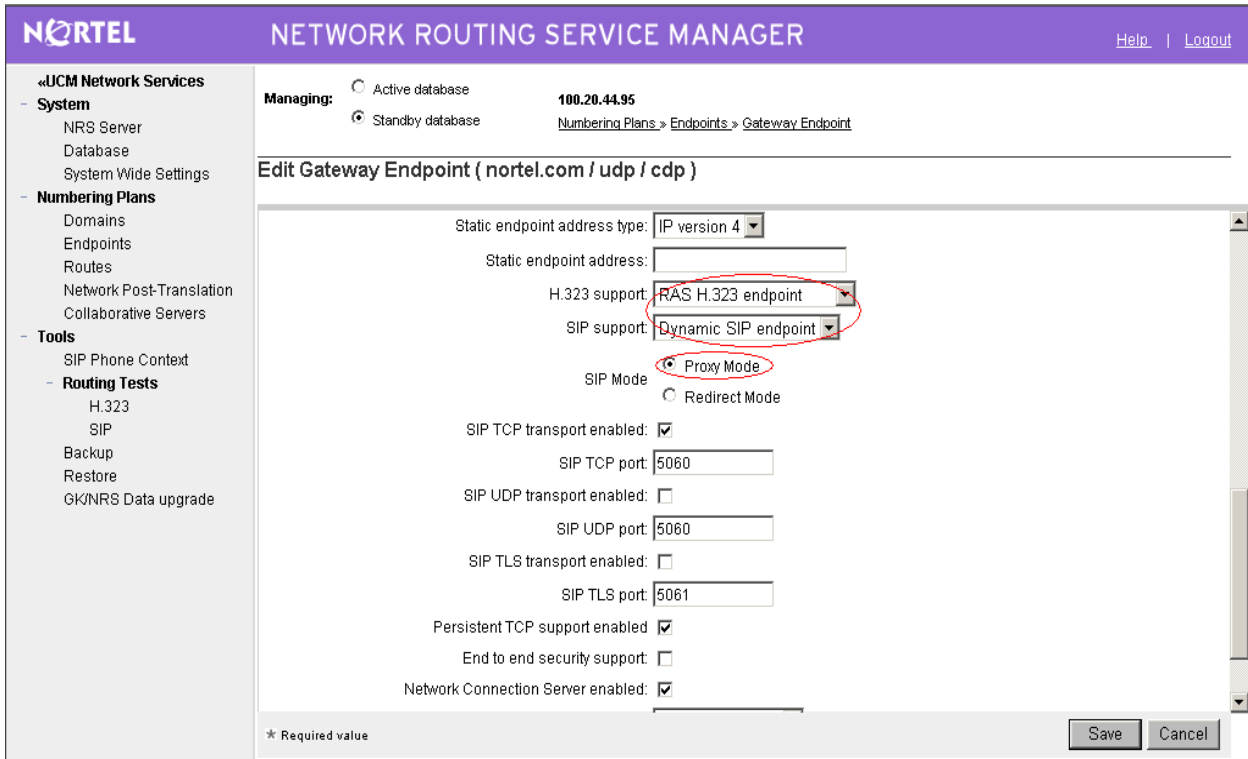


Figure NRS 2b – SSG endpoint configuration

4) Dialing plan routes for SSG endpoint configuration:

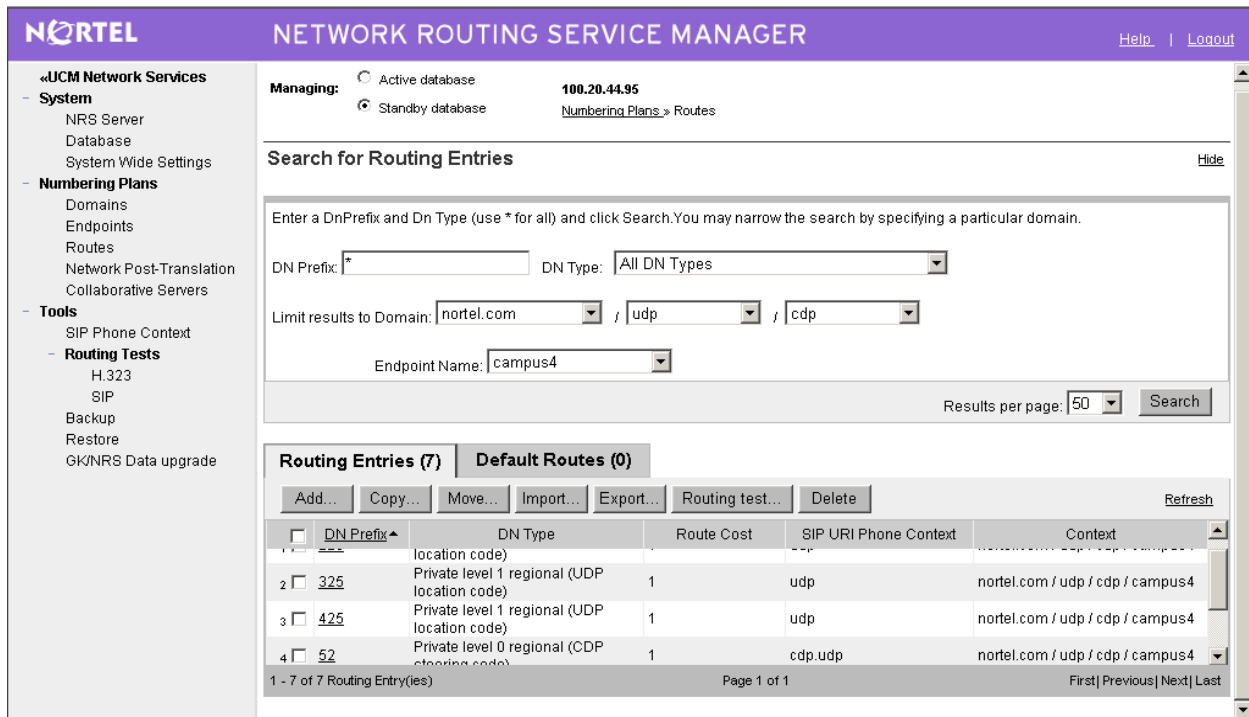


Figure NRS 3 – Dialing plan routes for SSG endpoint configuration

## 5) SSG endpoint registration status

The screenshot shows the NRS interface with the following details:

- Managing:** Active database, 100.20.44.95
- Search for Endpoints:** Endpoint ID: \* (with a search button)
- Limit results to Domain:** All service domains, All L1 domains, All LD domains
- Gateway Endpoints (23) / User Endpoints (3):**

ID	Supported Protocols	SIP Mode	Call Signaling IP	Description	# of Routing Entries	Context
2	endpoint / Static SIP endpoint	Proxy Mode	100.20.41.181	in lab 23	2	cdp
3	RAS H.323 endpoint / Dynamic SIP endpoint / NCS	Proxy Mode	100.20.45.163 / 100.20.45.163	CAMPUS 4 SSL	2	interop.com / udp / cdpe
4	Dynamic SIP endpoint	Proxy Mode	100.20.45.170		1	sipdecte.com / udpe / cdpe
5	Static SIP endpoint	Proxy Mode	100.20.45.173		0	interop.com / udp / cdp

Figure NRS 4 – SSG endpoint registration status

## 6) SR 2330/4134 endpoint configuration

The screenshot shows the NRS interface with the following details:

- Managing:** Standby database, 100.20.44.95
- Edit Gateway Endpoint ( nortel.com / udp / cdpe )**
- End point name:** SR4134 \*
- Description:** SR4134 endpoint
- Trust Node:**
- Tandem gateway endpoint name:** Not Applicable
- Endpoint authentication enabled:** Authentication on
- Authentication password:** [Empty field]
- E.164 country code:** [Empty field]
- E.164 area code:** [Empty field]
- E.164 international dialing access code:** [Empty field]
- E.164 international dialing code length:** [Empty field] (0-99)
- E.164 national dialing access code:** [Empty field]
- E.164 national dialing code length:** [Empty field] (0-99)
- E.164 local (subscriber) dialing access code:** [Empty field]

Figure NRS 5a – SR 2330/4134 endpoint configuration



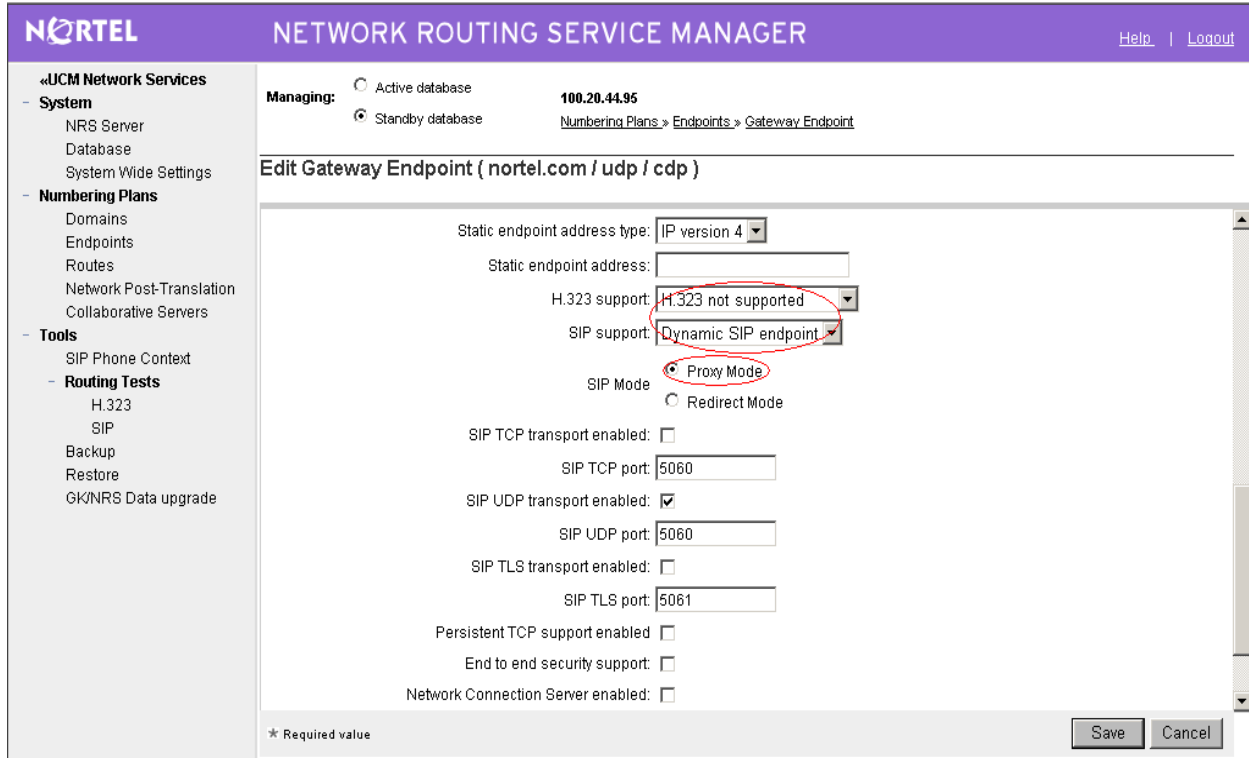


Figure NRS 5b – SR 2330/4134 endpoint configuration

7) Dialing plan routes for SR 2330/4134 endpoint configuration:

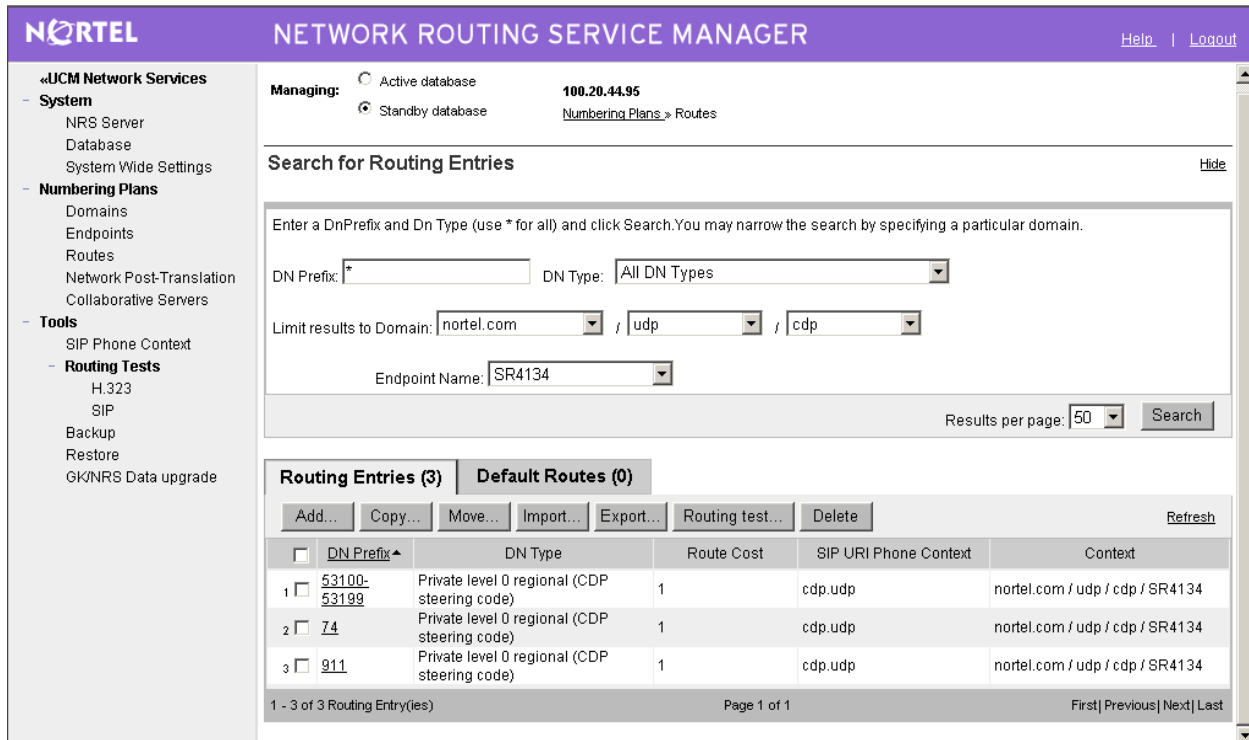


Figure NRS 6 – Dialing plan routes for SR 2330/4134 endpoint configuration

## 8) SR 2330/4134 endpoint registration status

The screenshot shows the Nortel Network Routing Service Manager (NRS) interface. The main content area displays the following information:

- Managing:** Active database (selected), Standby database (unselected). IP: 100.20.44.95. Link: [Numbering Plans > Endpoints](#)
- Search for Endpoints:** Search box for Endpoint ID, dropdowns for Domain (All service domains, All L1 domains, All L0 domains), and a Search button.
- Gateway Endpoints (23) | User Endpoints (3):** A table listing endpoints. The endpoint SR4134 is circled in red.

ID	Supported Protocols	SIP Mode	Call Signaling IP	Description	# of Routing Entries	Context
20 nmc	Static SIP endpoint	Proxy Mode	100.20.44.10	NMC	1	interop.com / udp / cdp
21 SR4134	Dynamic SIP endpoint	Proxy Mode	100.20.42.80		3	interop.com / udp / cdp
22 SRG50R3	RAS H.323 endpoint / Static SIP endpoint / NCS	Proxy Mode	100.20.41.180 / 100.20.41.180		0	interop.com / udp / cdp

Figure NRS 7 – SR 2330/4134 endpoint registration status

## SIP Clients Configuration

Configure the branch SIP endpoints to use SSM bind IP address as the Outbound Proxy ie.100.20.42.80:5060.

Please ensure that the SIP username and domain need to match the CS 1000 SIP Line settings. username@domain represents a globally unique identifier for a SIP user.

## CS 1000 Patches

Below patches are needed for version **CS: 600R LB: 6.00.18 LA: 6.00.18** of the CS 1000 system:

- ✓ nortel-CS 1000-sps-6.00.18.17-01.i386.000
- ✓ nortel-CS 1000-vtrk-6.00.18.23-08.i386.000

For higher versions of CS 1000, please refer Meridian PEP Library at

[http://qtcf0n6.ca.nortel.com/mpl/core\\_menu\\_view.cfm](http://qtcf0n6.ca.nortel.com/mpl/core_menu_view.cfm)

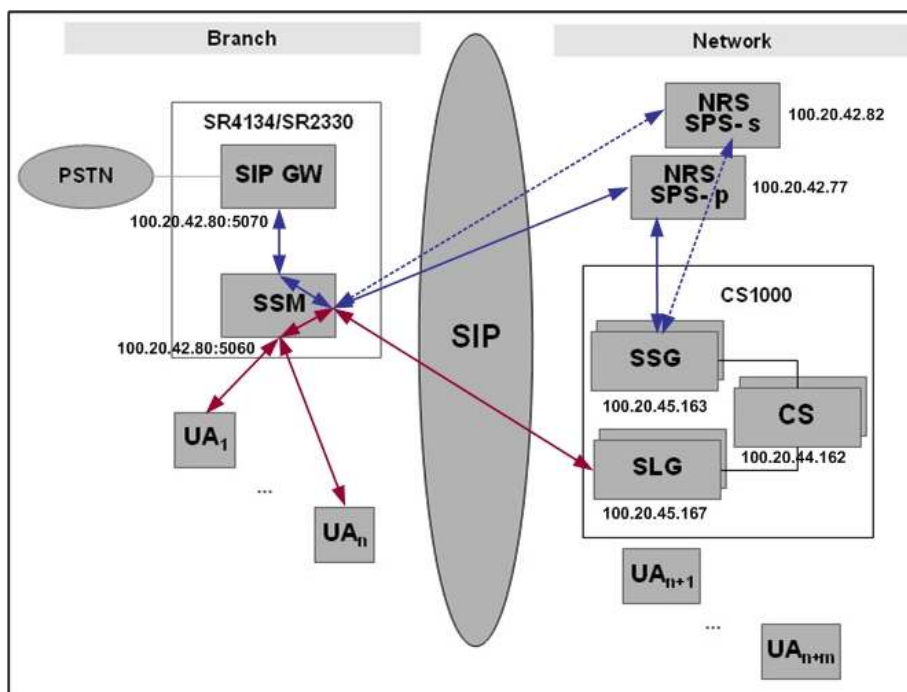
If you don't find the required versions in PEP Library please contact Nortel support.

## SR 2330/4134 Configuration

This section describes the configuration steps needed for SR 2330/4134 for CS 1000 branch solution. The following diagram complete with IP addresses will be used as reference for this chapter.

For configuration details on SSM, please refer to Secure Router Release 10.2 guide NN47263-510 Configuration — SIP Survivability.

For configuration details on SIP Gateway (SIP GW) please refer to Secure Router Release 10.2 guide NN47263-508 Configuration — SIP Media Gateway.



### Steps

1. Configure the Ethernet interface for connection to the SIP server and SIP phones:

```
configure terminal
interface ethernet 0/1
ip address 100.20.42.80 255.255.255.224
exit ethernet
```

2. Configure a default route to the branch router:

```
ip route 0.0.0.0/0 100.20.42.65
```

3. Configure the SIP Media Gateway to listen on port 5070:

```
voice service voip  
sip  
bind all ipv4:100.20.42.80:5070  
exit sip  
exit voip
```

4. To configure the SIP Survivability Module, bind the IP interface for SIP traffic using default port 5060:

```
voice service voip  
ssm  
bind ip ipv4:100.20.42.80
```

5. Enable SSM:

```
enable
```

6. Configure dialplan. Normal mode NTML is used to route gateway calls to SPSs and to replace IP address of SPS to domain name. Survivable dial plan is optional. Configure it only if number translation is required in survivable mode.

```
dialplan  
load normal normal_cs1k.ntm  
load survivable backup_cs1k.ntm  
exit dialplan
```

7. Enable SSM keepalives to configure SLG ip-address and monitor connectivity with SLG:

```
sip-server  
keepalive-server ipv4:100.20.45.167:5070 interval 60 retries 2 transport udp
```

8. Configure SSM domain to specify SLG domain:

```
domain dns:interop.com  
exit sip-server
```

9. Configure SSM Call Admission Control on the WAN interface connecting SLG:

```
cac  
max-calls ethernet0/1 256
```

10. Configure the CAC exclusion pool that identifies the IP address range of the SIP endpoints that use SSM:

```
exclude-pool 100.20.47.0 255.255.255.0  
exit cac
```

11. Point the SSM to the SIP Media Gateway IP interface as the default gateway (specifying the non-default port), Port should be same as configured for gateway's listening port in step 3.:

```
default-gateway ipv4:100.20.42.80:5070 transport udp  
exit ssm  
exit voip
```

12. Configure the outbound proxy on the SIP Media Gateway to point to the SSM:

```
sip-ua  
outbound-proxy ipv4:100.20.42.80:5060
```

13. Configure the primary and secondary SPS for the SIP Media Gateway:  
(No need to configure secondary sip-server if there is only one SPS used):

```
sip-server ipv4:100.20.42.77:5060  
sip-server ipv4:100.20.42.82:5060 secondary
```

14. Configure authentication parameters to be used for gateway to SPS calls and registration:

```
authentication SR 4134 1234
```

15. Configure keepalive to monitor primary and secondary SPS connectivity:

```
keepalive target sip-server  
keepalive target sip-server secondary
```

16. Configure dynamic registration from SR gateway to active SPS.

```
register dynamic  
exit sip-ua
```

17. Configure voice ports for FXS phones  
(example for 2 FXS phones connected to port 2/1 and 2/2)

```
voice-port 2/1  
signal loop-start  
station number 74001
```

```
no shutdown
exit voice-port
```

```
voice-port 2/2
signal loop-start
station number 74002
no shutdown
exit voice-port
```

18. Configure PRI interface bundle.  
(example to configure PRI E1 bundle on port 3/1 with switch-type as qsig)

```
interface bundle E1PSTN
link pri_e1 3/1 voice
isdn
switch-type primary-qsig
activate
exit isdn
exit bundle
```

19. Optional translation profile configuration.  
a. Configure translation profile for PSTN to SPS calls. (Example to translate 335.. number to 5.. numbers.) There can be more than 1 rule which can be called or calling or both numbers.

```
voice translation-rule 100
rule 1 /335/ /5/
exit translation-rule
```

```
voice translation-profile pstn2sps
translate calling 100
translate called 100
exit translation-profile
```

- b. Configure translation profile for SPS to PSTN calls. (Example to translate 5.. numbers to 335..)

```
voice translation-rule 200
rule 1 /5/ /335/
exit translation-rule
```

```
voice translation-profile sps2pstn
translate calling 200
translate called 200
exit translation-profile
```

20. Configure Dial peer for FXS phones:

```
dial-peer voice pots 1
destination-pattern 74001
port 2/1
forward-digits all
no shutdown
exit pots
```

```
dial-peer voice pots 2
destination-pattern 74002
port 2/2
forward-digits all
no shutdown
exit pots
```

21. Configure Dial peer for PRI interface and (optionally) apply translation profile.

(Following dial peer is for calls coming from SPS with a number starting with 53 to be translated to a number starting with 3353 before sending on PRI. Don't use translation profile if no translation required. )

```
dial-peer voice pots 3
destination-pattern 53.%
port 3/1
forward-digits all
no shutdown
translation-profile outgoing sps2pstn
exit pots
```

(Following dial peer is for calls coming from PSTN with a number starting with 3353 to be translated to a number starting with 53 before sending to SPS. Don't use translation profile if no translation required. )

```
dial-peer voice pots 4
destination-pattern 3353.%
port 3/1
forward-digits all
no shutdown
translation-profile incoming pstn2sr
exit pots
```

➔ If no translation required than instead of dial-peer 3 and 4, only 1 dial peer is required with destination-pattern 53.% (assuming that all PRI numbers are starting with 53).

➔ Following is an example if a 911 call is to be routed to PRI interface.

```
dial-peer voice pots 5
destination-pattern 911
port 3/1
forward-digits all
no shutdown
```

## NTML Examples

### Example of Normal mode NTML (normal\_cs1k.ntm)

This NTML is used by SSM to route gateway calls to active SPS (100.20.42.77 or 100.20.42.82) with domain nortel.com.

```

<translation>
  <address-switch field = "original-destination" subfield = "host">
    <address is = "100.20.42.77">
      <replace string=" nortel.com" field="destination" subfield="host">
        <replace string=" nortel.com" field="origin" subfield="host">
          <replace string=" nortel.com" field="original-destination" subfield="host">
            <route host="100.20.42.77" add-route="yes" replace-host ="no"/>
          </replace>
        </replace>
      </replace>
    </address>
    <address is = "100.20.42.82">
      <replace string=" nortel.com" field="destination" subfield="host">
        <replace string=" nortel.com" field="origin" subfield="host">
          <replace string=" nortel.com" field="original-destination" subfield="host">
            <route host="100.20.42.82" add-route="yes" replace-host ="no"/>
          </replace>
        </replace>
      </replace>
    </address>
  </address-switch>
</translation>

```

### Example of Backup mode NTML (backup\_cs1k.ntm)

This NTML is optional. Here is an example assuming that calls with certain prefix in backup mode needs to be converted to a 5 digit number extension.

```

<translation>
  <number-switch>
    <number is = "967?????">
      <drop literals = "3"/>
    </number>
    <number is = "613967?????">
      <drop literals = "6"/>
    </number>
    <number is = "1613967?????">
      <drop literals = "7"/>
    </number>
  </number-switch>
</translation>

```