IP Telephony...
Clear and Simple

Welcome to
BOSâNOVA
IP Telephony

Gateway Administrator’s Guide

DISCOVERY
telecom

BOSCOM LICENSE AGREEMENT AND WARRANTY

IMPORTANT — READ CAREFULLY

This BOScom License Agreement (the "AGREEMENT") is a legal agreement between you (either an individual or a single entity) and BOScom for the product accompanying this AGREEMENT. The product includes computer software, associated media and printed materials, and may include "online" or electronic documentation (the "SOFTWARE"). The PRODUCT may also include hardware (the “HARDWARE”). The SOFTWARE and the HARDWARE are referred to, collectively, as the PRODUCT.

BY INSTALLING AND/OR USING THE PRODUCT YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT.

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY ERASE ALL COPIES OF THE SOFTWARE IN YOUR POSSESSION, AND RETURN THE SOFTWARE AND ANY ACCOMPANYING HARDWARE TO THE PLACE FROM WHICH YOU OBTAINED IT.

COPYRIGHT.

All title and copyrights in and to the PRODUCT are owned by BOScom. The PRODUCT is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

GRANT OF LICENSE FOR THE SOFTWARE.

The SOFTWARE is licensed, not sold. BOScom grants to you a non-exclusive, non-transferable, royalty-free right to install and use the SOFTWARE, provided that the SOFTWARE will be used by a single person on a single computer and for personal non-commercial, internal use only. If accompanied by a proof-of-purchase document specifying "site license," "company license," or any other multiple-user type license scheme, then the terms of that document shall override this single-user restriction. Any rights not expressly granted herein are retained by BOScom.

OTHER RESTRICTIONS.

This AGREEMENT is your proof of license to exercise the rights granted herein and must be retained by you. You may not rent, lease, reverse engineer, decompile, modify, or disassemble the PRODUCT, or create derivative works based on the PRODUCT.

LIMITED HARDWARE WARRANTY

The HARDWARE is protected against defects in material and workmanship, under normal use, for one (1) year from the original purchase date.

If the HARDWARE fails to perform within the abovementioned warranty period, you must return the PRODUCT to BOScom and prepay any shipping charges, export taxes, custom duties and taxes, or any charges associated with transportation of the Product. In addition, you are responsible for insuring the PRODUCT shipped or returned and assume the risk of loss during shipment.

All returned PRODUCTS must be accompanied by a description of the problem, a proof of the place and date of purchase, and the original shipping and packing materials.

BOScom shall, at its sole discretion, either repair the PRODUCT or replace it with a product of the same functionally. Replacement products may be refurbished or contain refurbished materials. If BOScom cannot repair or replace the PRODUCT, BOScom will refund the depreciated purchase price of the PRODUCT.

This limited warranty does not apply to any PRODUCT not purchased from BOScom, or from a BOScom authorized reseller, or on which the serial number has been removed or defaced. This limited warranty also does not cover any PRODUCT that has been damaged or rendered defective as a result of (a) improper transportation or packing when returning the PRODUCT to BOScom; (b) use of the PRODUCT other than in accordance with its instructions, or other misuse or abuse of the PRODUCT; (c) modification of the PRODUCT; (d) service by anyone other than a BOScom-approved agent; (e) unusual physical or electrical stress or interference, failure or fluctuation of electrical power, lightning, static electricity, improper temperature or humidity, fire, or acts of God.

The maximum liability of BOScom under this limited warranty is limited to the purchase price of the PRODUCT covered by the warranty.

BOScom reserves the right to refuse PRODUCTS (i) that are not covered by the warranty; or (ii) for which there is no problem found. Such PRODUCTS shall be returned to the purchaser at purchaser’s expense.

DISCLAIMER.

EXCEPT AS EXPRESSLY STATED ABOVE OR AS REQUIRED BY LAW, BOSCOM DISCLAIMS ANY WARRANTY FOR THE PRODUCT. THE PRODUCT IS PROVIDED "AS IS" WITHOUT REPRESENTATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES

OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. BOSCOM ASSUMES NO RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE PRODUCT.

NO LIABILITY FOR CONSEQUENTIAL DAMAGES.

IN NO EVENT SHALL BOSCOM, ITS AGENTS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DIRECT, INDIRECT, SPECIAL OR OTHER CONSEQUENTIAL OR INCIDENTAL DAMAGES; DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING DIRECTLY OR INDIRECTLY OUT OF THE USE OF OR INABILITY TO USE THE PRODUCT, EVEN IF BOSCOM HAS BEEN ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

Because some states or jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

U.S. GOVERNMENT RESTRICTED RIGHTS.

For purchases made in the United States: The SOFTWARE and any accompanying documentation are provided with restricted rights. Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (b) (3) and (c) (1) (ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software-Restricted Rights at 48 CFR 52.227-19, as applicable.

AMENDMENTS.

BOScom may amend these terms and conditions at any time by posting a notice on one or more of its websites. Your continued use of the PRODUCT shall constitute your acceptance of such amended terms. Accordingly, we urge you to visit our websites periodically to review the current and effective terms and conditions for use of our products. Certain provisions of these terms and conditions may be superceded by expressly designated legal notices or terms outlined on our websites.

GOVERNING LAW.

This AGREEMENT and any and all claims relating to the PRODUCT shall be governed by the laws of the State of Israel, without regard to or application of choice of law or principles, and the courts of Tel-Aviv Jaffa shall have sole and exclusive jurisdiction over any dispute arising in connection with this Agreement and/or the use of the PRODUCT.

NO WAIVER.

No delay or failure to take action under these terms and conditions will constitute a waiver by BOScom unless expressly waived in writing by a duly authorized officer of BOScom.

Credit Notice to Netbricks:

BOScom purchased the source code for the ISDN PRI/BRI stack used in the next generation of BOScom PRI and BRI Gateways from Netbricks (http://www.netbricks.net/). Netbricks is a leading developer and supplier of portable software compliant with protocol standards as published by the governing institutions around the world.

EC Declaration Of Conformity

Manufacturer’s Name: BOScom Ltd.

Manufacturer’s Address: Rabin House
Teradion Industrial Park
D.N. Misgav 20179 Israel

Responsible Person: Yuval Barnea

Model number: BOSâNOVA E1/T1 VoIP Gateway

Description Of Equipment: VoIP Gateway that exchanges phone calls and fax transmissions between a PBX and data networks.

Year of Manufacturer: 2002

Directive Complied With: **EMC**: 89/336/EEC as amended by 92/31/EEC and 93/68/EEC

LVD: 73/23/EEC as amended by 93/68/EEC and 93/465/EEC

Harmonized Standards to which Conformity is Declared:
EN 55022: 1998 Class B
EN 55024: 1998
EN 61000-3-2: 1995 + A1; A2: 1998
+A14: 2000
EN 61000-3-3: 1995
EN60950:1992 + A1 + A2 + A3 + A4 + A11
IEC60950: 1991 + A1 + A2 + A3 + A4

We, the undersigned, hereby declare that the machinery specified above conforms to the above Directives and Standards.

Manufacturer:

Signature: Y. Barnea Date: September 19, 2002 Position: Engineering Manager

Full Name: Yuval Barnea Place: BOScom Ltd.

FCC Part 15

NOTE:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

TABLE OF CONTENTS

Section 1: Introduction 1
Package Contents 3
System Requirements 4
Using this Document 4
Guide to the Configurator Main Menu 5

Section 2: Installation 8
Safety Recommendations 9
Mounting the BOSâNOVA Gateway 10
PRI Cable Tester — On Claro PRI Gateways Only 10
Inspecting the PRI Cable 11
    PRI Cables for BOSâNOVA V–Series PRI Gateways 11
Back Panel Connections 13
    FXS 16-Port Back Panel 13
    FXS and FXO 4 and 8 Port Back Panel 15
    PRI Back Panel 16
    Claro E1/T1 PRI Gateway Back Panel 18
    Claro Analog Front Panel 20
LED Function Following Power Up 21
Startup Procedure 22
    Configuring the IP address via the Maintenance Wizard 22
    Configuring the IP address using the Terminal Server 23
    Configuring the IP address using Internet Explorer 26
    Configure the Officer Gateway's IP Address 27
Installing a Modem 28
    Requirements 28
    Installation 28
Installation Troubleshooting 30

Section 3: Configuring Dialing Parameters 31
Interactive Voice Responses (IVR) 32
    Enabling and Disabling Embedded IVR Scenarios 33
    Recording and Installing Embedded IVR Announcements 34
    Downloading and Uploading Libraries 36
H.323 Parameters 37
SIP (Session Initiation Protocol) 38
Fax Support 39
NAT Support 40
Advanced Parameters 41

Section 4: Configuring Voice and Telephony Parameters 43
Codec 44
    Displaying the Codec Parameter Table 44
    Explanations of the Columns 45
    Changing the Settings of a Codec 46
    Changing the Prioritization of a Codec 47

Volume 49
Answer Supervision 50
    Voice Detection 50
    Battery Reversal 51
Disconnect Supervision 52
    PBX Tones 52
    Threshold 54
    Silence Detection 55
    Power Denial — For Claro Analog Gateways 56
Timeout 57
Advanced 58
    Country/Impedance 58
    Echo Canceller 59
    BOS Tones 59
    Jitter Buffer 61
    Silence Suppression 61
    Voice Packet Priority—Tagging Packets 62
Statistic Servers 64
    Call Details Records (CDR) Server 64
    Q–CDR Server 64
    Quality Status Reporting (QSR) Server 65
Quality of Service (QoS) 65
    Enabling QoS in a Gateway 65
    Setting Test Frequency and Threshold 66

Section 5: Signal Analyzer 67
The Disconnect Signal Analyzer 68
    Before Running the DSA Wizard 68
    Method of Operation 68
The Dial Tone Analyzer 70

Section 6: V-Series and Claro PRI Configuration 71
Reviewing the Current Configuration 72
Changing the Configuration 73
B-channel Selection 77
The Restore Buttons 77
The Actions Drop-down List 78

Section 7: Numbering Plan Overview 80
Connection Types that are Supported 81
Network Configuration 82
Structure of a Telephone Number 83
    ITU E.164 Standard 83
    Other Components of a Telephone Number 84
How the Numbering Plan Works 85
The Basics of Configuration 88

Saving a Numbering Plan 89
Components of the Numbering Plan 90
  Private-Number Prefixes 91
  Maximum Private-Number Length 94
  Dial Public Numbers and/or Terminate Hop-off Calls 96
  Automatic Dialing 98
  The Officer Gateway 102
  Private to Public Number Associations 103
  Features Unique to Claro Configuration 104

Section 8: Numbering Plan Wizard 107
Guide to the Pages of The Numbering Plan Wizard 108
The Welcome Page 109
  Initial Numbering Plan Configuration 109
  Reconfiguring the Numbering Plan 110
Assigning a Descriptive Name 111
Connection Type 112
Selecting H.323 or SIP 113
Defining Claro Analog Port Grouping 114
  Associated Tables 115
Entering Claro Analog Group Information 116
  Associated Tables 118
Assigning Port Information 119
  Associated Tables 121
Assigning Private-Numbers 122
  Associated Tables 124
Assigning Private-Number Prefixes 125
  Associated Tables 127
Defining and Applying Hop-off Prefixes 128
  Associated Tables 131
Dialing public numbers 132
Configuring Automatic Dialing 134
Defining Claro PRI Phone Number Blocks 136
  Associated Tables 138
Defining Claro Analog Phone Numbers Per Port 139
  Associated Tables 141
Defining Force Dialout Direction 142
Review the Numbering Plan Configuration 143

Section 9: Numbering Plan Wizard—Connection Configuration 144
Connection Type 145
Configuring Gatekeeper as the Connection Type 147
  Procedure 147
  Registration Parameters: Service Prefixes 150
Configuring SIP Proxy as the Connection Type 153
  Procedure 153

Section 10: Numbering Plan Configurator Procedures 156
Overview of the Numbering Plan Configurator 157
Completion Rule Mode 158
Enabling Completion Rule Mode 158
Creating Rules for Completion Rule Mode 158
Forced Overlap Mode 159
Enabling Forced Overlap Mode 159
Creating Rules for Forced Overlap Mode 159
Testing the Application of Completion Rules 161
Hop-on Numbers 162
IP Bypass 163
Adding an Phone Number to the IP Bypass List 163
Adding a Caller ID to the IP Bypass List 164
Changing an IP Bypass Phone Number or Caller ID 165
Least Cost Routing (LCR) 166
Configuring LCR per BOSâNOVA Gateway 166
Enabling and Disabling BOSâNOVA Gateways for LCR 168
Configuring LCR for Third-Party Gateways 169
Enabling and Disabling Third-party Gateways for LCR 170
Maximum Private-number Length 171
Private to public number Associations 172
Rule Based Number Management 174
General Comments 174
Examples of RBNM 176
Creating and Applying RBNM 178
Operation Code and Operands for RBNM 180
Formal Operand Definition for RBNM 182
Session Initiation Protocol (SIP) 183
Configuring SIP Proxy Parameters 184
Adding and Associating Phone Number Prefixes 186
Conversion Rules 188
Third Party Gateways 189
What is a Mask? 191
Third Party IP Telephony Service Providers 193
Adding an IP Telephony Service Provider 193
Adding a Prefix 195
Adding a RBNM Rule 196

Section 11: Miscellaneous Aspects of the Numbering Plan Module 197
Verifying a Numbering Plan 198
Using the Test Button 200
How Gateways Accept Phone numbers 201
Inter-digit Time-out 202

Section 12: Using the Officer Gateway 203

Responsibilities of the Officer 204

Enabling and Disabling the Uniqueness Check 205

Network-wide Multi-path Priorities 206

Assigning Hop-off Prefix Priorities 206

Assigning Mask Priorities 208

Enabling and Disabling Gateways for LCR 209

Configuring Private Number Length 210

Authentication 210

Implementing Authentication 211

Adding a PIN to the Hop-off PIN List 212

Authentication for Caller ID Numbers 213

Authentication for BOSâNOVA Connects and Link & Talks 214

Authentication for Third-party Gateways 215

Creating Hop-off Schemes 216

Dialing Server 218

Assigning an Officer 218

Changing Officers 219

Adding a New Private 220

Reviewing Gateways' Synchronization Status 221

Updating Common Dialing Tables 224

Customize Log 225

Section 13: Network Address Translation 226

NAT Overview 227

Problems Arising from the NAT Process 227

Configuring NAT Support 228

Employing the Parameter: NET ID 228

Location of the Officer Gateway 229

Configuring End-points Behind a NAT 229

TCP/IP Ports Used by BOSâNOVA Gateways 232

TCP/IP Ports Used by BOSâNOVA Connect 234

Section 14: BOSâNOVA Connect and Connect Lite 235

BOSâNOVA Connect System Requirements 236

Installing a BOSâNOVA Connect 237

Upgrading a BOSâNOVA Connect 242

Manual Installation of the Driver 243

Reviewing Current Connect Configuration 245

Configuring a BOSâNOVA Connect with an Officer 246

Adding a Connect to the Officer Gateway 246

Modifying a Connect Configuration from the Officer Gateway 247

Configuring the Connect to Locate the Officer 248

Section 15: BOSâNOVA Link & Talk 249

Overview 250

Link & Talk System Requirements 251

TCP/IP Ports Used by Link & Talk 251

Link & Talk and the Officer Gateway 252

Adding a Link & Talk to the Officer Gateway 252

Modifying a Link & Talk Configuration from the Officer Gateway 253

Establishing the Link & Talk Web Site 254

Background: The Building Block Files 254

Creating the Link & Talk Web Presence 255

Creating the Link & Talk Tag 255

Examples of Link & Talk HTML 257

Reviewing Current Link & Talk Configuration 259

Installing a Link & Talk PC Plug-in 260

Uninstalling Link & Talk 260

Using Link & Talk 261

Troubleshooting 262

Section 16: Gateway Monitor 263

Overview 264

Gateway Log Monitor 264

Gateway Ports Monitor 266

Call Detail Records (CDR) 267

Quality of Service Records (QSR) 269

Section 17: Blue Seal Security Lock 271

Internal Firewall Settings 272

Configuring the Blue Seal Security Lock 273

Turning Off the Blue Seal Security Lock 273

Selecting a Protection Level 273

Remote Management 274

Using the Maintenance Wizard 274

Using a PC and a Serial Connection (RS-232) 275

Firewall Specifications 276

Section 18: Command Line Configurator and Hidden Parameters 278

Accessing the Command Line Configurator 279

Command Line Configurator (CLC) Commands 280

Sample CLC Procedure—How to change the Maximum Call Duration 282

Summary of Command Line Configurator Tutorial 285

Running Scripts Using the Command Line Configurator 285

Hidden Parameters 286

Section 19: Maintenance Wizard's Primary Applications 293
Running the Maintenance Wizard 294
Reviewing Product Information 295
Finding Gateways and Reviewing Their Status 296
Gateway with an Undefined IP Address 298
Connecting to a Gateway With a Known Address 299
Updating Software 301
Online Monitoring 302
Getting the Trace Files and Saving them Locally 303
Getting Current Trace Buffer 305
Listing Critical Trace Files 306
Setting the Diagnostic Levels 307
Opening the Terminal Server 308
Terminal Server Options 309
Checking the IP Connection to a Gateway or Computer 310
Configuring Network Time Protocol 312

Section 20: Maintenance Wizard's Secondary Applications 314
Copying Gateway Configuration Files to Another Location 315
Uploading Configuration Files 317
Setting Maximum Call Duration 318
Get the Trace Files Saved During the Previous Restart and Check for Emergency Traces 320
Setting the Date and Time 321
Binary Trace Transfer 322
Configuring IP Settings 324
Configuring a Modem 325
Changing the System Password 326
Configuring an SNMP Traps and Alarms Server 327
Configuring CDR and QSR buffers 328
Checking Open TCP/IP Ports 329

Section 21: SNMP 331
Support of SNMP Managers 332
Importing BOScom Private MIBs 332
Defining to which SNMP Managers a Gateway Sends Traps 333
Using the BOScom SNMP Manager Demo 334
Installing the BOScom SNMP Manager 334
Running the BOScom SNMP Manager 334
Using the BOScom SNMP Manager Main Screen 335
Adding a Gateway to the Registered Gateway List 336
Deleting a Gateway 336
CDR Table Content 336
Scanning the Network for Gateways 337
Viewing MIBs 338
Listening for Traps 339
Clearing the Traps Log 339

HP OpenView 340
Importing MIBS into HP OpenView 340
Checking the MIB Registration Tree 342
Checking Data Values of BOScom Private MIBs 342
Setting Traps and Alarms in HP OpenView 343

Section 22: Call Detail Records 345
Overview 346
CDR Buffer 346
CDR Server 346
How CDR Works—A Summary 347
CDR Components 348
Installing the CDR Depository and SSH Software 348
The CDR Parser 349
The MS SQL Server 351
CDR File Formats and Structures 352
Structure of the CDR File Header 352
Structure of the CDR Buffer File 353
Description of CDR Fields as Presented in MS SQL 356

Section 23: Web Support and FAQs 359
Using the BOScom VoIP Web Site 360
Frequently Asked Questions 363

Section 24: Index to the BOSâNOVA Gateway Administrator’s Guide...... 367

IP Telephony...
Clear and Simple

SECTION 1: INTRODUCTION

BOSâNOVA™ IP Telephony LAN/ WAN Gateways seamlessly integrate telephones, fax machines, PBXs, and remote BOSâNOVA Connects with your IP network into a single, superior enterprise telephony solution. The result: decreased communication costs as toll-free long-distance calls are placed over your TCP/ IP network, and dramatic reduction of telephony equipment costs by creation of an optimal communication environment that supports all functionality provided by the existing PBX, such as IVR, call forwarding, conferencing, and customizable recorded messages.

Standard BOSâNOVA Gateways are available as FXO and FXS analog Gateways as well as E1/ T1 PRI digital Gateways.

The BOSâNOVA Claro™ Gateway is also available in both digital and analog formats. Unlike the standard BOSâNOVA Gateways, the Claro is placed at the intersection between the PSTN, the PBX, and the IP network. Routing over the IP or the PSTN is automatic and fully user transparent. This means that dialing around the IP network is precisely the same as dialing around the PBX network, without the need to selectively access one network over another. “Native dialing” enables the caller to place calls naturally without considering the route. No retraining of users is required.

Advantages

- Guarantees high voice quality based on patent- pending QoS algorithms, even over public WANS such as the Internet
- Enables 5-minute Gateway installation aided by an intuitive installation wizard, and includes self-learning techniques for streamlined equipment expansion
- Features centralized, browser-based management and simple-to-use configuration menus for single-point administration of calling parameters, user lists, and security definitions

Browser-based management is available only via Microsoft Internet Explorer, version 5.0 and higher with a JVM. See “System Requirements” on page 4.

- Provides optimized interoperability based on the standard H.323 v.3 protocol to work with other H.323 compatible terminals, gateways, and gatekeepers, such as Microsoft NetMeeting, Cisco, AudioCodes, RADVision via IP Enhanced Communication Server, and others

- Offers a flexible codec licensing scheme enabling “mix-and-match” of supported codecs (G. 723.1, G. 729A, G. 711 A- law / µ- law and NetCoder ®) to satisfy specific customer requirements and scaled pricing
- Supports a wide range of applications enabled by the convergence of the voice and data networks, including call encryption, recording, monitoring, and statistics

Unique Algorithms Guarantee Call Quality

Call quality is preserved even over public WANs (such as the Internet) using unique patent-pending algorithms. BOScom’s proprietary technology provides built-in redundancies whereby packets are sent via multiple routes to ensure delivery and to improve QoS—even when QoS level degrades or the network malfunctions. Call quality is further increased by the ability of our Gateways to transfer calls with poor quality to the PSTN.

Ease of Installation

For those that are familiar with IP Telephony gateways, the BOSâNOVA LAN/ WAN Series provides a refreshing and dramatic change from the current offering. Simple and secure access, provided via Microsoft Internet Explorer, enables installation within minutes. The Disconnect Signal Analyzer Wizard allows the most complex configuration parameters to be set (such as identification of on-hook signals in FXO Gateway installations) using a sequence of tab-through screens wherein a single parameter is required; the single parameter is the phone numbers of two extensions that are connected to the Gateway.

To simplify the installation and avoid errors, a unique algorithm broadcasts information about the newly installed Gateway to all the other BOSâNOVA IP Telephony family members on the network.

Remote Monitoring and Control

The remote monitoring and control system simplifies both the installation and maintenance of the Gateways, since it allows problems to be localized and identified. The system’s design allows it to be monitored remotely yet securely, enabling remote upload of new versions, version maintenance, traces, and collection and analysis of statistics regarding Gateway operation and call/network quality. The administrator can choose to store Gateway configuration files on the network from a remote workstation, and then download them to a local computer. Gateway configurations can be exchanged or duplicated by simply copying and transferring the required configuration file over the network to the new gateway.

Secure Environment

BOSâNOVA Gateways are protected against hackers and other non-authorized personnel with three levels of security protection:

- Encrypted remote management
  Secure Shell™ (SSH) server software and proprietary encryption protocols secure against Internet hacking during remote management.
- Gateway level/Call level authentication
  To protect against toll fraud, BOSâNOVA Gateways enable restrictions to be set on Gateways and specify which callers are authorized to enter the network. In addition, user usage can be defined.
- Built-in firewall
  BOSâNOVA Gateways feature an embedded firewall providing protection against global data manipulation from within and outside the organization. The firewall can be configured to varied levels of security, including total block-out of all data except for VoIP. Select models, including all BOSâNOVA Claro Gateways, also feature the BOSâNOVA Blue Seal Security Lock™, that is, a mechanical means of configuring the gateway firewall.

Information- Rich Communication Environment

The BOSâNOVA Gateways maintain a log of errors and activities, and produce a detailed Call Detail Reporting (CDR) message at the end of every conversation. This message includes (in addition to the standard data, such as who called whom, length of conversation, etc.) statistical information about the call quality.

PACKAGE CONTENTS

The BOSâNOVA Gateway box includes the following:

- A BOSâNOVA VoIP Gateway Installation Guide
- One BOSâNOVA Gateway
- One power cable
- One Centronic cable with a crone for connection to a PBX for BOSâNOVA Gateways with more than 8 ports (cable #CB0058)
- Four self-adhesive rubber feet for table-top installation
- Two mounting brackets for 19-inch rack-closet mounting
- If ordered, one 9-foot, 50 pin to 50 pin, Centronic cable with accompanying RJ-11 brick for BOSâNOVA for BOSâNOVA Gateways with more than 8 ports (product #BOS7501)
- One ferrite core

SYSTEM REQUIREMENTS

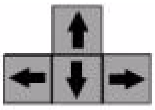
For a computer to display the BOSâNOVA Gateway Configurator, it must meet the following minimum requirements:

PC Processor	Pentium 133
Memory	32 Mb
Operating System	Windows 9x/Me or NT/2000/XP
Browser	• Microsoft Internet Explorer, version 5.0 or higher • A Java Virtual Machine (JVM) which can run Java version 1.1. **NOTE:** The Configurator has been tested, and is known to run excellently, on the Microsoft JVM. The Configurator was not tested using the Sun JVM. Installation of the Microsoft JVM is available from the BOSâNOVA CD-ROM Welcome screen. In addition, following is the address of a portal providing links to Microsoft JVM download sites: http://java-virtual-machine.net/download.html

USING THIS DOCUMENT

If you are viewing this document in an Adobe Reader, navigation is simplified by the following:

- **All page numbers are links**. Place the cursor over any page number and the cursor will turn into a hand, similar to this: 👆. Click any page number and the focus will jump to the designated area of the document.
- **Bookmarks are links**. The cursor will turn into a hand. Click and the focus will jump to the Bookmark entry.
- Click **F5** to toggle Bookmarks in and out of view.
- Use the right and left arrow keys to move forward or backward one page at a time.
- Use the up and down arrow keys to move up and down the page one line at a time (unless you are in full screen mode).
- To return to the previous focus, click the **Go To Previous View** button.



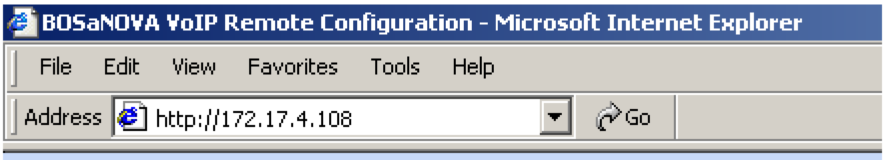
GUIDE TO THE CONFIGURATOR MAIN MENU

The Gateway Configurator is a browser based management tool which displays simple-to-use configuration menus for single-point administration of most aspects of a BOSâNOVA IP Telephony network.

Browser-based management is available only via Microsoft Internet Explorer, version 5.0 and higher with a JVM. See "System Requirements" on page 4.

To open a Gateway's Configurator:

1. Enter the Gateway's IP address in the Microsoft Internet Explorer **Address** field.

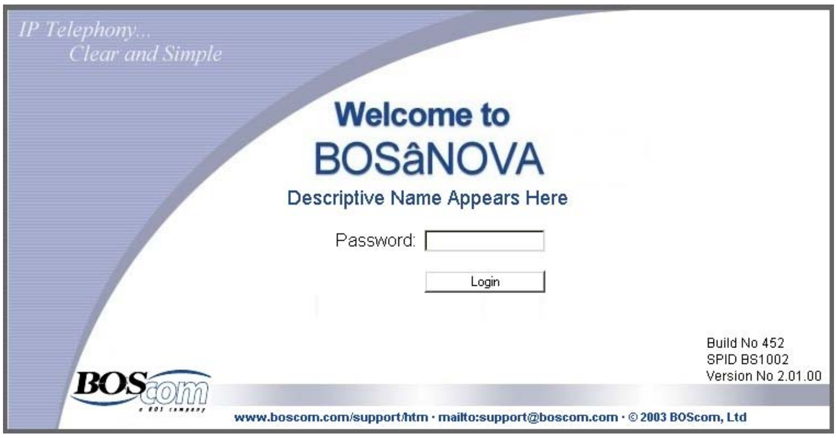


BOSaNOVA VoIP Remote Configuration - Microsoft Internet Explorer

Address http://172.17.4.108

2. Click **Go**. The "Welcome to BOSâNOVA" screen is displayed.

The first time you connect to the Gateway Configurator, a java applet will be downloaded to your computer. Depending upon the Internet connection, this may take up to three minutes.



IP Telephony...
Clear and Simple

Welcome to
BOSâNOVA
Descriptive Name Appears Here

Password:

Build No 452
SPID BS1002
Version No 2.01.00

www.boscom.com/support/htm · mailto:support@boscom.com · © 2003 BOScom, Ltd

3. Enter the password and click **Login**. The Configurator main menu is displayed.

The VoIP and Tools menus of the Gateway Configurator main menus vary according to Gateway type.

Figure 1: Claro PRI Configurator Main Menu

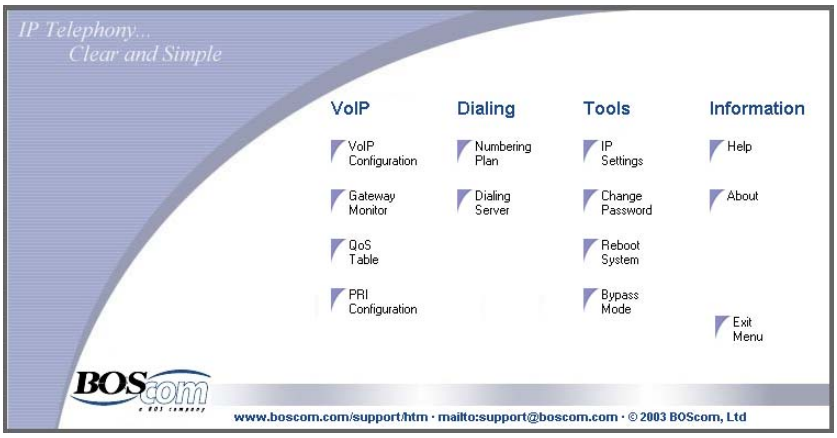
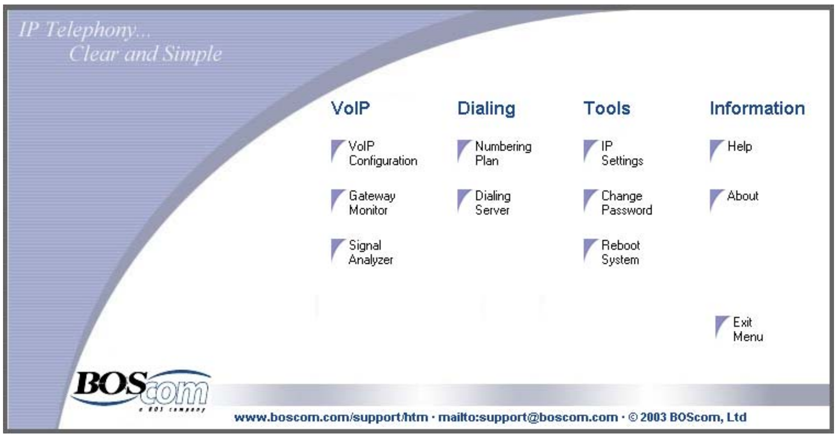


Figure 2: BOSâNOVA FXO Configurator Main Menu



The following table lists, in alphabetical order, the selections on the Configurator main menu and provides a brief explanation of each. The page number of the first relevant page of documentation is also listed.

Table 25: Selections on the Configurator Main Menu

Selection	Explanation	Page
About	Click to view the Gateway’s version, build, ID, and serial numbers as well as other information.	none
Bypass Mode	Only on Claro Gateways. Click to configure the Gateway’s response to PSTN to PBX calls, and PBX to PSTN calls. During normal use this setting should remain at **Fully active**.	none
Change Password	Click to change the Gateway’s password.	none
Dialing Server	Click to review the Gateway’s interaction with other Gateways.	218
Exit	Click to close the Gateway’s Configurator.	none
Gateway Monitor	Click to review port activity and CDR and QoS data. The Gateway’s Log is also here.	263
Help	Click to open the fantastic browser-based **Help**.	none
IP Settings	Click to change the System name or IP address.	none
Numbering Plan	Click to open the Numbering Plan Configurator.	80
PRI Configuration	Click to open the PRI Configurator.	71
QoS Table	Optional. Click to configure modem backup and the QoS relationship between Gateways.	65
Reboot System	Click to disconnect all active ports and reboot the Gateway.	none
Signal Analyzer	On FXO Gateways only. Click to run the Disconnect Signal Analyzer Wizard.	67
VoIP Configuration	Click to open the VoIP Configurator.	31

SECTION 2: INSTALLATION

This section contains explanations and procedures about the installation of both analog and digital Gateways. Some sections are not applicable to both.

- Safety recommendations, see p. 9
- Mounting the Gateway, see p. 10
- Inspecting a PRI cable, see p. 11
- Back or front panel connections
  - FXS 16 port Gateways, see p. 13
  - FXS and FXO 4 and 8 port Gateways, see p. 15
  - E1/T1 PRI Gateways, see p. 16
  - Claro PRI Gateway, see p. 18
  - Claro Analog Gateway, see p. 20
- LED functioning, see p. 21
- Configuring the IP address
  - Using the Maintenance Wizard, see p. 22
  - Using the Terminal Server, see p. 23
  - Using a browser, see p. 26
- Installing a modem, see p. 28
- Installation troubleshooting, see p. 30

SAFETY RECOMMENDATIONS

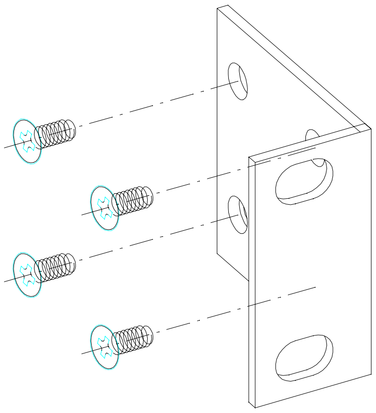
- Ensure that the Gateway is grounded. Faulty grounding may result in improper operation and/or a safety hazard. If the power outlet does not supply adequate grounding, use the grounding screw on the back panel for external grounding. (See *Back Panel Connections* on page 13.)
- Check the power at the site to ensure that it is free of spikes and noise. If necessary, install a power conditioner.
- Ensure that there is adequate over-current (fuse or circuit breaker) protection.
- Follow standard Electrostatic Discharge Damage (ESD) prevention procedures. Static discharge can cause immediate or intermittent equipment problems.
- Ensure that the cables are not exposed to sources of electrical noise (such as radios, transmitters, and broadband amplifiers).
- Ensure that the Gateway is installed in a clean, air-conditioned location. Accumulation of dust can cause malfunctioning.
- Ensure that the Gateway cover is securely attached. A poorly attached cover results in poor air circulation.
- Telecommunication lines must be disconnected before unplugging the main power connector and while the cover is removed.

MOUNTING THE BOSâ NOVA GATEWAY

The Gateway can be placed on a desk or shelf or can be mounted in a standard 19-inch rack-closet. A maximum of four Gateways can be stacked on top of each other.

Before setting the Gateway on a desk or shelf, and before stacking Gateways, affix the four self-adhesive rubber feet (supplied).

Two brackets with screws are supplied for rack-closet mounting.



The brackets are attached to the sides of the Gateway, flush with the front panel. Screws to affix the Gateway to the rack-closet are not supplied.

If the rubber feet are attached, the Gateway might not fit into a 19-inch rack-closet.

PRI CABLE TESTER — ON CLARO PRI GATEWAYS ONLY

The rear panel of a Claro PRI Gateway includes two testers:

- **PRI Tester–Wires**
  Insert a pair of wires into the tester—one wire per tester port—to determine if they supply either a PSTN or a PBX transmit signal. The LEDs of the RJ-45 tester light up accordingly. Then, assemble the RJ-45 connector and test it in the PRI RJ-45 Tester.
- **PRI Tester–RJ45**
  Insert an RJ-45 connector into the tester. If the left LED lights up, the RJ-45 connector is wired for a PSTN connection. If the right LED lights up, the RJ-45 connector is wired for a PBX connection.

See the following chapter for additional details regarding the wiring of a PRI RJ-45 adapter.

INSPECTING THE PRI CABLE

The following rules concern configuration of the PRI cable for different BOSâNOVA PRI Gateways:

- For **BOSâNOVA V–Series** PRI Gateways:
  Always inspect the 8-pin RJ- 45 connector on the PRI cable. It may be necessary to cross wires. Details and procedures are included in this section.
- For **BOSâNOVA Claro** PRI Gateways:
  In most Claro PRI installations—that is, when the PBX has an RJ-45 connector to which the PRI cable from the PSTN is connected—there is no need to inspect the 8-pin RJ- 45 connector. Straight Ethernet cables should be used. However, a PBX may also have a different connector type, in which case special cable(s) must be prepared.

PRI Cables for BOSâNOVA V–Series PRI Gateways

Inspect the 8-pin RJ- 45 connector on the PRI cable. It may be necessary to cross wires. The Gateway's female RJ-45 socket has the following pin out:

Pin number	Line type
1	not connected
2	not connected
3	Rx
4	Tx
5	Tx
6	Rx
7	not connected
8	not connected

This pin out does not depend upon which ISDN function group (network or terminal) is defined for the Gateway.

Telephone Switching System Defined as ISDN "Terminal"

In most cases, these are typical settings for PBX switches.

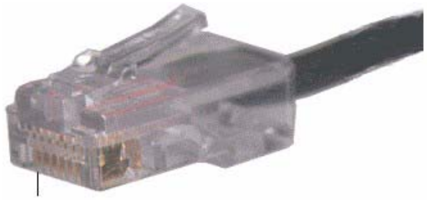
Telephone switch side	Gateway side RJ-45 male connector
1 and 2 (Rx)	4 and 5 (Tx)
4 and 5 (Tx)	3 and 6 (Rx)
	Pins 1, 2, 7, and 8 must be disconnected

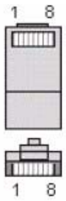
Telephone Switching System Defined as ISDN “Network”

In most cases, these are typical settings for public switches.

Telephone switch side	Gateway side RJ-45 male connector
1 and 2 (Tx)	3 and 6 (Rx)
4 and 5 (Rx)	4 and 5(Tx)
	Pins 1, 2, 7, and 8 must be disconnected

The following graphics illustrate the location of the pins on the RJ-45:





BACK PANEL CONNECTIONS

In addition to the power supply connection, the following ports exist on the back panel of every Gateway:

- PS/2 port for the keyboard
- 15-pin VGA port for the monitor
- 9-pin COM port
- RJ-45 port for the LAN or crossover cable

Upon delivery, the first three ports are hidden by a security cover.

FXS 16-Port Back Panel

If the power outlet does not supply adequate grounding, ***connect an external ground at ID #9****.*

This diagram illustrates the back panel connections of the FXS 16 port Gateways. Note that the 50 pin connector for lines 1–16 is attached to the ***lower*** slot.

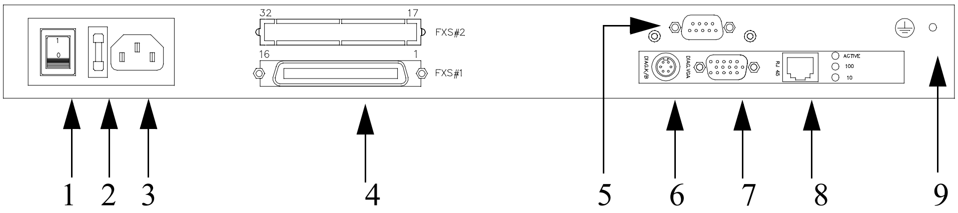
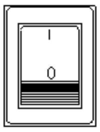
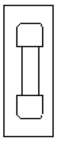
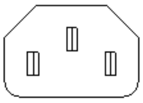
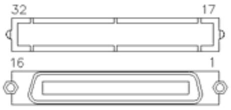
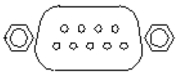
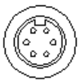
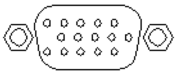
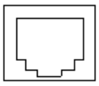
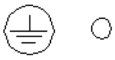
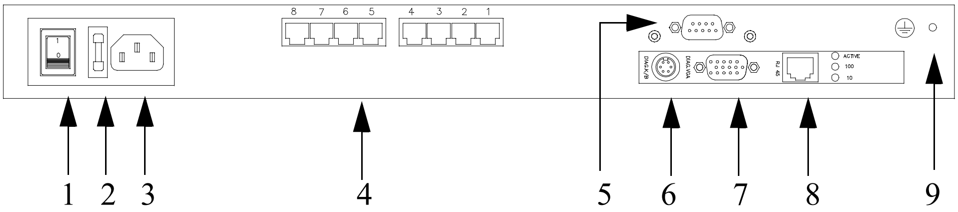


Table 26: Ports on FXS 16 Port Gateways

ID #	Graphic	Description
1		On/Off switch | = on 0 = off
2		Fuse chamber The fuse is housed behind a cover. Pop off the cover with a screwdriver.
3		The power cable is inserted into this socket.
4		The Sub-D 50 pin connectors from the PBX are inserted into this port. They may include small screws that are used to secure the connector.
5		A modem for QoS, or testing equipment such as a loop-back device, can be connected to the Gateway using this Sub-D 9 pin connector.
6		A keyboard can be connected to the Gateway using this mini-DIN 6 pin connector.
7		A monitor can be connected to the Gateway using this Sub-D 15 pin high-density connector.
8		Connect the Gateway to the Internet (LAN or WAN) using this RJ-45 port.
9		If the power outlet does not supply adequate grounding, ***connect an external ground to the screw at the right of the ground symbol.***

FXS and FXO 4 and 8 Port Back Panel

This diagram illustrates the back panel connections of the FXS and FXO 4 and 8 port Gateways. Note that phone line number 1 is located on the ***right***, not on the left.



If the power outlet does not supply adequate grounding, ***connect an external ground at ID #9****.*

Table 27: Ports on FXS and FXO 4 and 8 Port Gateways

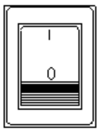
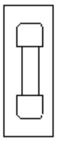
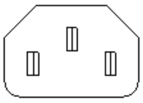
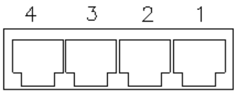
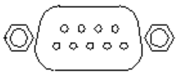
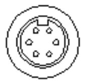
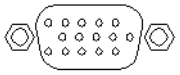
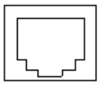
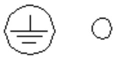
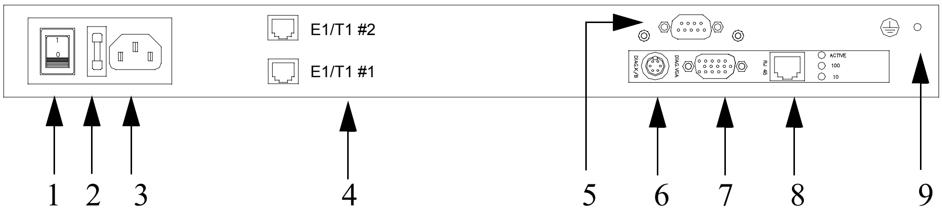
ID #	Graphic	Description
1		On/Off switch | = on 0 = off
2		Fuse chamber The fuse is housed behind a cover. Pop off the cover with a screwdriver.
3		The power cable is inserted into this socket.
4		RJ-11 plugs from telephones, fax machines, and other telephony equipment, or from an analog PBX, are inserted into these ports.
5		A modem for QoS, or testing equipment such as a loop-back device, can be connected to the Gateway using this Sub-D 9 pin connector.

Table 27: Ports on FXS and FXO 4 and 8 Port Gateways

ID #	Graphic	Description
6		A keyboard can be connected to the Gateway using this mini-DIN 6 pin connector.
7		A monitor can be connected to the Gateway using this Sub-D 15 pin high-density connector.
8		Connect the Gateway to the Internet (LAN or WAN) using this RJ-45 port.
9		If the power outlet does not supply adequate grounding, ***connect an external ground to the screw at the right of the ground symbol.***

PRI Back Panel

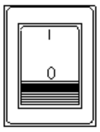
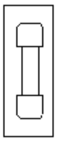
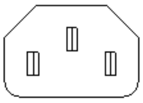
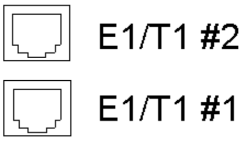
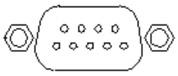
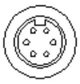
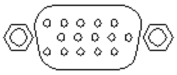
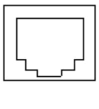
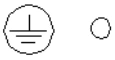
This diagram illustrates the back panel connections of the PRI Gateway. Note that E1/T1 port number 1 is located ***below*** E1/T1 port number 2.



If the power outlet does not supply adequate grounding, ***connect an external ground at ID #9****.*

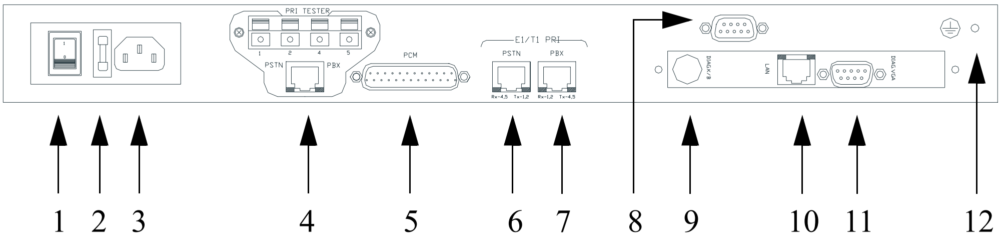
E1/T1 Gateways are supplied with ferrite cores for electromagnetic interference suppression (EMI). Place one on the PRI cable and one on the LAN cable, both as close as possible to the Gateway.

Table 28: Ports on a PRI Gateway

ID #	Graphic	Description
1		On/Off switch | = on 0 = off
2		Fuse chamber The fuse is housed behind a cover. Pop off the cover with a screwdriver.
3		The power cable is inserted into this socket.
4		RJ-11 plugs from the digital PBX, are inserted into these ports.
5		A modem for QoS, or testing equipment such as a loop-back device, can be connected to the Gateway using this Sub-D 9 pin connector.
6		A keyboard can be connected to the Gateway using this mini-DIN 6 pin connector.
7		A monitor can be connected to the Gateway using this Sub-D 15 pin high-density connector.
8		Connect the Gateway to the Internet (LAN or WAN) using this RJ-45 port.
9		If the power outlet does not supply adequate grounding, ***connect an external ground to the screw at the right of the ground symbol.***

Claro E1/T1 PRI Gateway Back Panel

This diagram illustrates the back panel connections of the Claro PRI Gateway. Note that PRI Tester is documented on page 10.



If the power outlet does not supply adequate grounding, ***connect an external ground at ID #12****.*

Claro E1/T1 Gateways are supplied with ferrite cores for electromagnetic interference suppression (EMI). Place one on the PRI cable and one on the LAN cable, both as close as possible to the Gateway.

Table 29: Ports on a Claro E1/T1 PRI Gateway

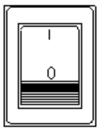
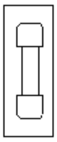
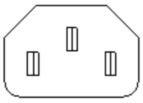
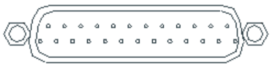
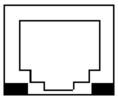
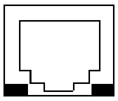
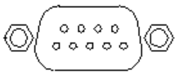
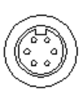
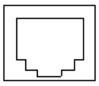
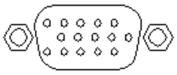
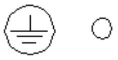
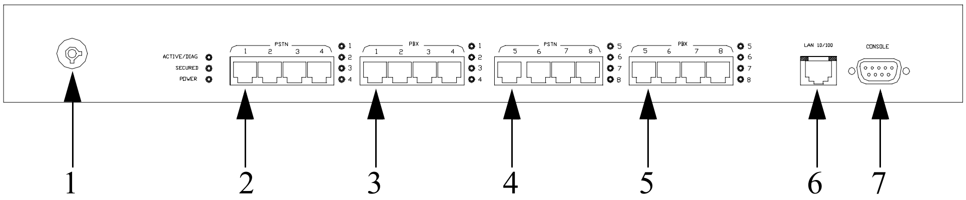
ID #	Graphic	Description
1		On/Off switch | = on 0 = off
2		Fuse chamber The fuse is housed behind a cover. Pop off the cover with a screwdriver.
3		The power cable is inserted into this socket.
4	PRI Tester	See “PRI Cable Tester — On Claro PRI Gateways Only” on page 10 for information about the PRI Tester

Table 29: Ports on a Claro E1/T1 PRI Gateway

ID #	Graphic	Description
5		This Sub-D 25 pin connector is reserved for future use.
6		Into this RJ-45 port, insert the cable which connect this location to the telephone company's Central Office.
7		Into this RJ-45 port, insert the cable from the digital PBX.
8		A modem for QoS, or testing equipment such as a loop-back device, can be connected to the Gateway using this Sub-D 9 pin connector.
9		A keyboard can be connected to the Gateway using this mini-DIN 6 pin connector.
10		Connect the Gateway to the Internet (LAN or WAN) using this RJ-45 port.
11		A monitor can be connected to the Gateway using this Sub-D 15 pin high-density connector.
12		If the power outlet does not supply adequate grounding, ***connect an external ground to the screw at the right of the ground symbol.***

Claro Analog Front Panel

This diagram illustrates the front panel connections of the Claro Analog Gateway.



If the power outlet does not supply adequate grounding, ***connect an external ground*** *to the screw on the rear panel.*

Table 30: Ports on a Claro Analog Gateway

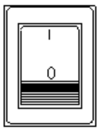
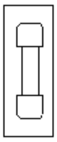
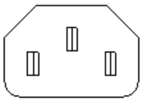
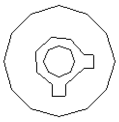
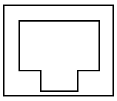
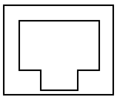
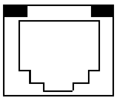
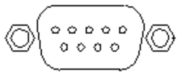
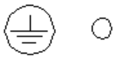
ID #	Graphic	Description
Rear panel		On/Off switch | = on 0 = off
Rear panel		Fuse chamber The fuse is housed behind a cover. Pop off the cover with a screwdriver.
Rear panel		The power cable is inserted into this socket.
1		Documentation on the Blue Seal Security Lock can be found in Section 14, beginning on page 271. Upon arrival, the lock is set at Low.
2 & 4		Into the RJ-11 ports marked PSTN, insert the cables which connect this location to the telephone company's Central Office.

Table 30: Ports on a Claro Analog Gateway

ID #	Graphic	Description
3 & 5		Into the RJ-11 ports marked PBX, insert the cables from the PBX or from single telephone units and/or fax machines.
6		Insert the connection to the Internet or the local network using this RJ-45 port.
7		A modem for QoS, or testing equipment such as a loop-back device, can be connected to the Gateway using this Sub-D 9 pin connector.
Rear panel		If the power outlet does not supply adequate grounding, ***connect an external ground to the screw at the right of the ground symbol.***

LED FUNCTION FOLLOWING POWER UP

After power up, if the Gateway is fully operational, the LEDs on the front panel will function as follows:

1. The Gateway and Diag. LEDs flash alternately until the Gateway has completed booting up.
2. The Diag. LED stops flashing.
3. The Gateway LED ***only*** continues flashing.

In addition, the LEDs indicate the following:

- If the Gateway LED stops flashing, regardless of whether it remains on or off, the Gateway has malfunctioned.
- If ***only*** the Diag. LED flashes, one or more of the Gateway services has malfunctioned.
- The Channel LEDs blink during call progress and remain solidly illuminated during conversation
- The Channel LEDs indicate which Gateway services are switching either on or off and can, thereby, indicate a malfunctioning application.
- The Power LED indicates whether or not there is power to the unit.

STARTUP PROCEDURE

After attaching the cables and power to the back panel, Startup involves:

a. Configuring the Gateway's IP address

b. Configuring the Officer Gateway's IP address, see p. 27

c. Applying the numbering plan

d. For PRI Gateways, confirming the PRI configuration

We recommend that you configure the Gateway's IP address using the Maintenance Wizard. However, you can also configure the IP address using either the Terminal Server or via Internet Explorer. These procedures are found on pages 22–26.

The Maintenance Wizard is available either from the CD or from Technical Support.

Configuring the IP address via the Maintenance Wizard

1. Connect the network adapters of the Gateway and the PC with a crossover cable or via a hub, such that the devices are connected to the same local network.
2. Run the Maintenance Wizard.
3. Select **Display all Gateways on the local IP network** and click **Next**. The **List Gateways** screen opens.
4. Click **Start**. The Wizard lists all Gateways and then displays instructions for selecting a Gateway.

A new Gateway's default IP address is 10.10.10.10.

5. Right-click the Gateway with the red X status indication.
6. From the pop-up menu, select **IP Settings**. The **IP Settings** dialog box opens.
7. Enter the IP address, Subnet mask, and Default Gateway and click OK. The Gateway reboots.
8. Wait 1–2 minutes for the Gateway to finish rebooting.
9. Click **Cancel** to close the Maintenance Wizard.

Configuring the IP address using the Terminal Server

Option 1:
Using a monitor and keyboard attached to the Gateway

1. Attach a monitor and keyboard to the Gateway.
2. Turn on the Gateway.
3. Wait 1–2 minutes for the system to boot.
4. When the bootup sequence finishes, press **Alt** + **F2**.
5. At the BOSâNOVA login prompt, *using lowercase letters only*, enter **voip** and press **Enter**.
6. Enter the password and press **Enter**. The default password is **1234**. The Terminal Server Main Menu is displayed.
7. Using the UP arrow and DOWN arrow keys on the keyboard, highlight **Change the network configuration**.
8. Using the Tab key on the keyboard, select **OK** and press **Enter**. The Network Configuration screen opens.
9. From the Network Configuration menu, highlight **Change basic network settings**.
10. Select **OK** and press **Enter**. The Change System Name screen appears.
11. Change or confirm the System Name. If using an H.323 gatekeeper, each Gateway should be assigned a unique System Name. The System Name can contain the letters A–Z, a–z, and 1–9. The first character must be a letter.
12. Select **OK** and press **Enter**. The IP Protocol screen appears.
13. Using the UP arrow and DOWN arrow keys on the keyboard, highlight either DHCP or Static IP.

⚠ *Assign a static IP address to the Officer Gateway. Otherwise, Private Gateways will lose contact with the Officer Gateway.*

14. To confirm your choice, use the space-bar on the keyboard to move the X beside either DHCP or Static IP.
15. Select **OK**, and press **Enter**.
16. Continue based upon the selection of either DHCP or Static:
    - DHCP requires confirmation. Select **OK** and click **Enter**.

- For a static IP address, change or confirm the IP address, the Subnet mask, the default Gateway, and the DNS Server:

If there isn't a DNS Server, leave the default setting of 127.0.0.1. This creates a loop back to the Gateway for errant packets.

  - To modify an entry, enter the changes, select OK, and press Enter.
  - To proceed without making changes, select OK, and press Enter.
  - To return to the Main Menu without saving any changes, press Cancel.

17. At the Save Settings screen, select:
    - **Yes** to save any changes that were made
    - **No** to return to the Main Menu without saving any changes

Option 2: Configuring the IP address: Using an RS-232 connection between COM ports

1. Turn on the Gateway and wait 1–2 minutes for the system to boot.
2. Attach a Windows-based PC to the Gateway via the COM port on the rear panel of the Gateway.
3. Click **Start** > **Programs** > **Accessories** > **Communications** > **HyperTerminal**. HyperTerminal opens.
4. Follow the HyperTerminal prompts:

   a. Assign a name to the connection and click **OK**.

   b. In the **Connect using** field of the Connect to dialog box, select the correct COM port and click **OK**.

   c. In the **Port Settings** dialog box, enter the following parameters:

      - **Bits per second**: 115200
      - **Data bits**: 8
      - **Parity**: None
      - **Stop bits**: 1
      - **Flow control**: Hardware

   Click **OK**.
5. Press **Enter**. This connects the PC to the Gateway.

6. At the BOSâNOVA login prompt, *using lowercase letters only*, enter **voip** and press **Enter**.
7. Enter the password and press **Enter**. The default password is **1234**. The Terminal Server Main Menu is displayed.
8. Using the UP arrow and DOWN arrow keys on the keyboard, highlight **Change the network configuration**.
9. Using the Tab key on the keyboard, select **OK** and press **Enter**. The Network Configuration screen opens.
10. From the Network Configuration menu, highlight **Change basic network settings**.
11. Select **OK** and press **Enter**. The Change System Name screen appears.
12. Change or confirm the System Name. If using an H.323 gatekeeper, each Gateway should be assigned a unique System Name. The System Name can contain the letters A–Z, a–z, and 1–9. The first character must be a letter.
13. Select **OK** and press **Enter**. The IP Protocol screen appears.
14. Using the UP arrow and DOWN arrow keys on the keyboard, highlight either DHCP or Static IP.

⚠ *Assign a static IP address to the Officer Gateway. Otherwise, Private Gateways will lose contact with the Officer Gateway.*

15. To confirm your choice, use the space-bar on the keyboard to move the X beside either DHCP or Static IP.
16. Select **OK**, and press **Enter**.
17. Continue based upon the selection of either DHCP or Static:
    - DHCP requires confirmation. Select **OK** and click **Enter**.
    - For a static IP address, change or confirm the IP address, the Subnet mask, the default Gateway, and the DNS Server:

If there isn't a DNS Server, leave the default setting of 127.0.0.1. This creates a loop back to the Gateway for errant packets.

- To modify an entry, enter the changes, select OK, and press Enter.
- To proceed without making changes, select OK, and press Enter.
- To return to the Main Menu without saving any changes, press Cancel.

18. At the Save Settings screen, select:
    - **Yes** to save any changes that were made
    - **No** to return to the Main Menu without saving any changes

Configuring the IP address using Internet Explorer

To configure the IP address using Internet Explorer:

1. Connect the Gateway to a PC. There are two ways to do this:

    a. Connect the Gateway and the PC to the same LAN.

    b. Connect a crossover cable to the network adapters of the PC and the Gateway.

2. Configure the PC such that the PC's IP address is 10.10.10.1 and its subnet mask is 255.0.0.0.

    a. Click the Windows **Start** button > **Settings** > **Network and Dial-up Connections**.

    b. Right-click **Local Area Connection** and select **Properties**.

    c. Select **Internet Protocol**.

    d. Click **Properties**.

    e. Complete the TCP/IP Properties dialog box and click **OK**.

3. Open a browser and type http://10.10.10.10. The Gateway Configurator opens.

10.10.10.10 is the Gateway's default IP address. Remember to record the new IP address after every change.

4. Enter the password and click **Login**. The default password is **1234**. The Configurator Main Menu opens.
5. Click **IP Settings**.
6. Configure the IP settings and click **OK**.
7. At the Reboot prompt, click **Reboot Now**.

The new settings are saved and the Gateway reboots.

Configure the Officer Gateway's IP Address

For general information regarding the BOSâNOVA IP Telephony network's Officer Gateway, see pages 85 and 204.

1. Open Microsoft Internet Explorer.
2. In the Address field, following the http://, type the IP address of the Gateway and click **Go**. The Gateway Configurator Welcome screen appears.
3. Enter the password and click **Login**. The Gateway Configurator main menu appears.
4. Click **Numbering Plan**. The first time the Numbering Plan item is selected, a message will prompt you to define the Gateway as either a Private or the Officer.
5. Click **OK**. The Change Function dialog box appears. **Private** will be listed as the Function type.
6. Enter the Officer's IP address and click **OK**. The Numbering Plan Wizard opens. Click **Cancel** if you are not authorized to configure the Numbering Plan. (Comments regarding Numbering Plan configuration appear in the following section.)

If, for any reason, the prompt is missed, complete steps 7–11:

7. From the Gateway Configurator main menu, select **Dialing Server**. The Dialing Server screen appears.
8. Click **Change**. The Change Function dialog box appears.
9. Ensure that the Function type is Private. If it is not, change it.
10. In the **Officer IP address** field, enter the IP address of the IP Telephony network's Officer Gateway.
11. Click **OK** and then click **Close**.

INSTALLING A MODEM

An external modem can be attached to the BOSâNOVA Gateway. External modems can be used for:

- Operating the Quality of Service (QoS) module
- Troubleshooting by Technical Support

Requirements

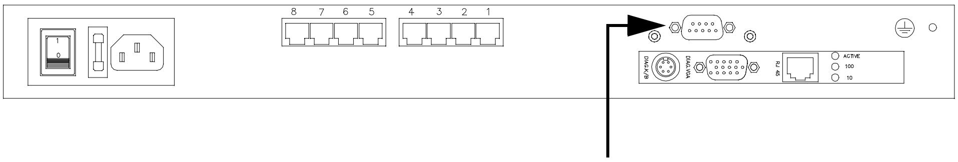
Installation of a modem requires the following:

- A customer supplied, Hayes AT command compliant, external modem with a Sub-D 25 pin serial port
- An RS232 external modem cable with a Sub-D 25 pin connector and a Sub-D 9 pin connector similar to the following:

- A standard phone cable to connect between the modem and the telephone jack in the wall

Installation

1. Turn off the Gateway.
2. Attach the 9 pin side of the RS232 cable to its corresponding socket on the Gateway.



Attach the 9 pin side of the cable here

3. Connect the 25 pin side of the RS232 cable to its corresponding socket on the modem.
4. Connect one end of the phone cable to the modem port labeled **Line**.

5. Connect the second end of the phone cable to the phone jack in the wall.

Typically, a modem has two ports for RJ11 connections. One is labeled Phone and the second is labeled Line. Be sure to attach the phone cable to the port labeled Line.

6. Connect the modem’s power cable to a wall outlet.
7. Restart the Gateway.
8. Allow at least 2 minutes for the Gateway to reboot. The Gateway will automatically detect and configure the modem.
9. To confirm that the modem was installed successfully:
   - If a monitor is connected, the line **Modem was detected on tty...** will appear.
   - If a monitor is not available, the modem’s LEDs will flash randomly for several seconds.
10. If the modem is not recognized, see “Configuring a Modem” on page 325.

INSTALLATION TROUBLESHOOTING

This section addresses installation problems discovered prior to the date of publication. If you encounter a new problem, please describe the problem in an e-mail addressed to support@boscom.com; in the subject line, type “Attention: Technical Writing Department.”

PROBLEM:
After replacing a TeleLynk Gateway with a new BOSâNOVA VoIP Gateway, the Configurator does not appear in the browser.

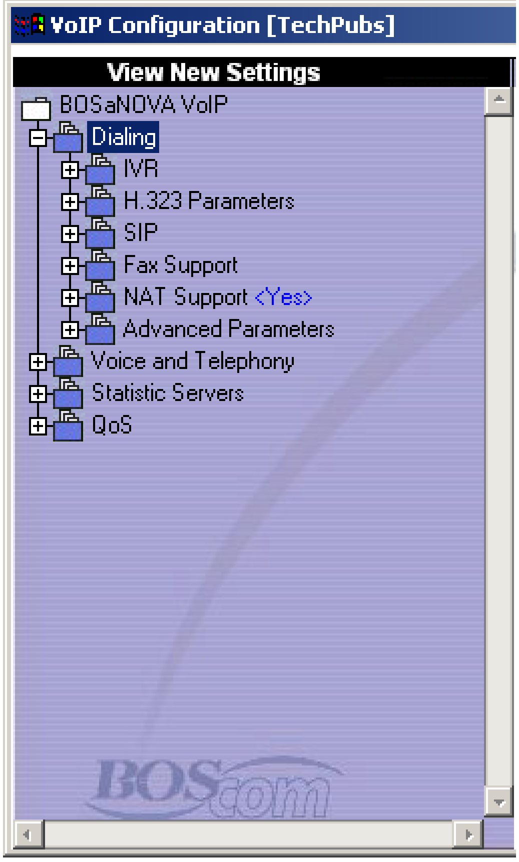
SOLUTION:
This may be caused by temporary internet files stored in the browser’s cache. The solution is to clear the cache. How this is done depends upon the browser. For example, in Internet Explorer 5.0:

1. In your browser, click **Tools > Internet Options**.
2. Select the **General** tab.
3. In the Temporary Internet files box, click **Delete files**. A confirmation box appears.
4. Click **OK** to confirm the decision.
5. Click **OK** to exit the Internet Options dialog box.
6. Reenter the address of the Configurator and click **Go**. The BOSâNOVA VoIP Configurator should appear.

SECTION 3:
CONFIGURING DIALING PARAMETERS

This section contains explanations and procedures relating to the Dialing parameters branch of the BOSâNOVA IP Telephony Gateway Configurator, including:

- Interactive Voice Responses (IVR), see p. 32
- H.323 Parameters, see p. 37
- SIP Parameters, see p. 38
- Fax Parameters, see p. 39
- NAT Support, see p. 40
- Advanced Parameters, see p. 41



INTERACTIVE VOICE RESPONSES (IVR)

BOSâNOVA Gateways include a library of voice announcements. The library is stored in the directory named \var\BOSaNOVA\cfg\VoiceMsg and is divided into scenarios.

Each scenario contains several prerecorded voice announcements. Each voice announcement is saved with a file name *SnnMccc.bnc*. where *nn* indicates the scenario number while *ccc* indicates the number of the recording.

In the Maintenance Wizard, these are called ***Embedded IVR Scenarios****. Embedded IVR Scenarios are not the same as the RADIUS AAA IVR.*

Table 31: Welcome Scenario

Message name	File name
Welcome message	S01M001.bnc

Table 32: Disconnect Reason Scenario

Message name	File name
DTMF Timeout	S02M001.bnc
Number not included	S02M002.bnc
Mechanical malfunction	S02M003.bnc
Configuration mistake	S02M004.bnc
Lines busy	S02M005.bnc
Remote disconnect	S02M006.bnc
Administrator disconnect	S02M007.bnc
Exceeded time limit	S02M008.bnc
Local disconnect	S02M009.bnc

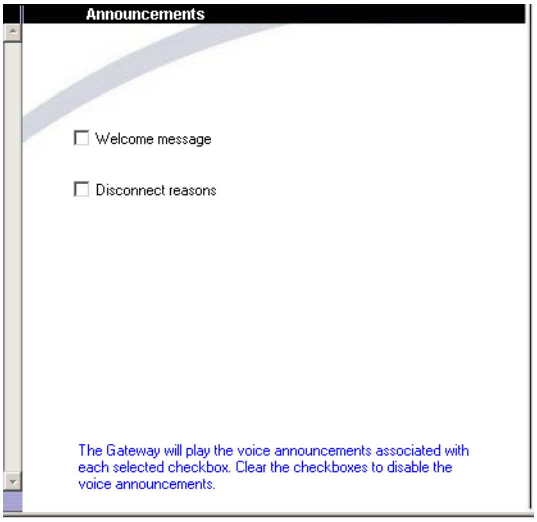
Table 33: Authorization Scenario *

Message name	File name
Destination cannot accept	S03M001.bnc
Code required	S03M002.bnc
Invalid code	S03M003.bnc
Mismatched code	S03M004.bnc
Unauthorized call	S03M005.bnc
* This scenario is active whenever either Numbering Plan Authentication or Hop-off Pin Authentication is enabled.	

Enabling and Disabling Embedded IVR Scenarios

To enable or disable a voice announcement scenario:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Dialing** branch.
3. Expand the **IVR** (Interactive Voice Response) branch.
4. Select **Embedded IVR Scenarios**. The following appears in the Configuration pane:



The Gateway will play the voice announcements associated with each selected checkbox. Clear the checkboxes to disable the voice announcements.

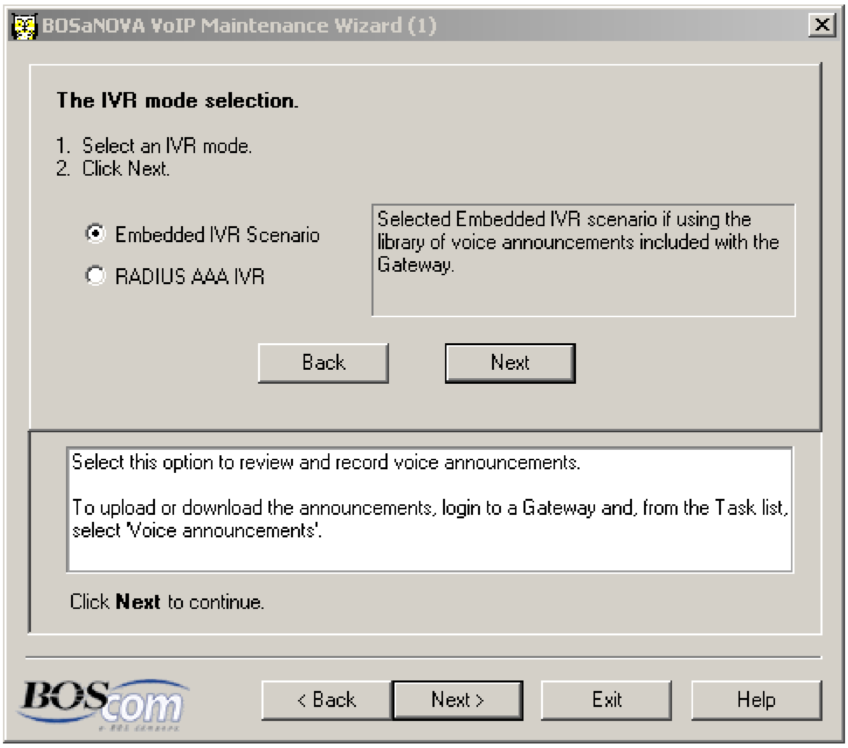
5. Select or clear the checkboxes for each scenario.
6. Click **Apply**.

Recording and Installing Embedded IVR Announcements

General documentation concerning the Maintenance Wizard begins with the chapter "Maintenance Wizard's Primary Applications" on page 293.

To record or install an Embedded IVR Scenario voice announcement, use the Maintenance Wizard.

1. From the Welcome Screen of the BOSâNOVA IP Telephony CD-ROM, select Run Maintenance Wizard. The Maintenance Wizard Welcome screen appears.
2. Ensure that you know the file name of the specfic recording. You can either download the file from the Gateway and record over it (see *Downloading and Uploading Libraries* on page 36) or you can create a file with the correct file name (see Table 31 – Table 33). When uploaded, it will over-write the Gateway's existing file.
3. Select **Configure voice announcements** and click **Next**. The IVR Mode selection screen appears.



The IVR mode selection.

1. Select an IVR mode.
2. Click Next.

● Embedded IVR Scenario

○ RADIUS AAA IVR

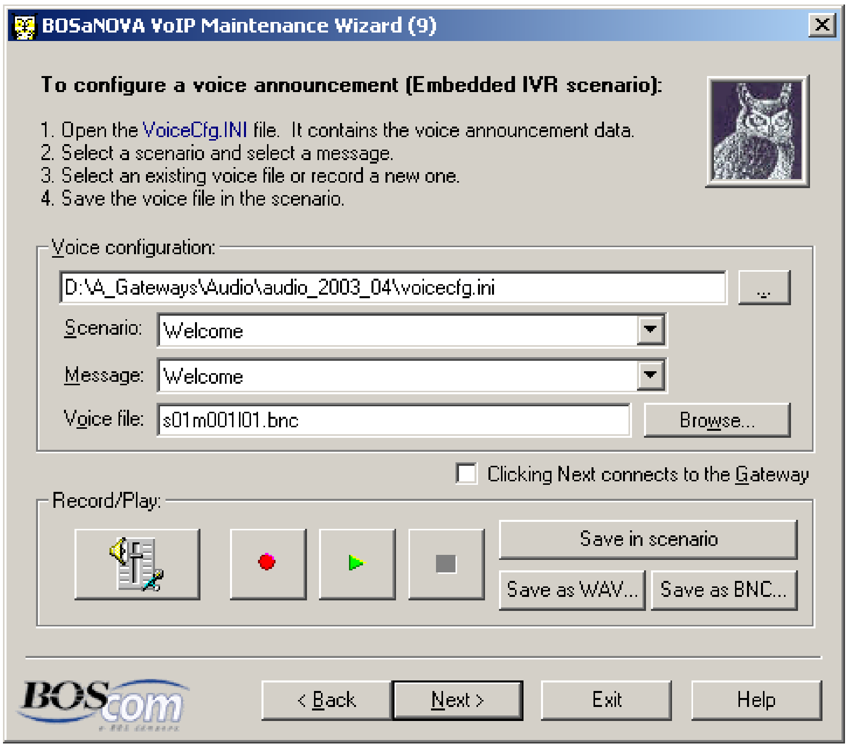
Selected Embedded IVR scenario if using the library of voice announcements included with the Gateway.

Select this option to review and record voice announcements.

To upload or download the announcements, login to a Gateway and, from the Task list, select 'Voice announcements'.

Click **Next** to continue.

4. Select **Embedded IVR Scenario** and click the enabled **Next**. The Voice Configuration screen appears.



BOSaNOVA VoIP Maintenance Wizard (9)

To configure a voice announcement (Embedded IVR scenario):

1. Open the VoiceCfg.INI file. It contains the voice announcement data.
2. Select a scenario and select a message.
3. Select an existing voice file or record a new one.
4. Save the voice file in the scenario.

Voice configuration: D:\A_Gateways\Audio\audio_2003_04\voicecfg.ini

Scenario: Welcome

Message: Welcome

Voice file: s01m001l01.bnc

☐ Clicking Next connects to the Gateway

5. Open the VoiceCfg.INI file. It contains the voice announcement data.

6. Select a scenario.

7. Select a message. The corresponding file name appears in the Voice file field.

8. Click ● (the record button) and record the new message.

9. Click ■ (the stop button) to discontinue recording.

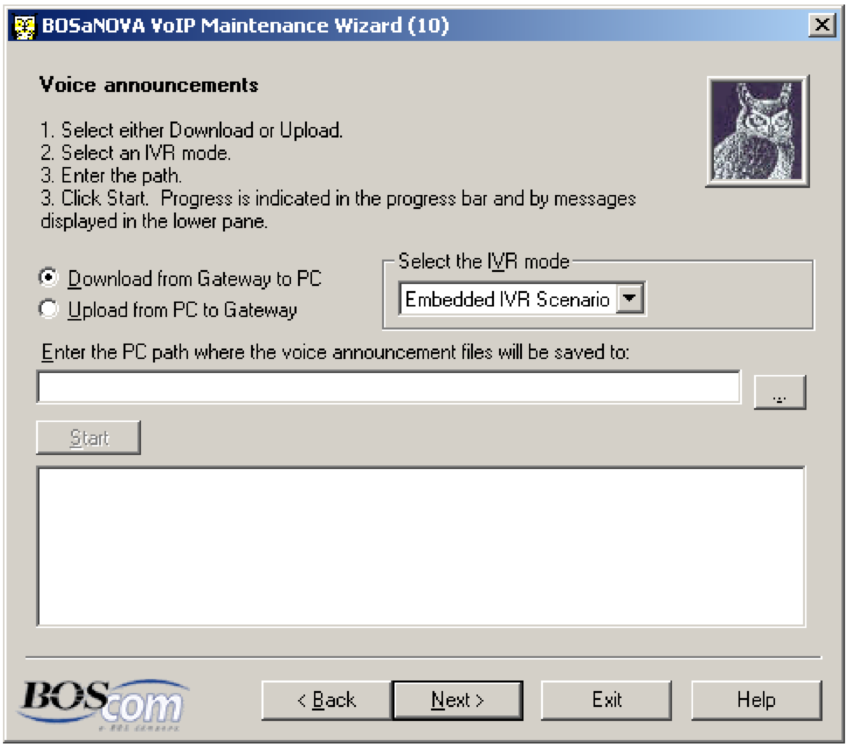
To edit the recording in a WAV editor, click Save as WAV. After editing, the file must be saved as a BNC.

10. Click **Save in scenario**.

Downloading and Uploading Libraries

To download or upload a library, use the Maintenance Wizard.

1. From the Welcome Screen of the BOSâNOVA IP Telephony CD-ROM, select Run Maintenance Wizard. The Maintenance Wizard Welcome screen appears.
2. Connect to the Gateway.
   - If you need help and know the Gateway's IP address, see "Connecting to a Gateway With a Known Address" on page 299.
   - If you need help and do not know the Gateway's IP address, see "Finding Gateways and Reviewing Their Status" on page 296.
3. Select the task **Voice announcements**.
4. Click **Next**. The Voice announcements screen appears.



BOSaNOVA VoIP Maintenance Wizard (10)

Voice announcements

1. Select either Download or Upload.
2. Select an IVR mode.
3. Enter the path.
3. Click Start. Progress is indicated in the progress bar and by messages displayed in the lower pane.

● Download from Gateway to PC
○ Upload from PC to Gateway

Select the IVR mode: Embedded IVR Scenario

Enter the PC path where the voice announcement files will be saved to:

5. Select either Download or Upload.
6. Select an IVR mode.
7. Enter the path to the library.
8. Click **Start**.

H.323 PARAMETERS

To access the H.323 parameters:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Dialing** branch.
3. Expand the **H.323 Parameters** branch.
4. Select from the following parameters:

   H.323 Fast Start
   When H.323 Fast Start is enabled, media stream delivery begins as soon as the connection is made. This simulates a normal telephone call. H.323 Fast Start minimizes the number of round trip message exchanges, enabling immediate media stream delivery upon call connection

   H.245 Tunneling
   H.245 Tunneling allows encapsulation of H.245 messages within any H.225-Q.931 message. Thus, tunneling reduces call-setup time and ensures a more efficient use of network resources. H.245 Tunneling can be used only when both endpoints have this capability.

   Q.931 Multiplexing
   Q.931 Multiplexing carries simultaneous calls through a single channel. Normally, this ensures more efficient use of network resources. Do not use multiplexing unless both endpoints have this capability.

   Open Media
   Before users begin speaking, signals are sent between Gateways. Some of these signals are audible and familiar, such as ring-back, that is, the call heard by the party that dialed when the destination phone is ringing. However, when a VoIP network includes equipment that is not BOSâNOVA equipment, there may be instances of non-interoperability. Non-interpretability may result in some signals not being audible. In other instances, the non-BOSâNOVA equipment might produce audible signals different than those produced by the BOSâNOVA equipment and the former might be preferred. In either instance, change the Open Media settings.

   If the call originates from the BOSâNOVA equipment, change the settings in the Originating Gateway box. If the destination Gateway is the BOSâNOVA equipment, change the settings in the Destination Gateway box.

SIP (SESSION INITIATION PROTOCOL)

To access the SIP parameters:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Dialing** branch.
3. Expand the **SIP** branch.
4. Select from the following parameters:

   Enable 100rel
   When selected, the 100rel tag is appended to the value of the header. This is useful for opening one-way media sessions before call establishment.

   Enable Early Media
   When selected, the SIP network is able to deliver real-time media traffic from the called party to the calling party after the calling party issues an INVITE but before the called party accepts the INVITE.

FAX SUPPORT

To access the Fax Support parameters:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Dialing** branch.
3. Expand the **Fax Support** branch.
4. Select the **T.38** sub-branch and configure the following parameters:

   T.38 Support
   T.38 is the ITU standard governing real-time fax relay over IP networks. The use of a T.38-compliant relay enables a Gateway to withstand several seconds of packet delay, lost packets, and packets in error without creating errors in the received image. When the checkbox is cleared, fax transmissions are sent as if they were VoIP.

   T.38 Redundancy Level
   Redundancy can compensate for a poor Internet connection. Enter a redundancy level between 0 and 3.

Setting the redundancy level to a value greater than 0 causes a significant increase in the network bandwidth consumed by the fax transmission.

   Dummy UDPTL messages
   Select if the T.38-compliant relay requires a constant stream of packets.

5. Select the Pass-Through sub-branch.
6. Select the codec that will be used by the Gateway for fax transmission.
7. Click **Apply**.

NAT SUPPORT

Network Address Translation (NAT) refers to a process whereby an application exchanges a computer's Local Area Network (LAN) IP address for the LAN's global IP address. NAT creates problems for IP Telephony networks. For a complete discussion of BOSâNOVA Gateway NAT support, see the chapter entitled "Network Address Translation" on page 226.

To access the NAT Support parameters:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Dialing** branch.
3. Select the **NAT Support** branch. The NAT Support checkbox appears in the Configuration pane. Select the checkbox if calls to and from this Gateway will traverse a Network Address Translation Server.
4. Expand the **NAT Support** branch.
5. Select from the following parameters:

   Mode

   - **BOS**
     When selected, the Gateway obtains its external IP address automatically. This address is included in H.323 messages where the local IP address is defined.
   - **Static NAT IP**
     When selected, enter the external IP address behind which this Gateway resides. This address will be included in H.323 messages where the local IP address is defined. This option may resolve interoperability issues.

   Send Keep Alive signal
   When Keep alive is selected, the Gateway sends a "dummy" SIP message to the SIP proxy server at intervals defined in the Keep Alive Timeout field. This prevents disconnect.

   Support via Rport
   When selected, a parameter called "rport" is defined in the Via header field. This parameter is useful for basic NAT traversal. The rport parameter allows a client to request that the server send the response back to the source IP address and port where the request came from. The rport parameter is analogous to the "received" parameter, except "rport" contains a port number, not the IP address.

ADVANCED PARAMETERS

To access the Advanced parameters:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Dialing** branch.
3. Expand the **Advanced** branch.
4. Select from the following parameters:

Inter-Digit Timeout

The Gateway continuously checks the speed the user dials. Dialing a phone number is considered completed when the user dials the # sign, or when a digit is not dialed within a time period equal to MAX (Ta, 2seconds), where Ta is the average time interval between digits.

The initial period of time that the Gateway waits for the first digit is defined by the Inter-digit Timeout parameter. The default value is 5 seconds.

Encryption

⚠ *When Encryption is enabled, the Gateways will not work with any standard SIP or H.323 Gateway.*

When selected, voice data and signalling data are encrypted using the Advanced Encryption Standard (AES) of the Federal Information Processing Standard (FIPS). The traffic cannot be identified as VoIP traffic, neither by call progress signaling nor by media Realtime Transport Protocol (RTP). Non-standard (configurable) ports and non-standard VoIP headers are used, and data in each packet is encrypted.

AES is a NIST-standard secret key cryptography method that uses 128-, 192- and 256-bit keys. In 2001, AES officially replaced the Triple DES method. Gateways use 128-bit keys and 128-bit blocks.

Encryption must be enabled for every Gateway in the IP Telephony network and each must be assigned ***the same*** Call Progress port and the same Voice RTP port.

Maximum IP Calls

Enter the number of simultaneous IP calls that this Gateway is allowed to support.

In some circumstances—for example, in cases of limited bandwidth—the Claro Gateway can support more IP phone calls than can the internet connection. As a result, the quality of service declines.

By limiting the number of IP phone calls, the Administrator assures better quality of service.

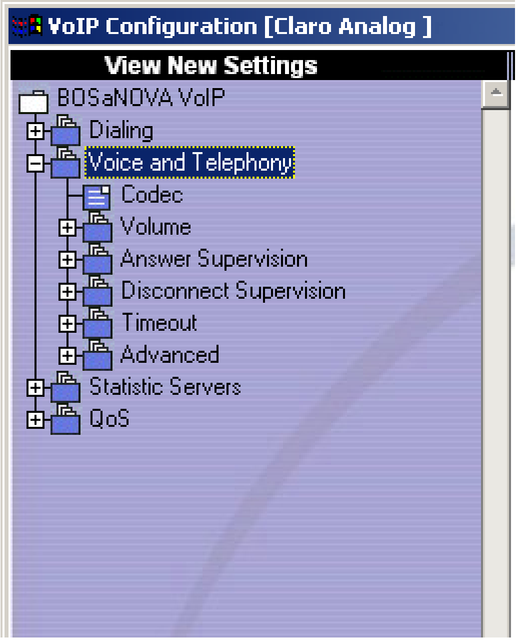
The limitation counts both incoming and outgoing IP calls. Thus, if a Gateway attempts to connect a call through a Gateway that has already reached its limit of simultaneous calls, the call will be rerouted via the PSTN.

IP Telephony...
Clear and Simple

SECTION 4:
CONFIGURING VOICE AND TELEPHONY PARAMETERS

This section contains explanations and procedures relating to the Voice and Telephony branch of the BOSâNOVA IP Telephony Gateway Configurator, including:

- Understanding codec parameters, see p. 45
- Setting codec parameters, see p. 46
- Volume settings, see p. 49
- Answer Supervision, see p. 50
- Disconnect Supervision, see p. 52
- Timeout settings, see p. 57
- Advanced settings, see p. 58
- Statistic Servers, see p. 64
- Quality of Service (QoS), see p. 65



CODEC

This section includes:

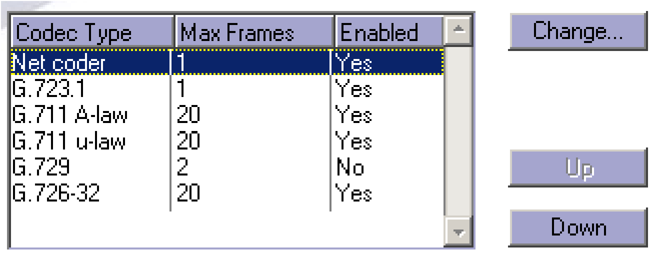
- Explanations of Codec parameters, see p. 45
- Procedures related to configuring of Codec parameters, see p. 46 – p. 47

Displaying the Codec Parameter Table

The settings for the Codec parameters are displayed in a three-column table.

To display the Codec parameter table:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Codec** sub-branch.
4. Select **Codec**. The Codec table is displayed.



Codec Type	Max Frames	Enabled
Net coder	1	Yes
G.723.1	1	Yes
G.711 A-law	20	Yes
G.711 u-law	20	Yes
G.729	2	No
G.726-32	20	Yes

Explanations of the Columns

Codec Type

Codec types are the voice compression/decompression (CoDec) methods supported by the Gateway. The Codec type is negotiated with the remote Gateway per call.

Max (maximum) Frames

The explanation of Max Frames is dependent upon the codec type.

- NetCoder
  Max Frames defines how many encoded 20-millisecond voice segments are sent in one RTP message. The default is 1.
- G.711.A-law / u-law
  Max Frames defines in milliseconds the length of the voice segment that is used to build one RTP message. The default is 20.
- G.723.1
  Max Frames defines how many encoded 30-millisecond voice segments are sent in one RTP message. The default is 1.
- G.726
  Max Frames defines how many encoded 1 millisecond voice segments are sent in one RTP message. The default is 20.
- G.729
  Max Frames defines how many encoded 10-millisecond voice segments are sent in one RTP message. The default is 2.

The license agreement regulates changes you can make to codec types G.723.1 and G.729.

Enabled

During the H.245 capability exchange procedure, Gateways *negotiate* to determine which codec will be used. The "master" Gateway selects the codec which is supported by both Gateways and which is highest in its table.

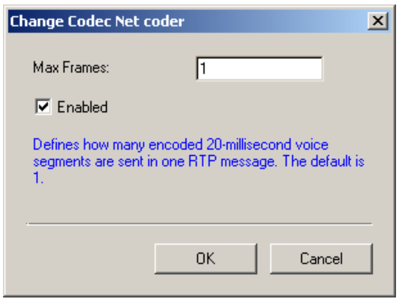
Enabled indicates that the codec specified is included in the capability table that is used during the H.245 capability exchange procedure.

Changing the Settings of a Codec

Use caution when changing codec parameters. The default settings are optimal for general purposes.

To change codec parameters:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Codec** sub-branch.
4. Select **Codec**.
5. Select a codec type from the table.
6. Click **Change**. The Change Codec dialog box opens.



Change Codec Net coder

Max Frames: 1

☑ Enabled

Defines how many encoded 20-millisecond voice segments are sent in one RTP message. The default is 1.

7. Enter the new Max Frames quantity.
8. Select or clear **Enabled**.

   When selected, the Gateway includes the codec type in the capability table that is used during the H.245 capability exchange procedure. If the Enabled checkbox is selected, Yes appears in the Enabled column of the parameters table. If the Enabled checkbox is cleared, No appears in the Enabled column of the parameters table.
9. Click **OK**. The new settings appear in the table.
10. The two advanced parameters are relevant when the NetCoder codec is enabled. If applicable, select **Advanced**.

    - **Support Variable Bit-rate**
      When NetCoder variable bit-rate is enabled, in response to changing Internet conditions, the end-points may change both bit-rate and number of frames per packet. This helps ensure excellent voice quality.

- **Support Reduced Bandwidth — Multi-packet**
  The NetCoder Multi-packet feature allows reduction of the required bandwidth when several calls are connected between the same Gateways.

11. Click **Apply**. The Reboot confirmation screen appears.
12. Select either **Reboot now** or **Reboot later**.

Changing the Prioritization of a Codec

During the H.245 capability exchange procedure, Gateways “negotiate” to determine which codec will be used. The “master” Gateway selects the codec which is supported by both Gateways and which is highest in its table. The location of the codec in the Codec Type table is called its prioritization.

The following table illustrates the relationship between bandwidth consumed by a codec and voice quality:

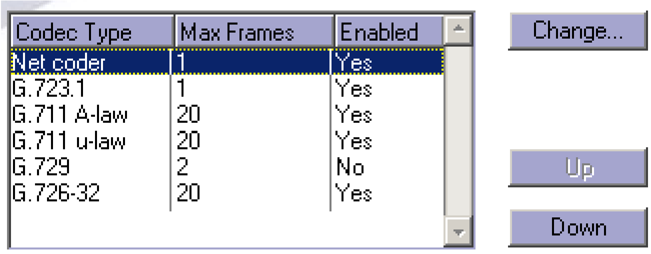
Table 34: Codec Bandwidth and Voice Quality

Codec Type	Bandwidth (kbit/sec)	Quality	Latency (msec)
G.711	64	Excellent (4.3)	20
G.723.1 *	6.3 5.3	Good (3.8) Fair (3.5)	30
G.726	32	Excellent (4.3)	20
G.729	8	Good (4.2)	10
NetCoder **	6.4	Good (4.2)	20

* The Gateways support both G.723.1 bit-rates. Specifically, the Gateway always chooses 6.3 kbps, but on receiving voice that is compressed with 5.3 kbps it automatically decreases its own bit-rate for both sending and receiving.
** The NetCoder codec allows for a variable bit rate, ranging from 6.4 to 9.6 kbit per second (6.4, 7.2, 8.0, 8.8 and 9.6 kbps). The Multi-packet feature, implemented for NetCoder 9.6 kbps, dramatically increases voice quality.

To increase or decrease the priority of the codec's type:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Codec** sub-branch.
4. Select **Codec**.
5. Select the codec type.
6. Note the **Up** and **Down** buttons beside the Codec Table.



Codec Type	Max Frames	Enabled
Net coder	1	Yes
G.723.1	1	Yes
G.711 A-law	20	Yes
G.711 u-law	20	Yes
G.729	2	No
G.726-32	20	Yes

Either:

- Click **Up** to move the codec type up one line in the table, or
- Click **Down** to move the codec type down one line in the table

The changed order is displayed immediately.

7. Click **Apply**. The Reboot confirmation screen appears.
8. Select either **Reboot now** or **Reboot later**.

VOLUME

The items in this branch control aspects of volume as perceived by the users.

To change a volume setting:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Volume** branch.
4. Set the volume for the following:
   - **Local Party's**
     This setting is measured in decibels (dB) and modifies the volume of the voice heard through the local party's telephone handset. 0 dB is a normal level. The possible range is -31 to 31. Raising the volume by 10 dB approximately doubles the volume in the handset.
   - **Remote Party's**
     This setting is measured in decibels (dB) and modifies the volume of the voice heard through the remote party's telephone handset. 0 dB is a normal level. The possible range is -31 to 31. Raising the volume by 10 dB approximately doubles the volume in the handset.
   - **Generated Tones**
     This setting is measured in decibels (dB) and defines the volume of the tones generated by the vocoder, for example, the volume of the busy signal and the volume of dual tone multi-frequency tones (DTMF). To increase the volume of the generated tones, decrease the setting (i.e., the reduction). The value can be set from 0 to 31 dB. The default is 0. Raising the volume by 10 dB approximately doubles the volume in the handset.

     If a device connected to the Gateway does not detect the Gateway generated DTMF tones, decrease this setting. However, when using certain PSTN devices, increasing the volume too much can negatively affect the DTMF tone signal quality.
5. Click **Apply**. The Reboot confirmation screen appears.
6. Select either **Reboot now** or **Reboot later**.

ANSWER SUPERVISION

In certain circumstances, it may be necessary to configure how an FXO or Claro Analog Gateway determine that a call has been answered. These parameters are called Answer Supervision.

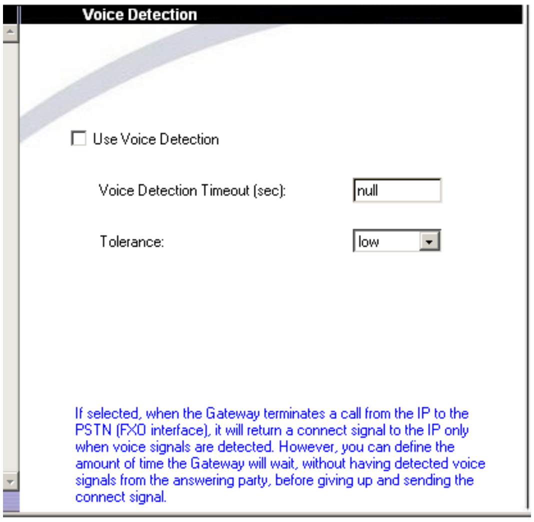
Voice Detection

The section is relevant to FXO and Claro Analog Gateways only.

If Voice Detection is enabled, when the Gateway terminates a call from the IP to the PSTN (FXO interface), it will return a connect signal to the IP only when voice signals are detected.

To configure Voice Detection:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Answer Supervision** branch.
4. Select **Voice Detection**. These fields appear in the Configuration pane:



Voice Detection

□ Use Voice Detection

Voice Detection Timeout (sec): null

Tolerance: low

If selected, when the Gateway terminates a call from the IP to the PSTN (FXO interface), it will return a connect signal to the IP only when voice signals are detected. However, you can define the amount of time the Gateway will wait, without having detected voice signals from the answering party, before giving up and sending the connect signal.

5. Select **Use Voice Detection**.
6. **Voice Detection Timeout** defines the amount of time the Gateway will wait, without having detected voice signals from the answering party, before giving up and sending the connect signal. Choose one of two options:
   - Select **null** to configure the Gateway to send the connect signal only when detecting voice signals.

- Enter a time period measured in seconds.

7. **Tolerance** defines how carefully the Gateway inspects the sounds. Since some telephony sounds can be mistaken as voice signals, for Voice Detection to operate properly, it may be necessary to increase the tolerance setting.
8. Click **Apply**.

Battery Reversal

*The section is relevant to Claro Analog Gateways only. When enabled, battery reversal affects **both answer and disconnect** supervision.*

The direction of current flow, also know as polarity, can be monitored to determine when a caller has answered or when a caller has disconnected. Monitoring for changes in polarity at the beginning and end of a call is commonly referred to as answer supervision and disconnect supervision.

When an outbound call is made on an analog loopstart trunk, the call starts when the current flows through the circuit. Once the called party has answered, the switch connected to the analog loopstart trunk can reverse the direction of current, i.e., change polarity, as an indication that the far end has answered. This is also called battery polarity reversal.

Polarity remains reversed for the duration of the call. When the called party hangs up the phone, the analog loopstart trunk can be notified of the disconnect by either reverting to the original current polarity, or by a momentary break in battery feed, commonly referred to as power denial (see p. 56).

When selected, the Gateway connects the call if it receives a battery reversal signal from the PSTN and disconnects the call when it receives a battery normal signal. Also, when the Gateway receives a connect from the IP, it sends a battery reversal signal to the PBX.

To configure Voice Detection:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Answer Supervision** branch.
4. Select **Battery Reversal**.
5. Select the Battery Reversal checkbox.
6. Click **Apply**.

DISCONNECT SUPERVISION

For various reasons, after a user hangs up, FXO Gateways may fail to disconnect. To correct this, a Gateway, when certain conditions occur, can be "forced" to disconnect. Disconnect Supervision parameters are configured on this branch of the Configurator.

PBX Tones

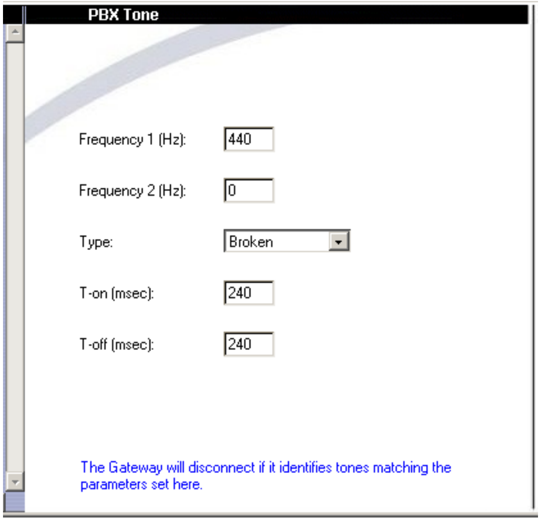
The table below lists the parameters of common signals emitted by PBXs and recognized by the Gateway. If the PBX uses any of these, no configuration should be necessary.

Table 35: Common PBX Signals

Signal Name	Type	Freq. 1	Freq. 2	T-on *	T-off *
ANSI T1.401–1993 Line Busy Tone	Busy	480	620	0.5	0.5
ITU-T Q.35 Line Busy Tone	Busy	425	-	0.5	0.5
Busy Tone (France)	Busy	440	-	0.5	0.5
Busy Tone (Japan, Israel)	Busy	400	-	0.5	0.5
ANSI T1.401–1993 re-order or congestion	Congestion	480	620	0.25	0.25
ANSI T1.401–1993 Fast Busy Tone	Congestion	440	-	0.24	0.24
ITU-T Q.35 congestion	Congestion	425	-	0.25	0.25
Panasonic Fast Busy	Congestion	400	-	0.25	0.25
ANSI T1.401–1993 Dial Tone	Dial	350	440	3	-
ITU-T Q.35 Dial Tone (Europe, except France, Belgium)	Dial	425	-	3	-
Dial Tone (France)	Dial	440	-	3	-
Dial Tone (Japan, Israel)	Dial	400	-	3	-
ANSI T1.401–1993 Ringing	Ringback	440	480	1	3
ITU-T Q.35 Ringing	Ringback	425	-	1	3

To configure PBX's signals that do not match any of those appearing in the table:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Disconnect Supervision** branch.
4. Select **PBX Tones**. These fields appear in the Configuration pane:



PBX Tone

Frequency 1 (Hz): 440

Frequency 2 (Hz): 0

Type: Broken

T-on (msec): 240

T-off (msec): 240

The Gateway will disconnect if it identifies tones matching the parameters set here.

5. Enter the following parameters as appropriate:
   - Frequency 1
     This parameter can be set from 300 to 1400 Hz. The default setting is 345. If there is no signal, set this to zero.
   - Frequency 2
     This parameter can be set from 300 to 1400 Hz and should be set higher than Frequency 1. The default setting is 445. If the signal contains only one tone, set Frequency 2 to zero.
   - T-on
     This parameter can be set from 0.1 to 15 sec. The default is 0.25 seconds.
   - T-off
     This parameter can be set from 0.1 to 15 sec. The default is 0.25 seconds. If the signal is a continuous tone (that is, a dial tone), set this parameter to 0.

A signal without a T-off parameter is a continuous signal, that is, a dial tone.

6. Select either **Continuous** or **Broken**.

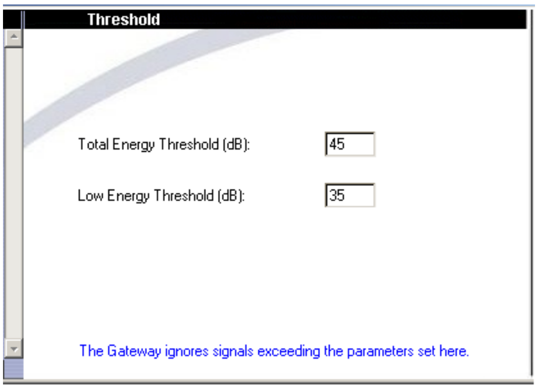
Threshold

The Threshold settings are used to fine-tune noise filtration and the execution of disconnect prompted by PBX Tones. Change these settings only when instructed to do so by Technical Support.

The Total Energy Threshold setting must be greater than the Low Energy Threshold setting.

To change Threshold settings:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Disconnect Supervision** branch.
4. Select **Threshold**. The following fields appear in the Configuration pane:



Total Energy Threshold (dB): 45

Low Energy Threshold (dB): 35

The Gateway ignores signals exceeding the parameters set here.

5. Enter the following parameters as appropriate:
   - Total Energy Threshold
     The Total Energy Threshold setting defines the decibel level of signals that the vocoder recognizes as voice. Signals below this level are assumed to be noise and are filtered out.

     This parameter can be set from 0 to -50 decibels (dB). The default is -45 dB.
   - Low Energy Threshold
     The Low Energy Threshold setting defines the decibel level of signals that the vocoder recognizes as PBX disconnect tones. Signals below this level are ignored.

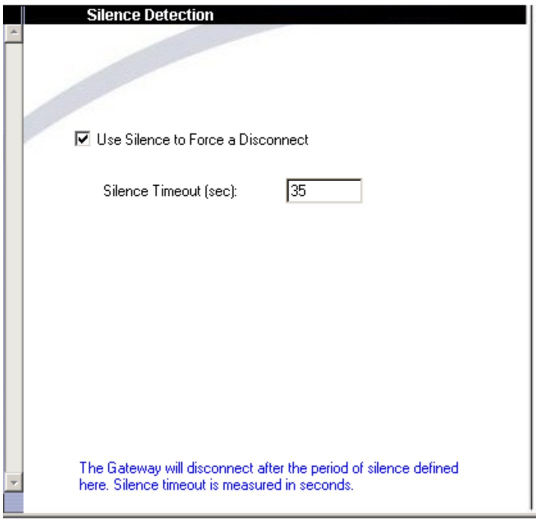
     This parameter can be set from 0 to -50 decibels (dB). The default is -35 dB.
6. Click **Apply**.

Silence Detection

The Gateway can be configured to disconnect after detecting a period of silence.

To set the Silence Detection parameter:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Disconnect Supervision** branch.
4. Select **Silence Detection**. The following fields appear in the Configuration pane:



Silence Detection

☑ Use Silence to Force a Disconnect

Silence Timeout (sec): 35

The Gateway will disconnect after the period of silence defined here. Silence timeout is measured in seconds.

5. Select the **Use Silence to Force a Disconnect** checkbox.
6. Enter the length of the period of silence that will force a disconnect. The minimum setting is 0. The maximum setting is 999. The default setting is 30, that is, half-a-minute.
7. Click **Apply**. The Reboot confirmation screen appears.
8. Select either **Reboot now** or **Reboot later**.

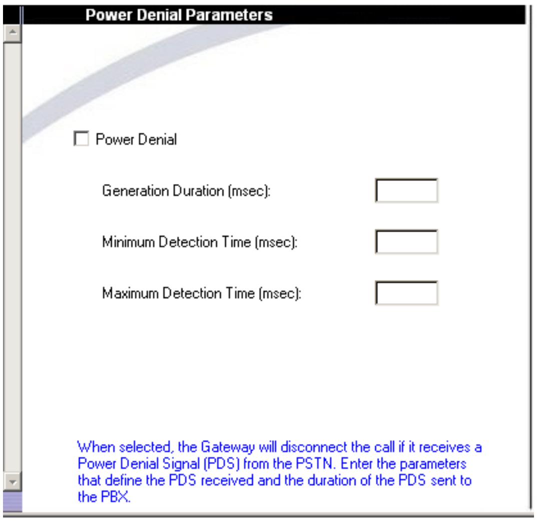
Power Denial — For Claro Analog Gateways

To indicate that a call has been disconnected, a PSTN Central Office sends either a battery reversal signal (see p. 51) or a power denial signal to the PBX. However, Claro Analog Gateways are installed between the PSTN and the PBX. Therefore, the Claro Analog Gateway must replicate the signal it receives from the PSTN and send it to the PBX.

Contact either the PBX technician or the PSTN Central Office to determine the type of signal used.

To configure power denial for a Claro Analog Gateway:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Disconnect Supervision** branch.
4. Select **Power Denial**. The following fields appear in the Configuration pane:



Power Denial Parameters
☐ Power Denial
Generation Duration (msec):
Minimum Detection Time (msec):
Maximum Detection Time (msec):

When selected, the Gateway will disconnect the call if it receives a Power Denial Signal (PDS) from the PSTN. Enter the parameters that define the PDS received and the duration of the PDS sent to the PBX.

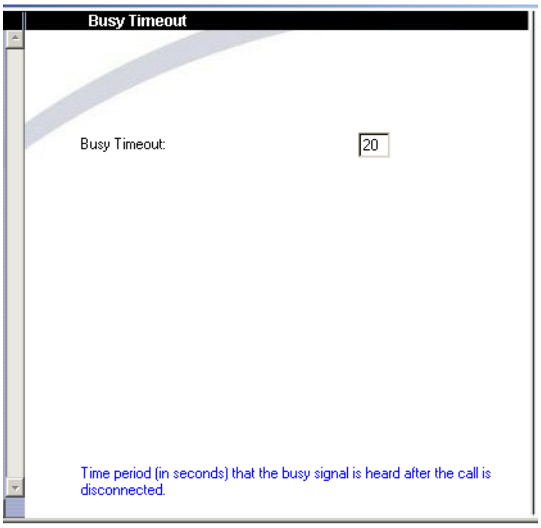
5. Select the Power Denial checkbox.
   - **Generation Duration**
     Enter the length of the power denial signal sent by the Gateway to the PBX.
   - **Minimum/Maximum Detection Time**
     The Gateway must first detect the power denial signal. The Gateway will not send a signal to the PBX if the power denial signal is less than or greater than the parameters entered here.
6. Click **Apply**.

TIMEOUT

The items in this branch control the duration of certain audible tones.

To set the time-out:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Timeout** branch.
4. Select either **Busy** or **Ring**. The following field appears in the Configuration pane:



Busy Timeout: 20

Time period (in seconds) that the busy signal is heard after the call is disconnected.

5. Enter the appropriate setting:
   - **Busy**
     This setting is measured in seconds and defines the amount of time that the busy signal is heard after the call is disconnected.
   - **Ring**
     This setting is measured in seconds and defines the amount of time that the called party's phone rings until the ringing is automatically discontinued.
6. Click **DTMF Interval** and enter a period of time measured in seconds. This parameter defines the period of time the Gateway pauses between the sending of each dual-tone multi-frequency (DTMF) tone.
7. Click **Apply**. The Reboot confirmation screen appears.
8. Select either **Reboot now** or **Reboot later**.

ADVANCED

The items in this branch control parameters that are rarely adjusted.

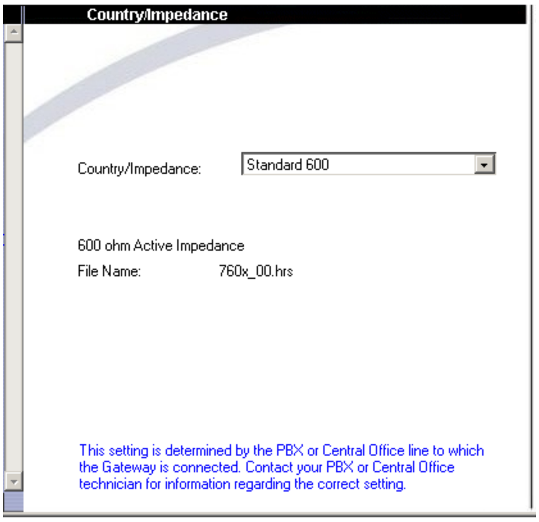
Country/Impedance

This parameter is displayed in FXO Gateways only.

The correct setting is determined by the PBX or Central Office line to which the Gateway is connected. Contact your PBX or Central Office technician for information regarding the correct setting.

To set the Country/Impedance:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Advanced** branch.
4. Select **Country/Impedance**. The following fields appear in the Configuration pane:



Country/Impedance: Standard 600

600 ohm Active Impedance

File Name: 760x_00.hrs

This setting is determined by the PBX or Central Office line to which the Gateway is connected. Contact your PBX or Central Office technician for information regarding the correct setting.

5. From the drop down list, select the settings given to you by your PBX or Central Office technician.
6. Click **Apply**. The Reboot confirmation screen appears.
7. Select either **Reboot now** or **Reboot later**.

Echo Canceller

A number of circumstances can cause an echo effect. Selecting Echo Canceller minimizes or cancels the echo effect.

To select Echo Canceller:

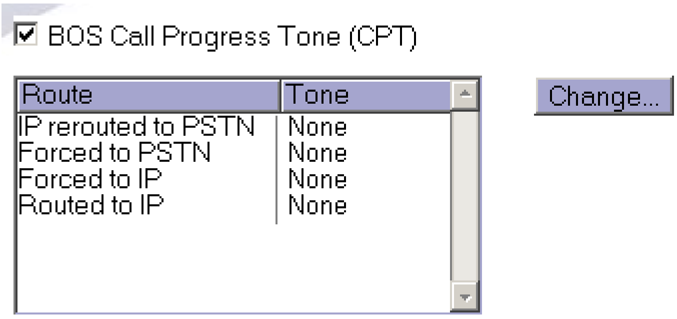
1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Advanced** branch.
4. Select **Echo Canceller**.
5. Select the **Echo Canceller** checkbox.
6. Click **Apply**. The Reboot confirmation screen appears.
7. Select either **Reboot now** or **Reboot later**.

BOS Tones

When the BOS Call Progress Tone is enabled, the caller hears a short, repeating tone during call progress.

To enable BOS tones:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Advanced** branch.
4. Select **BOS Tones**. The following fields appears in the configuration pane:



☑ BOS Call Progress Tone (CPT)

Route	Tone
IP rerouted to PSTN	None
Forced to PSTN	None
Forced to IP	None
Routed to IP	None

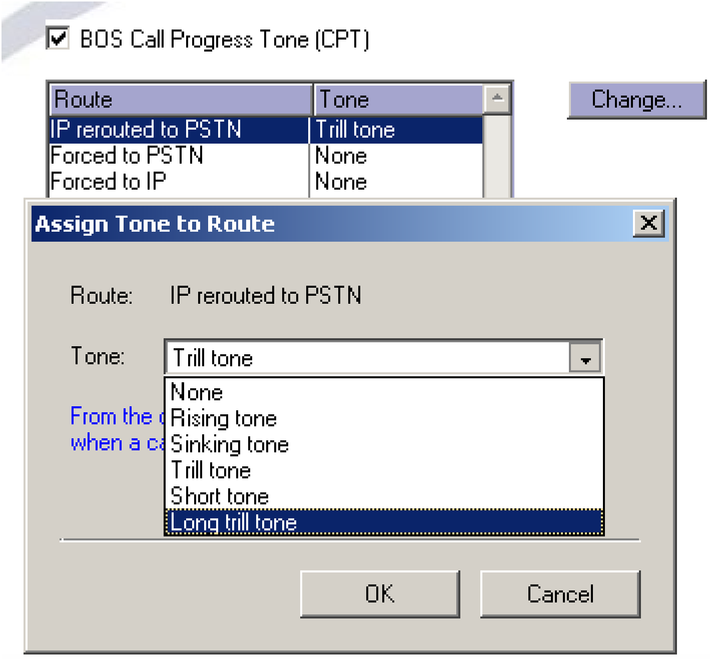
5. Select the **BOS Call Progress Tone** checkbox.

6. Select the route to which a tone will be assigned. There are four routes.

Table 36: BOS CPT Routes

Route	Tone Sent from BOS_Signals Table	GWs	Field Name
IP rerouted to PSTN	when the IP fails and the call is rerouted to the PSTN	Claro only	PstnNotIPSignal_U4
Forced to PSTN	when the call is forced (by prefix) to the PSTN	Claro only	PstnForcedSignal_U4
Forced to IP	when the call is forced (by prefix) to the IP	Claro only	IPForcedSignal_U4
Routed to IP	when the call goes to the IP normally, that is, after open voice)		IPOnlySignal_U4

7. Click **Change**. The Assign Tone to Route dialog box for the specific route is displayed.



☑ BOS Call Progress Tone (CPT)

Route	Tone
IP rerouted to PSTN	Trill tone
Forced to PSTN	None
Forced to IP	None

Assign Tone to Route

Route: IP rerouted to PSTN

Tone: Trill tone

8. Assign a tone to the designated route and click **OK**.

9. Repeat steps 6–8 as required.

10. Click **Apply**. The Reboot confirmation screen appears.

11. Select either **Reboot now** or **Reboot later**.

Jitter Buffer

Jitter adjusts delay in the voice transfer and thereby helps to improve the voice quality. It is often necessary when the VoIP network suffers from poor Internet connections. By default, jitter buffer is enabled. Disable it only upon consultation with Technical Support.

To disable Jitter Buffer:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Advanced** branch.
4. Select **Jitter Buffer**.
5. Clear the **Jitter Buffer** checkbox.
6. Click **Apply**. The Reboot confirmation screen appears.
7. Select either **Reboot now** or **Reboot later**.

Silence Suppression

This parameter must be set if using a PBX that does not return a busy tone.

Disabling Silence Suppression improves voice quality. However, this increases the transfer rate and causes the Gateway to engage more network bandwidth.

To disable Silence Suppression:

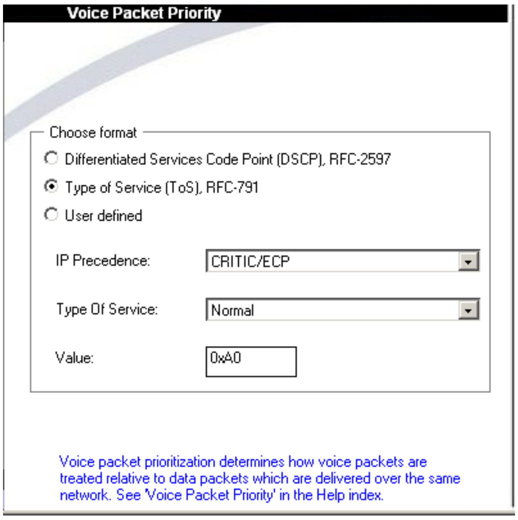
1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Advanced** branch.
4. Select **Silence Suppression**.
5. Clear the **Silence Suppression** checkbox.
6. Click **Apply**. The Reboot confirmation screen appears.
7. Select either **Reboot now** or **Reboot later**.

Voice Packet Priority—Tagging Packets

Use the Voice Packet Priority dialog box to enable and format the tagging of VoIP packets. Tagging is the assigning of a voice packet prioritization format to the IP Telephony network. Tagging gives one class of network traffic—in this case, VoIP packets—priority over other classes of traffic. Because VoIP is a real-time application, it requires a strict performance level.

To enable Voice Packet Priority:

1. From the Configurator main menu, select **VoIP Configuration**.
2. Expand the **Voice and Telephony** branch.
3. Expand the **Advanced** branch.
4. Select **Voice Packet Priority**. The following fields appear in the Configuration pane.



Voice Packet Priority

Choose format

○ Differentiated Services Code Point (DSCP), RFC-2597

● Type of Service (ToS), RFC-791

○ User defined

IP Precedence: CRITIC/ECP

Type Of Service: Normal

Value: 0xA0

Voice packet prioritization determines how voice packets are treated relative to data packets which are delivered over the same network. See 'Voice Packet Priority' in the Help index.

5. From the right pane, select and configure a format.

We recommend either of the following settings:
(a) As pictured above, use ToS. For IP precedence, select ***CRITIC/ECP****. For ToS, select* ***Normal****.*
(b) Use User Defined and define the value to 0xA0.

- **Differentiated Service (DiffServ)**
  This is the most recent set of Class of Service (CoS) rules which determine how Gateways forward a network packet. DiffServ makes use of a six-bit field in the IP header, called the Differentiated Services Code Point (DSCP), which indicates how a packet is to be forwarded. How Gateways forward packets is known as Per Hop Behavior (PHB).

The PHB distinguishes between service levels based upon bandwidth, queueing theory, and dropping (discarding the packet) decisions.

DiffServ replaces Type of Service (ToS). The Differentiated Services charter is at http://www.ietf.org/html.charters/diffserv-charter.html.

To use Differentiated Service, all Gateways on the IP Telephony network must be DiffServ-enabled, that is, able to process the DiffServ field.

- **Type of Service (ToS)**
  ToS refers to a field within an IP header that instructs a Gateway to assign a specific Class of Service (CoS) level to a packet. ToS makes use of only three bits in the layer 2 packet header and is, therefore, limited in its ability to manage IP Telephone network traffic.
- **User Defined**
  The system administrator can assign values using hexadecimal numbers. (The prefix 0x indicates hexadecimal digits.) Use two hexadecimal digits; two hexadecimal digits represent one byte.

6. Click **Apply**. The Reboot confirmation screen appears.
7. Select either **Reboot now** or **Reboot later**.

Additional information on DiffServ and ToS is available from the following RFCs: 1349, 2474, 2475, 2597, 2598, 2638.

STATISTIC SERVERS

Three types of statistic servers can be used with BOSâNOVA Gateways:

- BOSâNOVA Call Details Record (CDR) Server
- Q–CDR Server
- Quality Status Record

The two CDR Server options are completely independent of each other. Either may be enabled or both may simultaneously be enabled.

Call Details Records (CDR) Server

Enable this feature if Call Detail Records (CDR) are administered by BOSâNOVA equipment.

CDR is a program that records information about incoming and outgoing calls. The information is stored in a buffer on the Gateway. See also, the section *Call Detail Records* beginning on page 345.

To view the CDR information:

1. From the Configurator main menu, select **VoIP Configuration**.
2. From the Parameters field, expand the Statistics Server branch.
3. From the Parameters field, select **Enable CDR sending**.
4. In the right pane, select the checkbox.
5. From the Parameters field, select **CDR Server IP**.
6. Enter the IP address of the CDR Server, that is, the computer that will receive the CDR buffer.

Q–CDR Server

Enable this feature if Call Detail Records (CDR) are administered by third-party equipment. Select the checkbox and select the format being used.

There are two possible definitions of the direction:

- If the Gateway initiates the connection, define the direction as Outbound.
- If the CDR Server initiates the connection, define the direction as Inbound.

Then, enter the IP address, TCP/IP port number, and password of the third-party CDR Server.

Quality Status Reporting (QSR) Server

QSR is a program that records information about the quality of different Internet paths between Gateways.   The information is stored in a buffer on the Gateway.

To view the QSR information:

1. From the Configurator main menu, select **VoIP Configuration**.
2. From the Parameters field, expand the Statistics Server branch.
3. From the Parameters field, select **Enable QSR sending**.
4. In the right pane, select the checkbox.
5. From the Parameters field, select **QSR Server IP**.
6. Enter the IP address of the QSR Server, that is, the computer that will receive the QSR buffer.

QUALITY OF SERVICE (QoS)

The Quality of Service (QoS) module monitors calling parameters in order to determine which route will provide the best call quality.

The Quality of Service (QoS) module monitors call quality by:

- keeping track of packets received
- keeping track of packets lost
- monitoring jitter
- monitoring latency period (time lapse) for both directions of the conversation

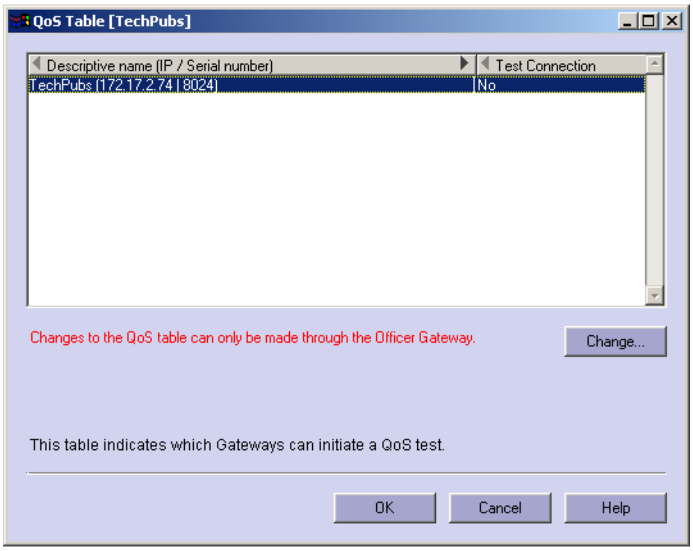
Based upon the information gathered during monitoring, the Gateway chooses the best routes to transmit and receive packets.

Enabling QoS in a Gateway

To configure a Gateway to support the QoS module:

1. In a browser, enter the IP address of the BOSâNOVA ***Officer*** Gateway.
2. On the Sign-on screen, enter your password.
3. Click **Login**.

4. From the menu, select **QoS Table**. The QoS Table screen is displayed.



TechPubs (172.17.2.74 | 8024) No

Changes to the QoS table can only be made through the Officer Gateway.

This table indicates which Gateways can initiate a QoS test.

5. Click **Change**. The Change QoS Settings dialog box opens.
6. Select **Initiate Quality of Service**. Selecting the checkbox indicates that the Gateway can both initiate a test signal and receive a test signal from another Gateway.
7. Click **OK**.

Setting Test Frequency and Threshold

To set QoS test frequency and the voice quality threshold at which an IP call is transferred to the PSTN:

1. In a browser, enter the IP address of the BOSâNOVA Gateway.
2. On the Sign-on screen, enter the password.
3. Click **Login**.
4. From the menu, select **VoIP Configuration**. The VoIP Configuration screen is displayed.
5. In the left pane, expand the QoS branch.
6. In the left pane, select **Frequency of Test**.
7. In the right pane, select either Fast, Medium, or Slow.
8. In the left pane, select **Threshold**.
9. In the right pane, enter an amount between 2.1 and 3.9. The higher the entry, the sooner the call will be transferred.
10. Click **Apply**.

IP Telephony...
Clear and Simple

SECTION 5: SIGNAL ANALYZER

The Signal Analyzer is a Wizard that can be run during the configuration of an FXO Gateway. The Wizard can execute two analysis:

- Use the **Disconnect Signal Analyzer** to (a) detect the signal generated by a PBX when a call is disconnected and (b) to configure the Gateway to recognize that signal. In most circumstances, the DSA Wizard will identify the PBX signals and automatically configure the Gateway to recognize them. If the Gateway does not recognize the disconnect signal, then it will not disconnect the calls between FXO Gateways.

  If the disconnect signal is not standard, the DSA wizard will listen to the PBX and then configure the Gateway to recognize the non-standard PBX disconnect signal.

- Use the **Dial Tone Analyzer** to (a) determine if the phone line connected to the Gateway is active and (b) to identify the tone received following initial off-hook.

For information related to the Disconnect Signal Analyzer see "Disconnect Supervision" on page 52.

THE DISCONNECT SIGNAL ANALYZER

Use the **Disconnect Signal Analyzer** to (a) detect the signal generated by a PBX when a call is disconnected and (b) to configure the Gateway to recognize that signal.

Before Running the DSA Wizard

Before running the DSA Wizard, you will need:

- two PBX lines available to connect to the Gateway
- to know the extension number of the line you connect to port one

Method of Operation

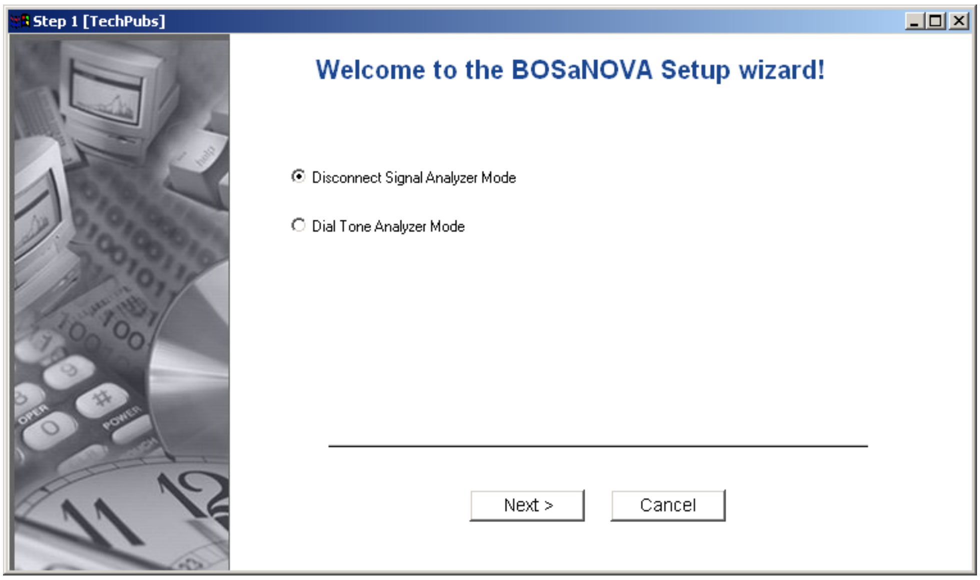
The Gateway uses the line connected to port two to call the Gateway through the PBX to the line connected to port one. The Gateway answers the call and line two hangs up. The Gateway then listens on line one for the disconnect signal. The DSA records and analyzes the disconnect signal, generates a graph, and displays the frequency and duration of the tone on and tone off segments of the signal.

⚠ *When the wizard starts, the Gateway will stop functioning and all active calls will be disconnected.*

To run the DSA:

1. Open a browser and connect to the configurator of the Gateway.

2. Select **Signal Analyzer**. The welcome screen opens.



Step 1 [TechPubs]

Welcome to the BOSaNOVA Setup wizard!

● Disconnect Signal Analyzer Mode

○ Dial Tone Analyzer Mode

3. Select **Disconnect Signal Analyzer** and click **Next**. The Gateway closes all active lines and restarts in the signal analyzer mode.

This may take some time. You must wait for confirmation before clicking ***Next****.*

4. Click **Next**.
5. Enter the PBX phone number for the line connected to port #1
6. Enter the amount of time you want the analyzer to record the signal.
7. Click **Next**. The Gateway calls itself from line 2 to line 1.
8. If the DSA did not recognize the signal, you must click **Next** and complete steps 9–13. However, if the signal is recognized, click **Finish**.
9. Use the mouse to select a section of the graph at least three seconds long.
10. Click **Next**.
11. Move the border. It is recommended to try and center the green line in the wave form. The default setting is 50%. The frequency and duration of the tone-on and tone-off segments of the signal are displayed.
12. Click **Next**. If the signal is recognized you will be asked to click **Finish** and this will end the wizard. If the signal is not recognized you will be asked to repeat steps **3** through **12**.
13. Click **Finish**.

THE DIAL TONE ANALYZER

Use the **Dial Tone Analyzer** to (a) determine if the phone line connected to the Gateway is active and (b) to identify the tone received following initial off-hook.

To run the Dial Tone Analyzer:

1. Open a browser and connect to the configurator of the Gateway.
2. Select **Signal Analyzer**. The DSA welcome screen opens.
3. Select **Dial Tone Analyzer** and click **Next**. The Gateway closes all active lines and restarts in the signal analyzer mode.
4. Follow the prompts that appear in the interface.

SECTION 6:
V-SERIES AND CLARO PRI CONFIGURATION

This section contains explanations and procedures about the PRI Configuration branch of the BOSâNOVA IP Telephony Gateway Configurator, including:

- Reviewing the current configuration, see p. 72
- Changing the configuration, see p. 73
- B-channel selection, see p. 77
- Using the restore buttons, see p. 77
- Making selections from the Actions drop down list, see p. 78

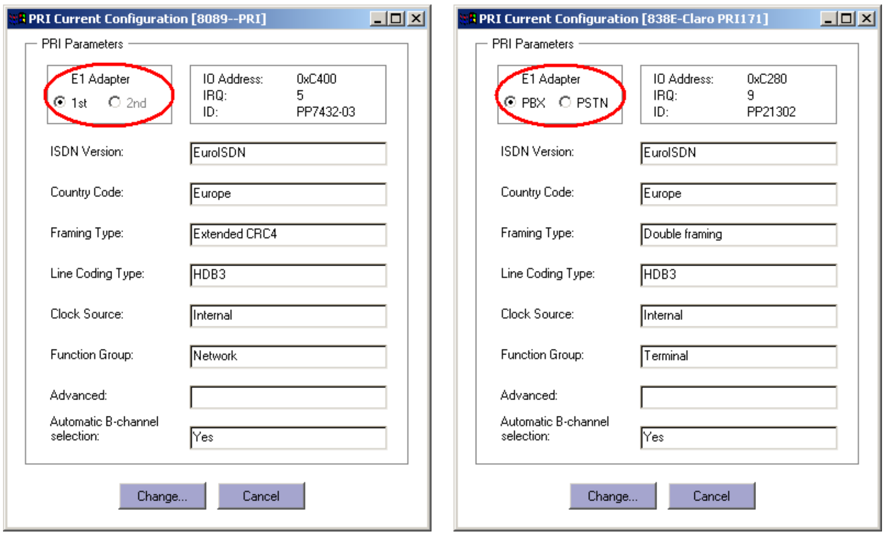
REVIEWING THE CURRENT CONFIGURATION

Reviewing the current configuration is done via the PRI Configuration screen.

1. In your browser, enter the IP address of the BOSâNOVA Gateway Configurator.
2. On the login screen, enter your password and click **Login**. The Configurator main menu is displayed.

*If **PRI Configuration** does not appear in the VoIP menu, the Gateway is not a PRI Gateway.*

3. From the Configurator main menu, select **PRI Configuration**. The PRI Current Configuration screen appears and displays the Gateway's existing settings.



PRI Current Configuration [8089--PRI]

PRI Parameters

E1 Adapter ● 1st ○ 2nd

IO Address: 0xC400
IRQ: 5
ID: PP7432-03

ISDN Version: EuroISDN
Country Code: Europe
Framing Type: Extended CRC4
Line Coding Type: HDB3
Clock Source: Internal
Function Group: Network
Advanced:
Automatic B-channel selection: Yes

PRI Current Configuration [838E-Claro PRI171]

PRI Parameters

E1 Adapter ● PBX ○ PSTN

IO Address: 0xC280
IRQ: 9
ID: PP21302

ISDN Version: EuroISDN
Country Code: Europe
Framing Type: Double framing
Line Coding Type: HDB3
Clock Source: Internal
Function Group: Terminal
Advanced:
Automatic B-channel selection: Yes

Comparison of V-Series and Claro PRI Current Configuration Screens

In contrast to the V-Series PRI—from version 2.11.00 and higher—the Claro PRI Current Configuration screen displays a PBX Adapter and a PSTN Adapter.

4. Review the settings. Click **Cancel** to return to the Configurator main menu.

CHANGING THE CONFIGURATION

*Clicking **Change** opens the PRI Configurator and Tester screen and disconnects all active lines.*

To make changes to the configuration, and to test the Gateway, on the PRI Current Configuration screen, click **Change**. The Gateway restarts in Configuration mode and the PRI Configurator and Tester screen opens.

At any time, press **Cancel** to close the PRI Configurator and Tester screen without saving changes. Wait 1-2 minutes for the Gateway to restart.

To view the impact of any change made in the PRI Parameters box, you must first click Send to PRI.

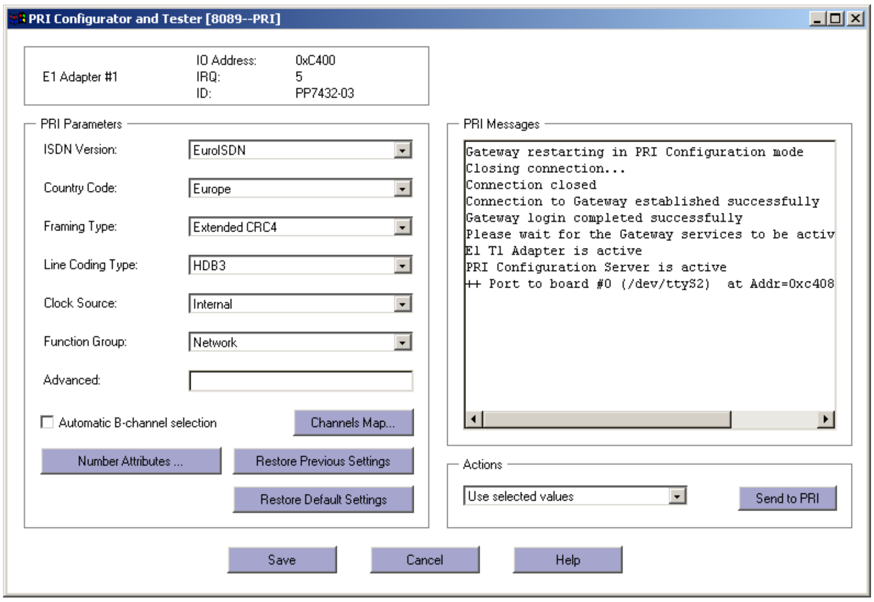
To configure the PRI settings:

1. Ensure that all cables are properly attached to the rear panel of the Gateway.
2. From the Configurator main menu, select **Bypass Mode** and ensure that the Gateway is in **Software bypass** mode.
3. Know the number to be dialed to connect to the Gateway and a number that can be dialed from the Gateway.
4. From the PBX technician or from the Central Office technician, obtain accurate setting information for the following parameters:
   - ISDN Version
   - Country Code
   - Framing Type
   - Line Coding Type
   - Clock Source
   - Function Group

Step 4, opening the PRI Configurator and Tester screen, disconnects all active lines.

5. From the PRI Current Configuration screen, click **Change**. A warning message is displayed.

6. Click **Yes** to confirm the choice. The PRI Configurator and Tester screen opens but remains disabled until the Gateway has restarted in configuration mode.



PRI Configurator and Tester [8089--PRI]

E1 Adapter #1

IO Address: 0xC400
IRQ: 5
ID: PP7432-03

PRI Parameters

ISDN Version: EuroISDN
Country Code: Europe
Framing Type: Extended CRC4
Line Coding Type: HDB3
Clock Source: Internal
Function Group: Network
Advanced:

□ Automatic B-channel selection

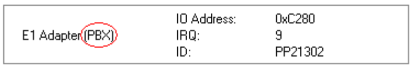
PRI Messages

```
Gateway restarting in PRI Configuration mode
Closing connection...
Connection closed
Connection to Gateway established successfully
Gateway login completed successfully
Please wait for the Gateway services to be activ
E1 T1 Adapter is active
PRI Configuration Server is active
++ Port to board #0 (/dev/ttyS2)  at Addr=0xc408
```

Actions

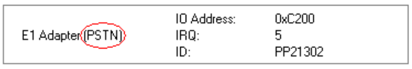
Use selected values

In the Claro PRI—from version 2.11.00 and higher—the interface indicates which Configurator and Tester screen has been opened: the PBX Adapter or the PSTN Adapter. These correspond to the ports on the Claro PRI.



E1 Adapter (PBX)

IO Address: 0xC280
IRQ: 9
ID: PP21302



E1 Adapter (PSTN)

IO Address: 0xC200
IRQ: 5
ID: PP21302

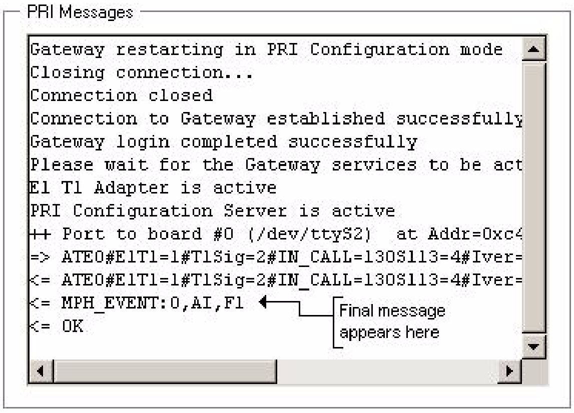
7. For each drop-down list, select the correct setting as per the instructions you received from the PBX technician or the Central Office technician.

8. From the Actions drop-down list, select **Use selected values**.

9. Click **Send to PRI**.

   If the PRI configuration is fine, the final message in the PRI messages field will be:

   <= MPH_Event:0, AI, F1.



PRI Messages

```
Gateway restarting in PRI Configuration mode
Closing connection...
Connection closed
Connection to Gateway established successfully
Gateway login completed successfully
Please wait for the Gateway services to be act
E1 T1 Adapter is active
PRI Configuration Server is active
++ Port to board #0 (/dev/ttyS2)  at Addr=0xc4
=> ATE0#E1T1=1#T1Sig=2#IN_CALL=130S113=4#Iver=
<= ATE0#E1T1=1#T1Sig=2#IN_CALL=130S113=4#Iver=
<= MPH_EVENT:0,AI,F1
<= OK
```

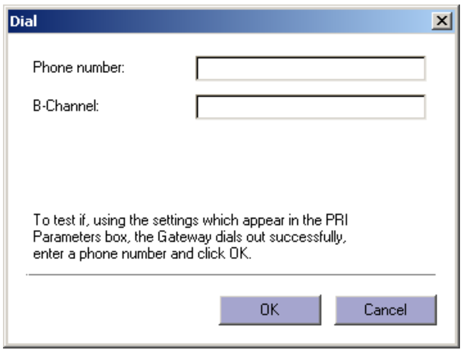
   If F1 does not appear at the end of the string, one of the settings controlling lower level synchronization is wrong. The parameters controlling lower level synchronization are Framing Type, Line Coding Type, and Clock Source. Correct the setting and click **Send to PRI**.

10. Call the Gateway and observe the PRI Messages field as the call is received. If the PRI configuration is fine, the final message in the PRI messages field will be:

    <=RING … nnn

    where, nnn represents the number dialed to call the Gateway. If the number dialed to call the Gateway does not appear at the end of the string, one of the settings controlling call progress is wrong. The parameters controlling call progress are ISDN Type, Country Code, and Function Group. Correct the setting and try again.

11. From the Actions drop-down list, select **Dial** and click **Send to PRI**. The Dial dialog box appears.



Dial

Phone number:

B-Channel:

To test if, using the settings which appear in the PRI Parameters box, the Gateway dials out successfully, enter a phone number and click OK.

12. Enter a phone number that should be reachable from the Gateway, disregard the B-Channel field, and click **OK**.

13. Observe the PRI Messages field as the call progresses. If the PRI configuration is fine, and the receiver of the called phone is not lifted, the final message in the PRI messages field will be either:

    <= PROGRESS or <=ALERT...

    If the receiver of the called phone is lifted, the final message in the PRI messages field will be:

    <= CONNECTED...

    If none of these messages appear, one of the settings controlling call progress is wrong. The parameters controlling call progress are ISDN Type, Country Code, and Function Group. Correct the setting and try again.

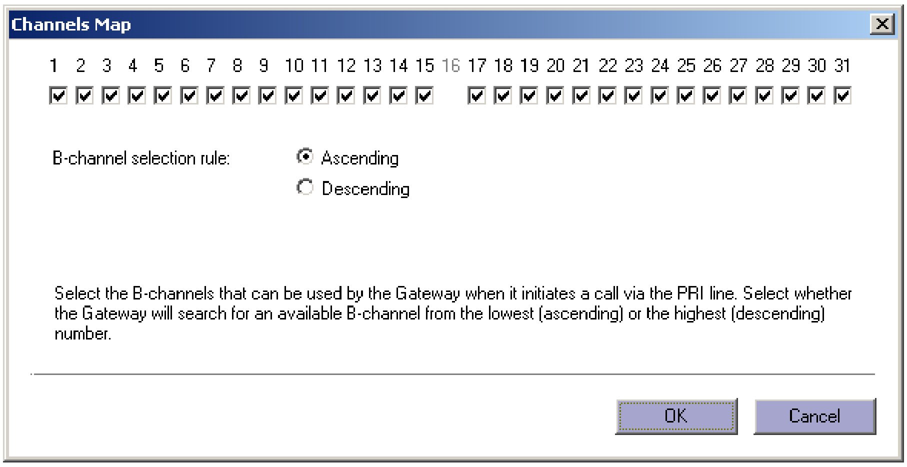
14. Click **Save**. The PRI Configurator and Tester closes and the Gateway restarts.

B-CHANNEL SELECTION

By default, the Automatic B-channel selection (bearer channel) checkbox is selected. This allows the Gateway to select the B-channel that carries the main data.

In limited circumstances, some of the B-channels might not be available for Gateway usage. In this case:

1. Clear the Automatic B-channel selection checkbox.
2. Click **Channels Map**. The Channels Map dialog box opens.



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑		☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

B-channel selection rule: ● Ascending
○ Descending

Select the B-channels that can be used by the Gateway when it initiates a call via the PRI line. Select whether the Gateway will search for an available B-channel from the lowest (ascending) or the highest (descending) number.

3. Select the B-channels that are available to the Gateway.
4. Select the direction the Gateway will search for an available B-channel, either ascending or descending, and click **OK**.

THE RESTORE BUTTONS

At the bottom of the PRI Parameters box are two buttons:

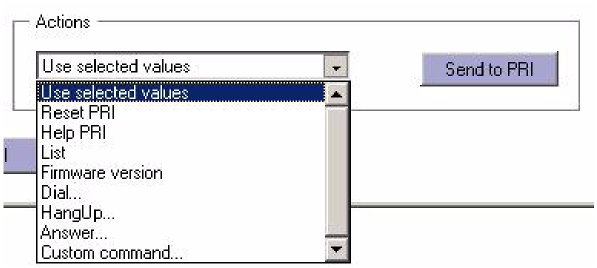
Restore Previous Settings

Click **Restore Previous Settings** to return to the last saved configuration, that is, the settings that were displayed on the PRI Configuration screen.

Restore Default Settings

Click **Restore Default Settings** to return to the factory assigned Gateway configuration.

THE ACTIONS DROP-DOWN LIST



The Actions Drop-down List

Three types of actions are available from the drop-down list:

- actions which affect the PRI board,
- actions which display information concerning the PRI board, and
- actions which exit to the PRI line.

To view the impact of any change made in the PRI Parameters box, you must first click Send to PRI.

Following are explanations of the items in the Actions drop-down list:

- **Use Selected Values:**
  Select **Use Selected Values** and click **Send to PRI** to reconfigure the PRI board according to the settings in the PRI Parameters box. As explained above (in the PRI Configurator and Tester section), this will also reveal the status of lower level synchronization.
- **Reset PRI:**
  Select **Reset PRI** and click **Send to PRI** to reset the PRI hardware.
- **Help PRI:**
  Select **Help PRI** and click **Send to PRI** to display a list of commands that can be sent to the PRI board. The list is displayed in the PRI Messages box. If necessary, enter any of these commands in the Advanced field of the PRI Parameters box.
- **List:**
  Select **List** and click **Send to PRI** to display a list which compares current values with default values. The list is displayed in the PRI Messages box.

- **Firmware Version:**
  Select **Firmware Version** and click **Send to PRI** to display version information regarding the programming that is contained in the read-only memory. The version information is displayed in the PRI Messages box.
- **Dial:**
  Select **Dial** and click **Send to PRI** to test if, using the settings which appear in the PRI Parameters box, the Gateway dials out successfully. The Dial dialog box opens. Enter a phone number, click **OK**.
- **Hang up:**
  Select **Hang up** and click **Send to PRI** to disconnect from a test which is connected. The Hang-up dialog box opens. In the Call ID field, enter the number that appears in the PRI Messages box, either after the word <=CONNECTED or after the word <=RING. That number, which can be from 1 - 99, is the Call ID. Click **OK**.
- **Answer:**
  Select **Answer** and click **Send to PRI** to test if, using the settings which appear in the PRI Parameters box, the Gateway answers successfully. The Answer dialog box opens. In the Call ID field, enter the number that appears in the PRI Messages box, either after the word <=CONNECTED or after the word <=RING. That number, which can be from 1 - 99, is the Call ID. Click **OK**.
- **Custom command:**
  Enter any command and click **Send to PRI**. Commands must match Omnitel Netbricks specifications.

SECTION 7:
NUMBERING PLAN OVERVIEW

This section provides:

- An overview of Connection Types supported by BOSâNOVA Gateways, see p. 81
- An overview of the structure of telephone numbers as established by the ITU E.164 standard, see p. 83
- How the BOSâNOVA Numbering Plan works, see p. 85
- Basic concepts concerning configuration of the Numbering Plan, see p. 88
- Saving a Numbering Plan, see p. 89
- An overview of each of the Numbering Plan's parameters, see p. 90

Configuration is assigned per port.
Notwithstanding the fact that lines are attached to ports, since Gateways contain ports, all documentation and User Interface refers to the configuration of ports, not lines.

CONNECTION TYPES THAT ARE SUPPORTED

A BOSâNOVA Gateway can be connected to a VoIP network via one of three Connection Types.

- ***Select*** a Connection Type using the Numbering Plan Wizard (see *Connection Type* on page 145).
- ***Configure*** the Connection Type using both the Numbering Plan Wizard and the Numbering Plan Configurator.

Connection via a BOSâNOVA Officer Gateway

The Officer Gateway is the Gateway on a BOSâNOVA IP Telephony network which compiles, maintains, and distributes a synthesis of all the other Gateway information. The section entitled *Using the Officer Gateway*, which begins on page 203, contains an overview of the responsibilities of, and procedures for configuring, the Officer Gateway.

Much of this section relates only to VoIP networks operating via a BOSâNOVA Officer Gateway.

Connection via a SIP Proxy

A SIP proxy is a computer running the Session Initiation Protocol (SIP). SIP is one of two protocols for carrying voice over IP. Procedures for configuring a SIP Proxy begin on page 183.

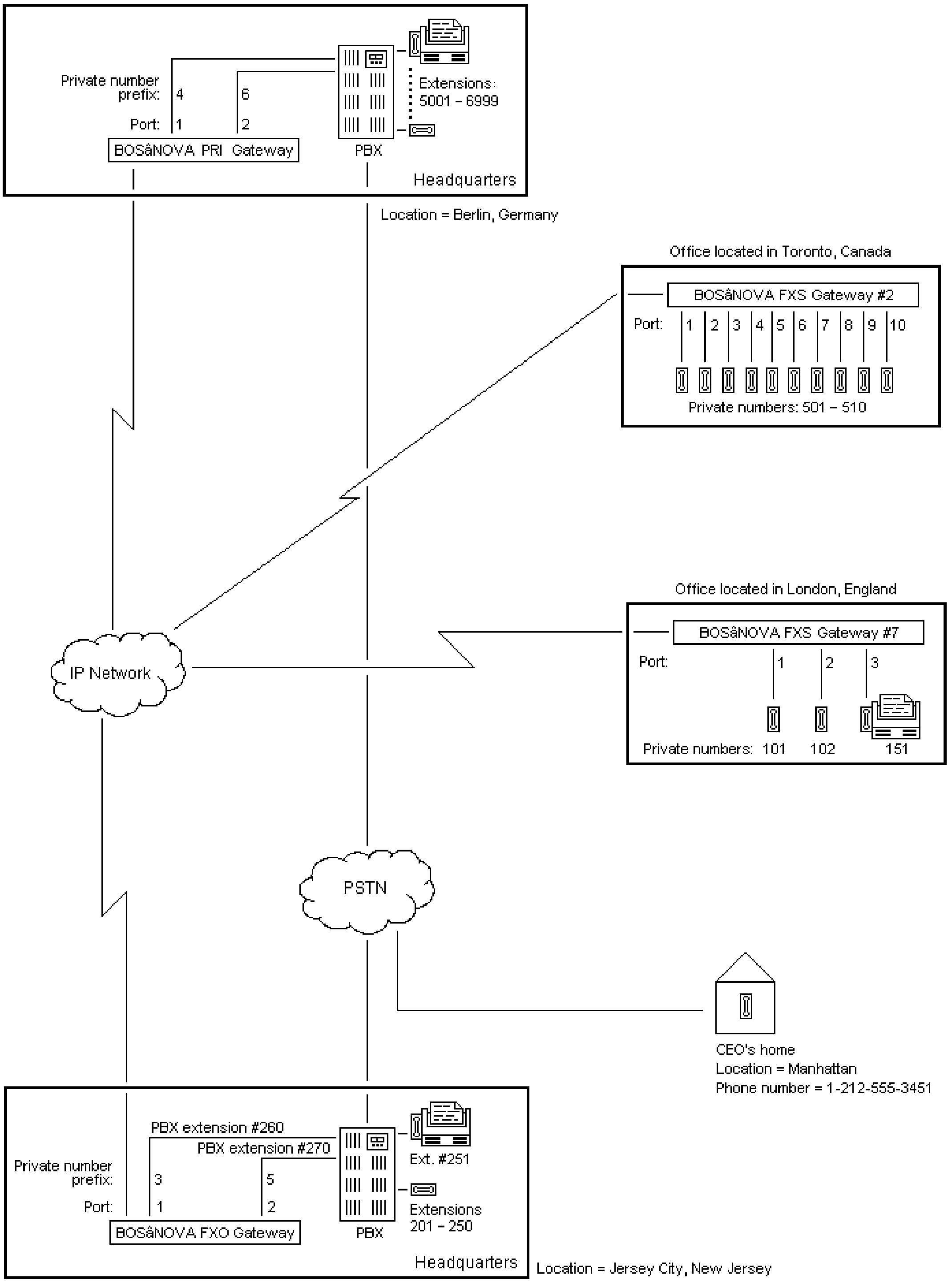
Connection via an H.323 Gatekeeper

A gatekeeper is a computer that performs address resolution and manages call control and network resources. It also provides call authorization and call accounting. Procedures for configuring an H.323 Gatekeeper begin on page 147.

See “Selecting H.323 or SIP” on page 113 for an overview of the SIP and H.323 protocols.

NETWORK CONFIGURATION

The following diagram illustrates the IP Telephony network that will be discussed throughout this section.



STRUCTURE OF A TELEPHONE NUMBER

To configure a numbering plan, the administrator must possess a basic understanding of the structure of an international telephone number. This structure is based, in part, upon the ITU E.164 standard.

ITU E.164 Standard

E.164 defines an international telephone number as being made up of a maximum of 15 digits. The 15 digits are divided into three categories:

Country Code (CC)
The CC is the 1–3 digit prefix dialed when calling to a particular country from another country.

Each country has been assigned an ID number. Mexico's CC is 52; Canada and the United States share the CC 1; Greenland's CC is 299.

National Destination Code (NDC)
The NDC is the digit or digits assigned to an area within the country. Therefore, it is also called the ***area code***. The NDC is dialed when calling to a particular area in the country from another country and when making a call within the same country from one area to another.

For example, metro Toronto's area code (that is, NDC) is 416. Manhattan's NDC is 212.

Subscriber Number (SN)
The subscriber number is the local telephone number without an NDC or a CC. In other words, it is the number you call when you call your neighbor across the street.

For example, the subscriber number (that is, telephone number) for information anywhere in the United States is 555-1212.

Table 37: E.164 Phone Number Structure, Examples

E.164 Number of:	CC	NDC (area code)	SN (telephone number)
Toronto	1	416	123-4567
Chicago	1	312	123-4567
London	44	207	123-4567
Berlin	49	30	123-4567

Other Components of a Telephone Number

In addition to the E.164 structure, there are other digits in the structure of a telephone number. They include:

National Trunk Prefix (NTP)
The NTP is the digit or digits dialed before the NDC when calling from one area to another area within the same country. In most countries, the NTP is either 0 or 1. In Mexico, the NTP is 01. (This is also known as the National Direct Dialing prefix.) For example, from New York to London one must dial 011-44-20-1234567. However, from another area in the UK to London, one must dial 0-20-1234567. In this case, the zero is the National Trunk Prefix.

International Access Codes (IACs)
The IAC is the international prefix needed to dial a call from one country to another country. It is dialed before the CC. In many countries this is either 00 or 011. In Israel, the user can choose from three companies that provide this service whose IACs are 012, 013, and 014. (This is also known as the International Direct Dialing prefix.)

Access Code
When dialing through a company's local switchboard (a PBX) to a number outside of the company, the user must first be allocated a line to the PSTN. The number dialed to get an outside line is called an access code.

Following are examples of phone number structures:

Table 38: From an Office Extension to a Foreign Country

To dial … from …	Access Code	International Access Code	CC	NDC (area code)	SN (telephone number)
Toronto from London	9	00	1	416	123-4567
Chicago from Tel Aviv	9	012	1	312	123-4567
London from New York	9	011	44	207	123-4567

Table 39: From an Office Extension to Another Area in the Same Country

To dial … from …	Access Code	National Trunk Prefix	NDC (area code)	SN (telephone number)
Toronto from Montreal	9	1	416	123-4567
Chicago from Miami	9	1	312	123-4567
London from Oxford	9	0	207	123-4567

HOW THE NUMBERING PLAN WORKS

Three components contribute to the operation of the BOSâNOVA IP Telephony Gateway Numbering Plan:

Dialing tables

The first component is the ***dialing tables***. As depicted in Figure # 3, two lists, called “dialing tables,” are kept on all Gateways.

- **Local dialing table**
  The local dialing table records the current dialing table configuration of the Gateway, including recent changes.
- **Common dialing table**
  The common dialing table is a synthesis of all local dialing tables.

Officer and Private Gateways

The second component is the division of responsibility between Gateways. This is reflected in the interface via a military metaphor.

- One Gateway is assigned the role of ***Officer***.
- The other Gateways are assigned the role of ***Private***.

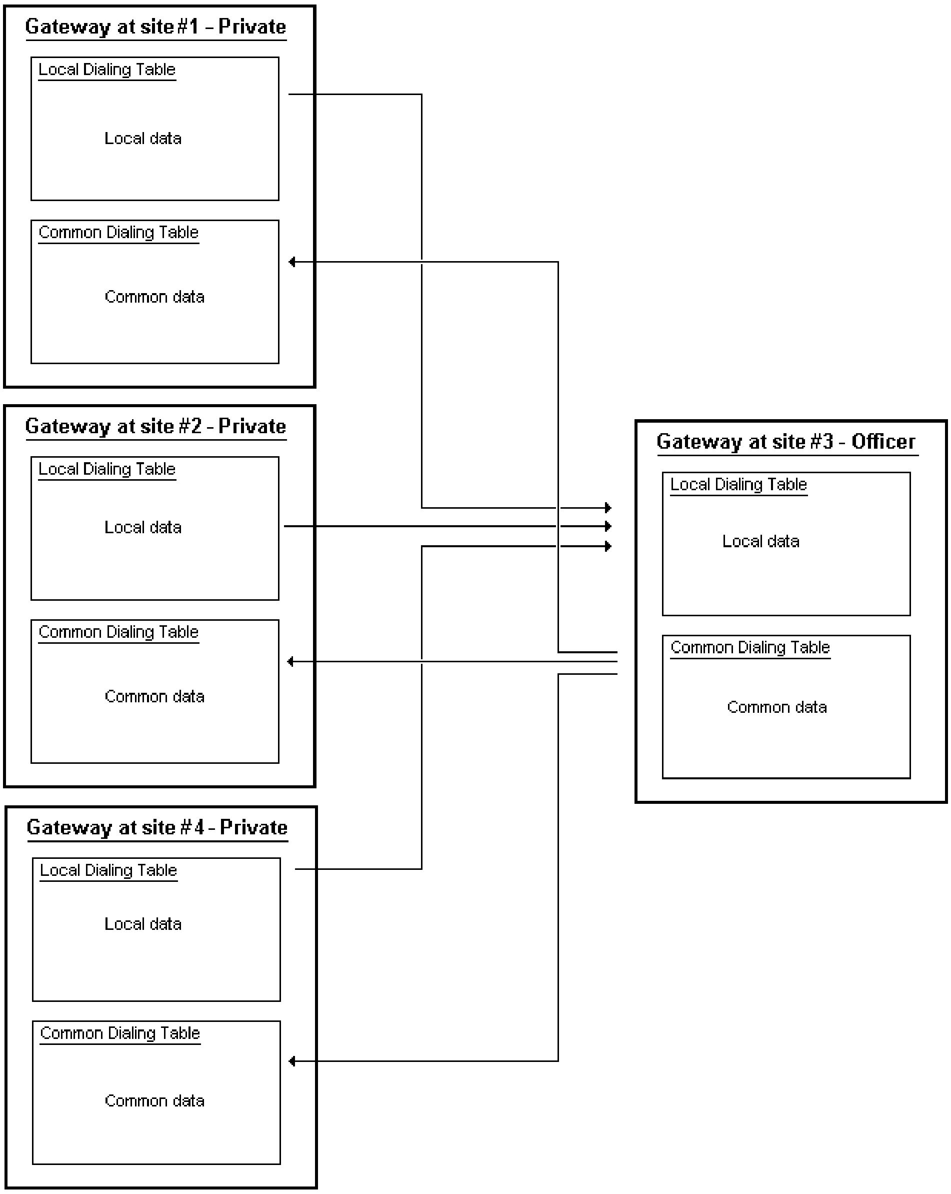
As depicted in Figure # 3, the Officer Gateway compiles, maintains, and distributes a synthesis of all local dialing tables called, as mentioned above, the common dialing table. Prior to distribution, the Officer assigns a version number to the updated common dialing table.

In addition, the Officer Gateway approves or rejects changes to the numbering plan submitted by other Gateways. For example, referring again to Figure # 3, if the network administrator attempted to add a third line to Gateway #2 and assign that line the private-number prefix “2,” the Officer would reject that assignment since private-number prefix “2” is used by Gateway #1.

When the version number of the Private’s common dialing table matches the latest common dialing table version number being distributed by the Officer, the dialing tables are ***synchronized***. If they are not identical, the dialing tables are not synchronized.

The dialing tables are used by the Gateways to resolve phone numbers.

Figure 3: Dialing Tables and Division of Responsibility



The Officer Gateway also functions as a Private Gateway and has its own local dialing table which it includes in the common dialing table.

Private and Public Numbers

The third component is the ability to differentiate between, and resolve calls, using both ***private-numbers*** and ***public-numbers***.

- **Private-numbers**
  Private-numbers are short numbers that, usually, are used within an enterprise. They are also called "internal" numbers or extensions.
- **Public numbers**
  Public numbers are regular telephone numbers (based upon the ITU E.164 standard), are at least seven digits in length, and are dialed to get any number on a PSTN. Examples of public telephone numbers are:

  In the USA: 1-212-555-1212

  In the UK: 44-116-282-0600

A prefix is usually attached to private numbers (see p. 91). The term "full private-number" is used when we refer to the combination of prefix + private-number.

As a result, configuration can include the ability to redirect calls from the Gateways to the PSTN (hop-off calls) and to assign a private-number to a public-number. Regarding the Claro Gateway, configuration can allow users to dial all phone numbers normally, (that is, as per the ITU E.164 standard) including extensions of a PBX. Users can dial as if they were using the PSTN, when, in fact, their call is routed over the IP Telephony network, not the PSTN.

THE BASICS OF CONFIGURATION

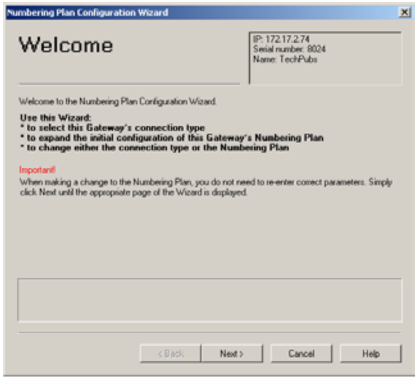
Familiarity with the following three points simplifies configuration of the Numbering Plan.

1. We recommend that you first map out the numbering plan of the entire IP Telephony network. Configuration is easier if the design of the numbering plan is complete before beginning configuration of the Gateways.

Configuration is applied per port. Therefore, the design of the numbering plan must account for each port of each Gateway.

2. Numbering Plan configuration is completed:

- **85% in the Numbering Plan Wizard:** The Numbering Plan Wizard opens automatically the first time you run the Gateway. Subsequently, access the Numbering Plan Wizard by selecting **Local Parameters** or **Connection Type** and clicking **Change** in the Numbering Plan Configurator.



Numbering Plan Configuration Wizard

Welcome

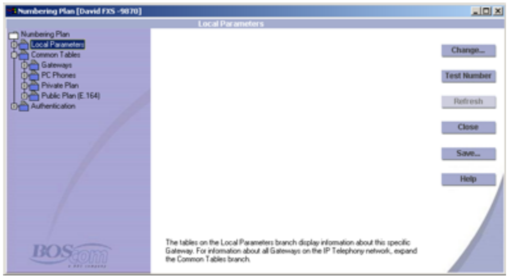
IP: 172.17.2.74
Serial number: 8024
Name: TechPubs

Welcome to the Numbering Plan Configuration Wizard.

Use this Wizard:
*** to select this Gateway's connection type**
*** to expand the initial configuration of this Gateway's Numbering Plan**
*** to change either the connection type or the Numbering Plan**

Important!
When making a change to the Numbering Plan, you do not need to re-enter correct parameters. Simply click Next until the appropriate page of the Wizard is displayed.

- **10% in the Numbering Plan Configurator:** Rule Based Number Management (RBNM) is configured in the Numbering Plan Configurator. Also, components of the Numbering Plan controlled by the Officer are configured in the Officer's Numbering Plan Configurator. These include Private-number length, BOSâNOVA Connects, third party Gateways, and Hop-off Private to Public number associations.

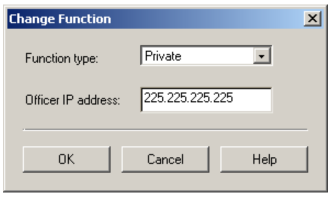


Numbering Plan [David FXS -9870]

Local Parameters

The tables on the Local Parameters branch display information about this specific Gateway. For information about all Gateways on the IP Telephony network, expand the Common Tables branch.

- **5% in the Dialing Server:** The IP address of the Officer Gateway is entered in the Dialing Server.



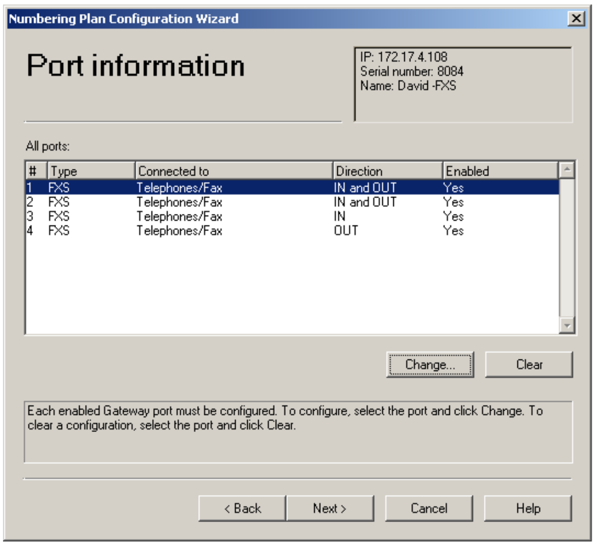
Change Function

Function type: Private

Officer IP address: 225.225.225.225

3. There is a difference between initial configuration and subsequent reconfiguration:

   - **During initial configuration:**
     Configure each page of the Numbering Plan Wizard before continuing to the next page. On several pages—for example, the two pages pictured below—***enter information for each port before continuing to the next page***.



Numbering Plan Configuration Wizard

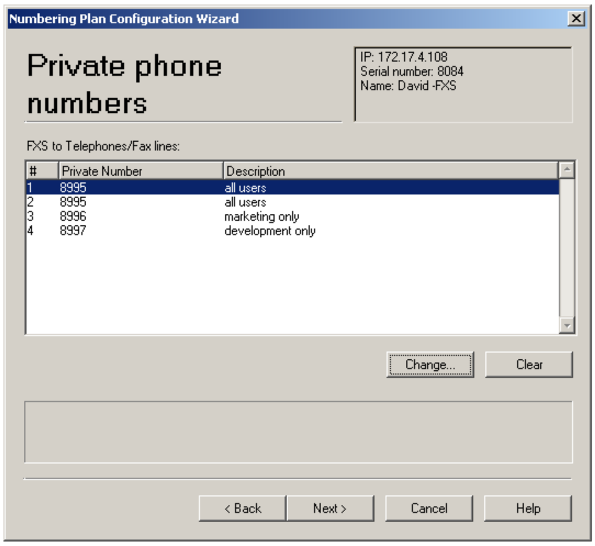
Port information

IP: 172.17.4.108
Serial number: 8084
Name: David -FXS

All ports:

#	Type	Connected to	Direction	Enabled
1	FXS	Telephones/Fax	IN and OUT	Yes
2	FXS	Telephones/Fax	IN and OUT	Yes
3	FXS	Telephones/Fax	IN	Yes
4	FXS	Telephones/Fax	OUT	Yes

Each enabled Gateway port must be configured. To configure, select the port and click Change. To clear a configuration, select the port and click Clear.



Numbering Plan Configuration Wizard

Private phone numbers

IP: 172.17.4.108
Serial number: 8084
Name: David -FXS

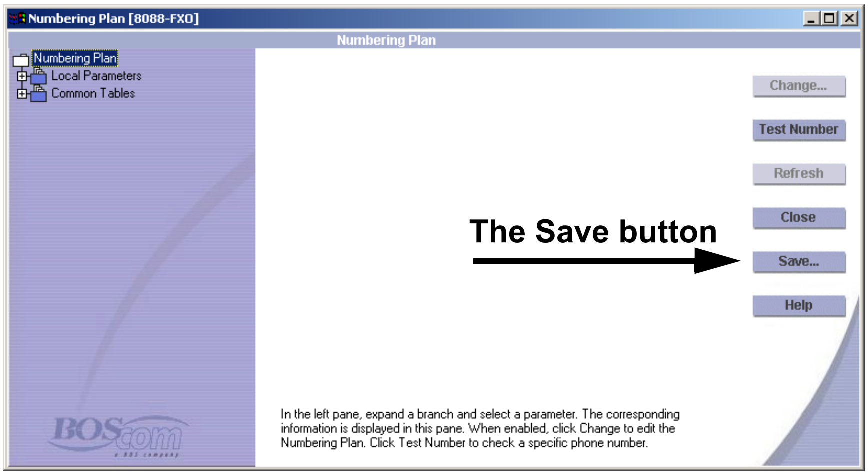
FXS to Telephones/Fax lines:

#	Private Number	Description
1	8995	all users
2	8995	all users
3	8996	marketing only
4	8997	development only

   - **During subsequent reconfiguration:**
     Click **Next** until the necessary page of the Wizard is displayed.

SAVING A NUMBERING PLAN

To save the entire IP Telephony network's Numbering Plan, from the main screen of the Numbering Plan Configurator, click **Save**. The Save dialog box opens. Designate a **Save in** location and **File name** and click **Save**. The plan is saved as a CSV file and can be opened in, for example, Microsoft Excel.



Numbering Plan [8088-FXO]

Numbering Plan

In the left pane, expand a branch and select a parameter. The corresponding information is displayed in this pane. When enabled, click Change to edit the Numbering Plan. Click Test Number to check a specific phone number.

COMPONENTS OF THE NUMBERING PLAN

The section contains an explanation of each parameter that may be configured when configuring a Numbering Plan.

For even the most simple configuration, the administrator must:

- Decide which *private-numbers* or *private-number prefixes* will be assigned to which ports, see p. 91
- Determine the *maximum private-number length*, see p. 94
- Assign an Officer Gateway, see p. 102

For configuration allowing use of the PSTN, the administrator must:

- Enable *Dial public numbers*, see p. 96.
  This feature must be enabled in order to use the BOSâNOVA Gateway Native Dialing feature.
- Allow termination of *Hop-off calls*, see p. 96

The following are optional:

- The administrator may configure *Automatic dialing*, see p. 98
- The administrator may configure *Private to public number associations*, see p. 103

For Claro Gateways the administrator must/may:

- Configure *Public number* blocks, see p. 105
- Enable *Dial private numbers*, see p. 105
- Configure *Private number blocks*, see p. 105
- Configure *IP Bypass numbers*, see p. 106
- Configure *Force dialout direction*, see p. 106

Private-Number Prefixes

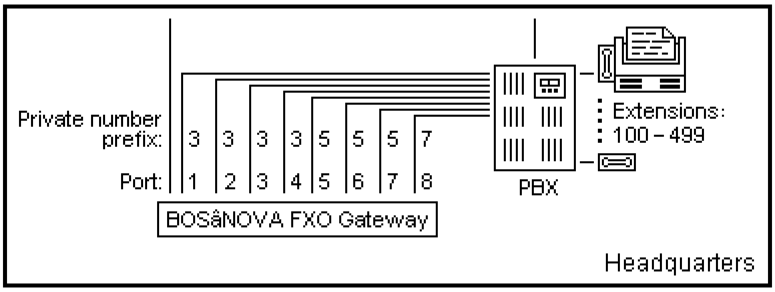
The procedure for assigning Private-number prefixes begins on page 125.

The administrator must assign private-number prefixes.

Private-Number Prefixes in a Gateway Connected to a PBX

In the context of an FXO or PRI Gateway connected to a PBX, private-number prefixes serve to identify the FXO or PRI port, and thereby the line into the PBX. Usually the ports of an FXO and PRI share the same private-number prefix, thereby creating a "pool" of lines. With an FXO, however, to enable special uses, one or more ports can be assigned a different private-number prefix.

In the following illustration, there are two pools of lines and one line designated for a special use.

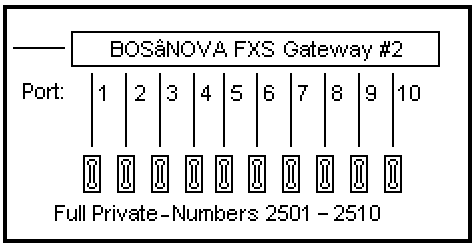


Private-Number in a Gateway Connected to Telephones

In the context of an FXS Gateway connected to telephony equipment, the administrator assigns private numbers, not private-number prefixes. The private-numbers serve to identify the FXS port, and thereby the line to the telephony equipment. The ports of an FXS can share the same private-number and thereby create a "pool" of lines. However, one or more ports can be assigned a unique private-number.

Private-number ***prefixes*** are not configured in an FXS connected to telephony equipment. However, the organization of the IP Telephony network's numbering plan is simplified greatly by using the first number of the private numbers to identify the Gateway on the IP Telephony network. Thus, the first number of a private-number might be thought of as a pseudo-private-number prefix.

In the following example, the private-numbers are 501–510. The number “2,” which precedes the private-number, is entered as part of the private-number. However, in this example, the number “2” can actually serve to identify the Gateway. Dialing any four digit “full private-number” which begins with a 2 will result in the call being forwarded to this Gateway.



To simplify a numbering plan, assign the same first number to all private-numbers on an FXS Gateway.

Private-Number Prefixes in a Gateway Connected to the PSTN

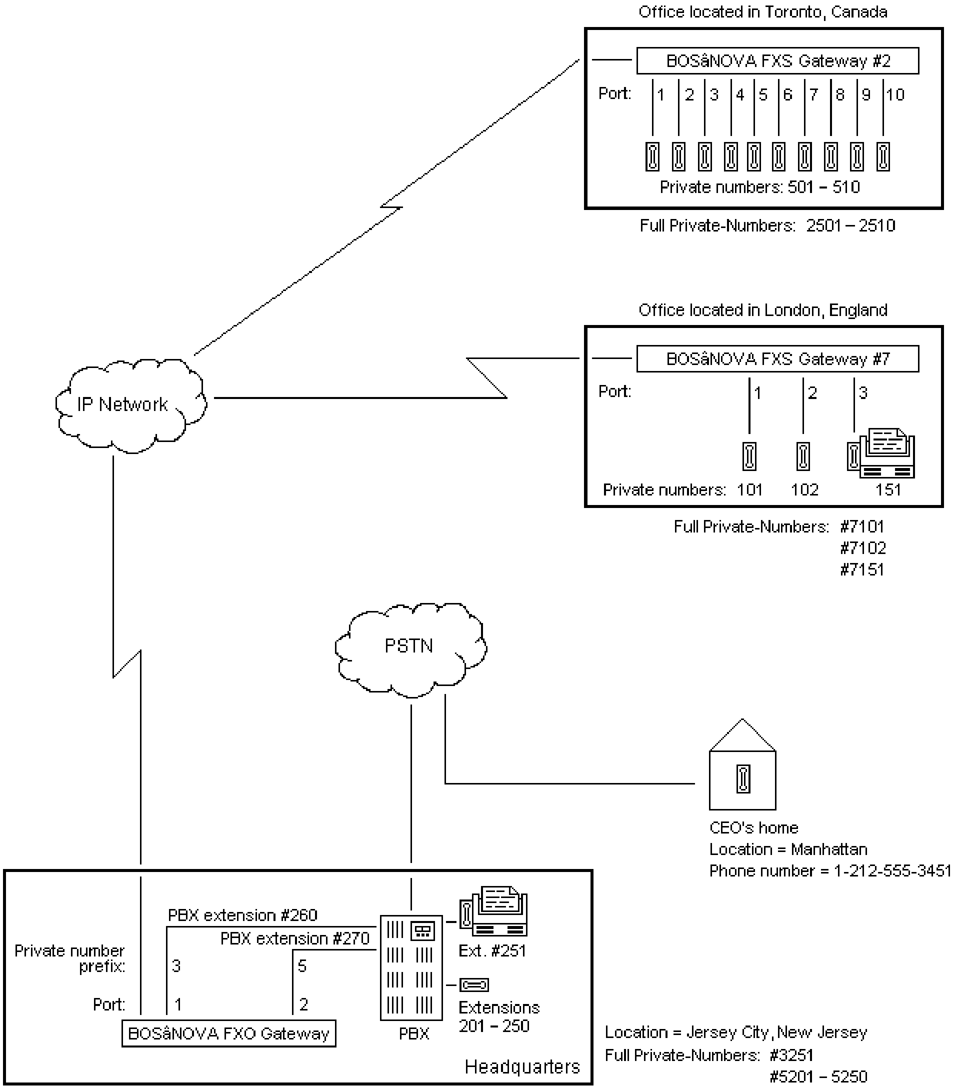
In the context of an FXO or PRI port connected to the PSTN, private-number prefix is not relevant. Instead, in these configurations, hop-off prefixes (see p. 128) take the place of private number prefixes.

Example of Private-Number Prefixes

In Figure # 4 on the following page:

- To dial from extension #101 to extension #102 within the London office, the user will dial #7102.
- To dial from extension #101 in the London office, to extension #501 in the Toronto office, the user will dial #2501.
- To dial from extension #101 in the London office, to extension #201 in the Jersey City office, the user will dial #5201.
- To send a fax from the London office to Jersey City office, the user dials #3251.
- To send a fax from the Jersey City office to the London office, the user must first dial the PBX extension which accesses the Gateway. Together, the user dials 260-7151.

Figure 4: Examples of Private-Number Prefixes


Office located in Toronto, Canada
BOSâNOVA FXS Gateway #2
Port: 1 2 3 4 5 6 7 8 9 10
Private numbers: 501 – 510
Full Private-Numbers: 2501 – 2510
Office located in London, England
BOSâNOVA FXS Gateway #7
Port: 1 2 3
Private numbers: 101 102 151
Full Private-Numbers: #7101 #7102 #7151
IP Network
PSTN
CEO's home
Location = Manhattan
Phone number = 1-212-555-3451
PBX extension #260
PBX extension #270
Private number prefix: 3 5
Port: 1 2
BOSâNOVA FXO Gateway
PBX
Ext. #251
Extensions 201 – 250
Headquarters
Location = Jersey City, New Jersey
Full Private-Numbers: #3251 #5201 – 5250

Maximum Private-Number Length

The procedure for configuring maximum private-number length begins on page 171.

The administrator must compile information that will enable him to determine the optimum maximum private-number length.

Maximum private-number length is determined by:

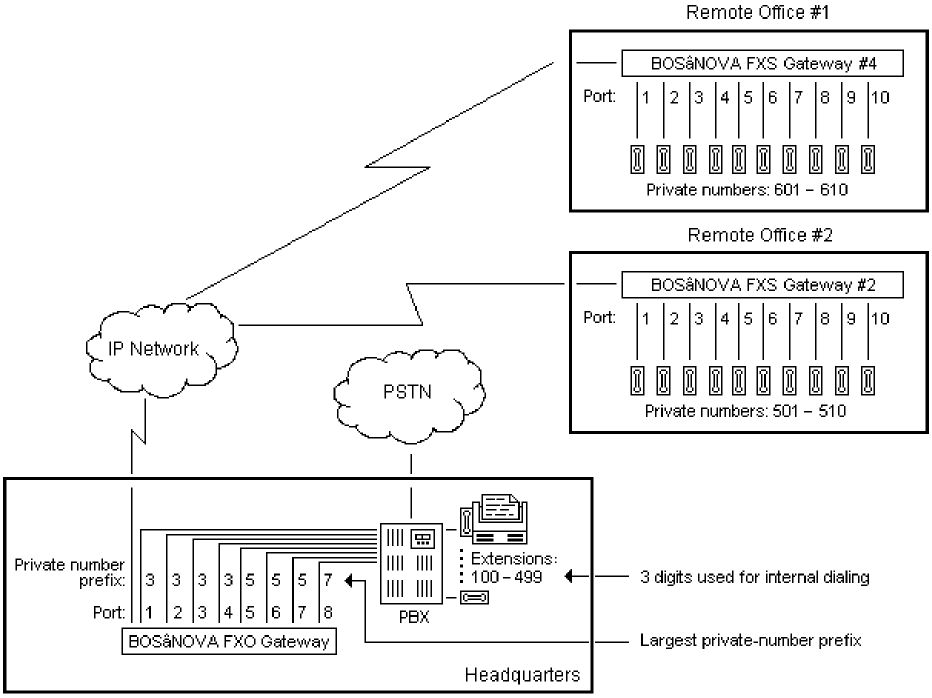
- the range spanned by PBXs that will be part of the IP Telephony network. If internal extensions are three digits in length, this sum is 3. If internal extensions are four digits in length, this sum is 4.
- the private-number prefixes that have been assigned. If all private-number prefixes are one digit, then this sum is 1. If some private-number prefixes are two digits in length, then this sum is two.

The following formula illustrates the calculation:

Number of digits used by the PBX with the greatest number of extensions
+
Number of digits in the largest assigned Private number prefix

Maximum Private number length

Figure 5: Determining Correct Maximum Private Number Length

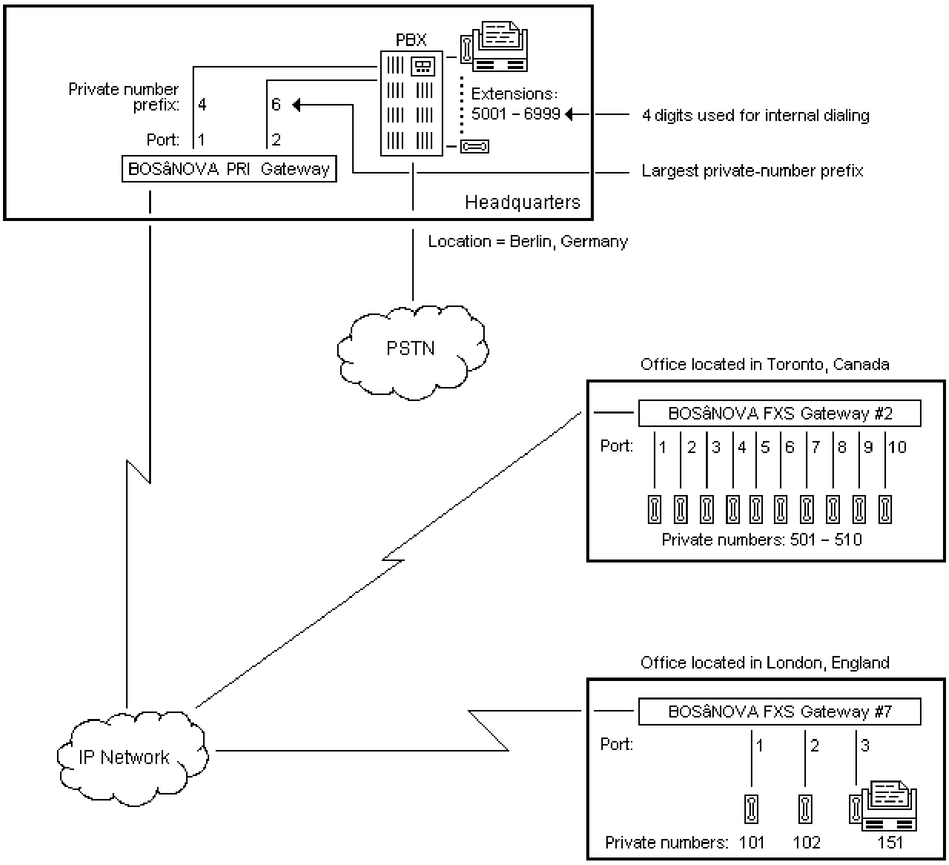


Remote Office #1
BOSâNOVA FXS Gateway #4
Port: 1 2 3 4 5 6 7 8 9 10
Private numbers: 601 – 610
Remote Office #2
BOSâNOVA FXS Gateway #2
Port: 1 2 3 4 5 6 7 8 9 10
Private numbers: 501 – 510
IP Network
PSTN
Private number prefix: 3 3 3 3 5 5 5 7
Port: 1 2 3 4 5 6 7 8
BOSâNOVA FXO Gateway
PBX
Extensions: 100 – 499
3 digits used for internal dialing
Largest private-number prefix
Headquarters

In the first example, three digits are used for internal dialing by the PBX. The largest assigned private-number prefix is 7. Seven (7) is a number with only one digit.

3 plus 1 equals 4, that is, the maximum private number length can be defined as small as 4. The full private-numbers of the FXS Gateways will be 4 digits, 4601 – 4610 and 2501 – 2510.

Figure 6: Second Example of Determining Correct Maximum Private Number Length



In the second example, based upon the sample IP Telephony network configuration, four digits are used for the internal extensions. The largest assigned private-number prefix is 6. Six (6) is a number with only one digit.

4 plus 1 equals 5, that is, the maximum private number length can be defined as small as 5. The full private-numbers of the FXS Gateways will be either 4 or 5 digits, depending on the decision of the administrator.

Dial Public Numbers and/or Terminate Hop-off Calls

The procedure for enabling dialing of public numbers begins on page 132. The procedure for enabling termination of hop-off calls begins on page 128.

The question **Dial public numbers** determines if users will be able to employ ***native dialing*** to dial, via a Gateway, to numbers o n the PSTN. We call that feature ***hop-off calls***. We call the ability to make hop-off calls as if dialing via the PSTN, native dialing.

*An IP Telephony network may be configured as a Virtual Private Network (VPN), that is, that **all calls are made using only private-numbers** even though some calls may be carried over the PSTN. Therefore, in the case of VPNs, clear the Dial public numbers checkbox.*

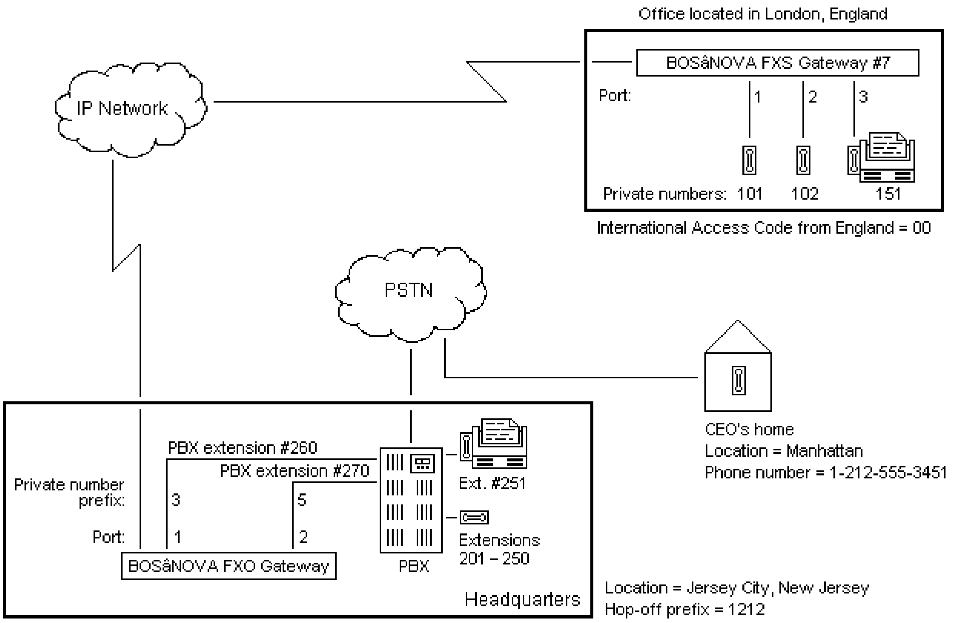
To allow use of public-numbers, the administrator must:

- enter E.164 information (see p. 83) in the Numbering Plan Wizard for both the originating and the terminating Gateway
- enter authorized hop-off prefixes and assign them per port

In the following example:

- the FXS Gateway is authorized to allow Dial Public Numbers
- the FXO Gateway is authorized to terminate Hop-off Calls with the hop-off prefix 1212.

To dial the CEO’s home from London, the user dials 00-1212-555-3451.



Automatic Dialing

The procedure for configuring automatic dialing begins on page 134. Automatic dialing is not relevant to PRI Gateways.

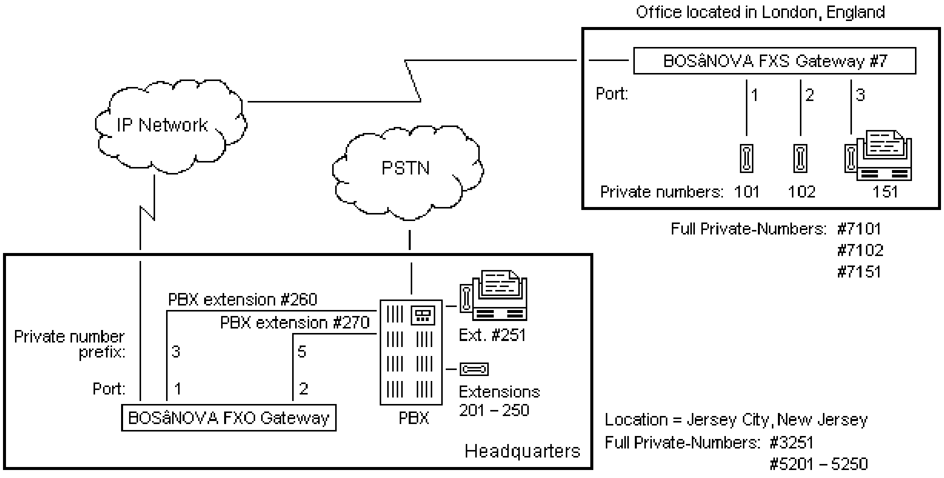
The administrator must decide if Automatic Dialing will be enabled. These numbers are dialed immediately when a port is activated, that is, when an FXO port detects a ring or when an FXS port detects off-hook.

With an FXS Gateway, this is synonymous with *hot-dialing*; all the user needs to do is lift the handset. With an FXO Gateway, the user dials the PBX extension number associated with a port of the Gateway and the Gateway dials the remainder of the number. Thus, this is a form of short-cut dialing.

Basic Example

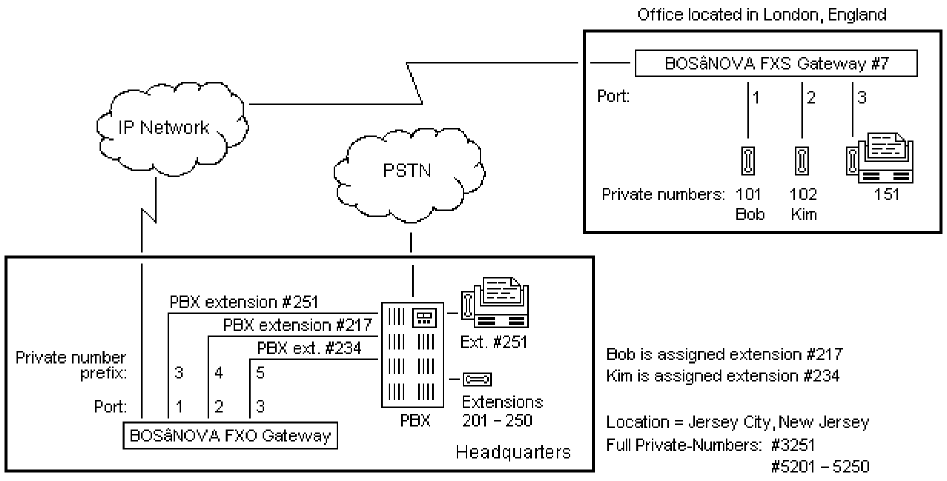
In the following example, the fax machines have been configured with autodialing.

- As soon as the fax machine in the London office is activated, the Gateway dials 3251, thereby creating a connection to the fax machine in the Jersey City headquarters.
- The fax machine at the headquarters, on the other hand, must dial PBX extension #260 associated with FXO port number 1. As soon as port number 1 is activated, the Gateway dials #7151, thereby creating a connection to the fax machine at the London office.



Remote PBX-Extension and Flash

This example illustrates an application of Automatic Dialing which results in a "virtual" or a remote PBX-extension.



In this example, Kim and Bob work in the office located in London, England. However, calls made by, and to, Kim and Bob are dialed ***as if*** they were working at the headquarters.

To accomplish this, the following must be configured:

- Port #3, connected to PBX extension #234, must be configured to automatically dial #7101. When a user at headquarters dials #234, the Gateway will automatically ring Bob's phone in London.
- Port #2, connected to PBX extension #217, must be configured to automatically dial #7102. When a user at headquarters dials #217, the Gateway will automatically ring Kim's phone in London.
- Kim and Bob's ports in London must be configured so that, as soon as they pick up the handset, the Gateway dials their private-number prefix, thereby connecting them to the PBX at the headquarters. Thus, Kim and Bob can dial three-digit extensions exactly as if they were sitting at desks at the headquarters.

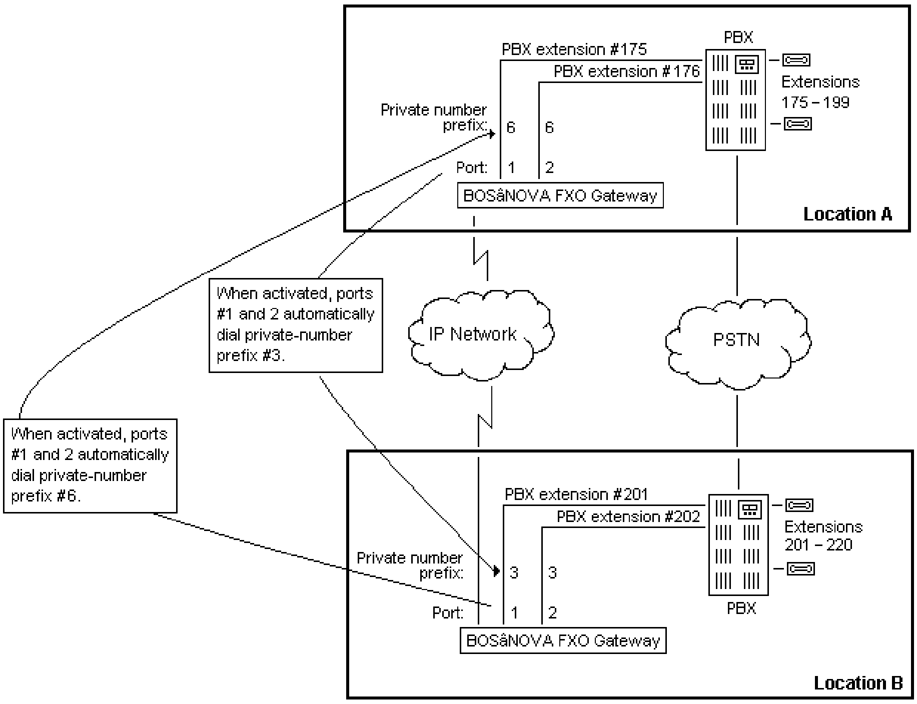
Furthermore, Kim and Bob, from the London Office, can exploit the PBX's flash feature. By momentarily depressing and releasing the handset switch, Kim or Bob will disconnect from their current call and then, via the already existing IP connection, receive a new dial-tone from the PBX. They can then use PBX features such as conference call or call transfer.

The flash is detected by the FXS and transmitted to the FXO which generates the flash to the PBX extension.

Back-to-Back Automatic Dialing

Back-to-back automatic dialing is a configuration that can be used with a small IP Telephony network. It simplifies the dialing process but limits the overall flexibility of the network. In a small network, the constraint is not apparent.

The following example illustrates a back-to-back configuration.



In this example, any user in location A who dials extensions #175 or #176 will be connected to the PBX at location B. A user at location B who dials extension #201 or #202 will be connected to the PBX at location A.

To accomplish this, the following must be configured:

- Ports #1 and 2 at location A, connected to PBX extensions #175 and 176, must be configured to automatically dial #3. The user will dial #175 or 176 and then the extension number at location B.
- Ports #1 and 2, connected to PBX extensions #201 and 202, must be configured to automatically dial #6. The user will dial #201 or 202 and then the extension number at location A.

Automatic Dialing and Hop-off

In the following example, line #1 in the London office can be configured to "hot-dial" the home of the CEO in Manhattan. The international portion of the call will be over IP.

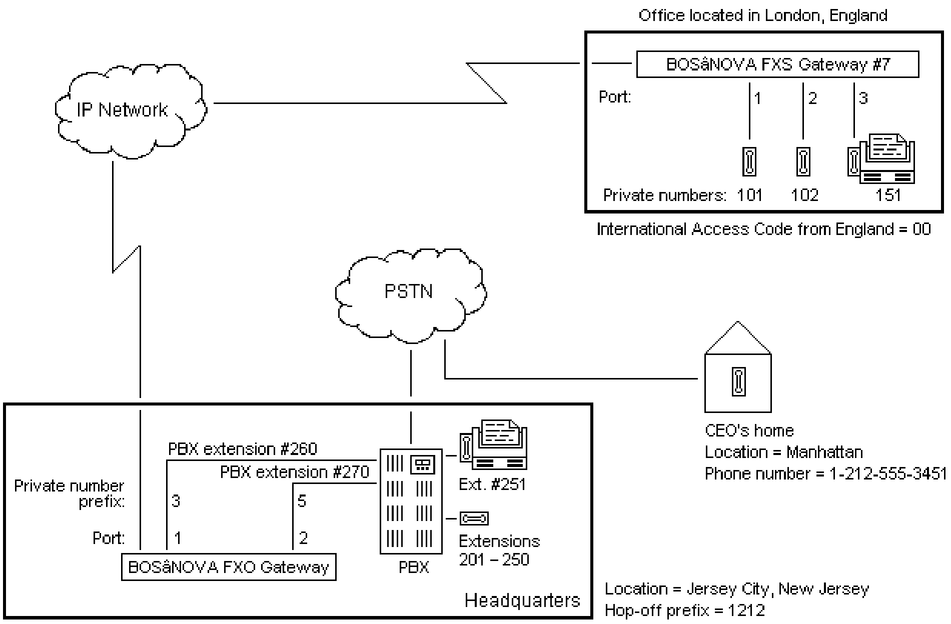
The following must be configured:

- The Gateway in the London office must be configured to allow dialing of public numbers (see p. 132).
- Port #1 of the London Gateway must be configured to automatically dial the number of the CEO's home in Manhattan (see p. 134).

The administrator will enter the complete public number, including the International Access Code, as if the user were dialing via the PSTN. Thus, the number entered will be 00-1-212-555-3451.

- One or more ports of the Gateway in Jersey City must be configured both to allow hop-off calls, and with a hop-off prefix matching the telephone number at the CEO's home (see p. 128).

If all of this is done, as soon as the handset of the phone attached to line #1 in London is lifted, a connection will be made, via the Jersey City Gateway, with the phone at the CEO's home.



The Officer Gateway

The procedure for selecting an Officer begins on page 218.

The administrator must decide which Gateway will serve as the Officer. For an explanation of Officer responsibilities, see p. 85.

When determining which Gateway should be selected as Officer, consider:

- The quality of the Internet conditions.
  The Gateway with the best Internet connection should be the Officer.
- The condition of the power supply.
  The Officer should be protected by a surge protector, a voltage regulator, and an Uninterruptible Power Supply (UPS).

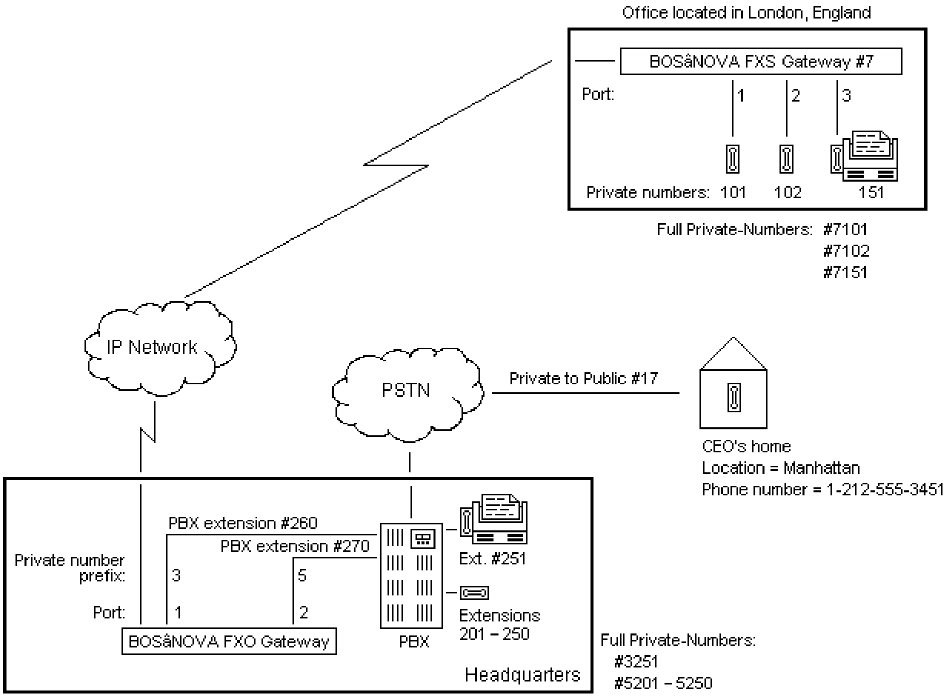
Private to Public Number Associations

The procedure for assigning private-to-public number associations begins on page 172.

The administrator must decide if users will be able to access public numbers using private numbers.

Private to public numbers associations are short numbers that, when dialed, connect a user to a number on the PSTN. Essentially, this is another form of short-cut dialing.

In the following example, the private number 17 has been associated with the public number 1-212-555-3451. From anywhere on the IP Telephony network, dialing 17 will connect to the CEO's home.



The procedure for defining Public number blocks begins on page 196.
The procedure for defining Private-number blocks begins on page 136.
The procedure for configuring IP Bypass numbers begins on page 196.

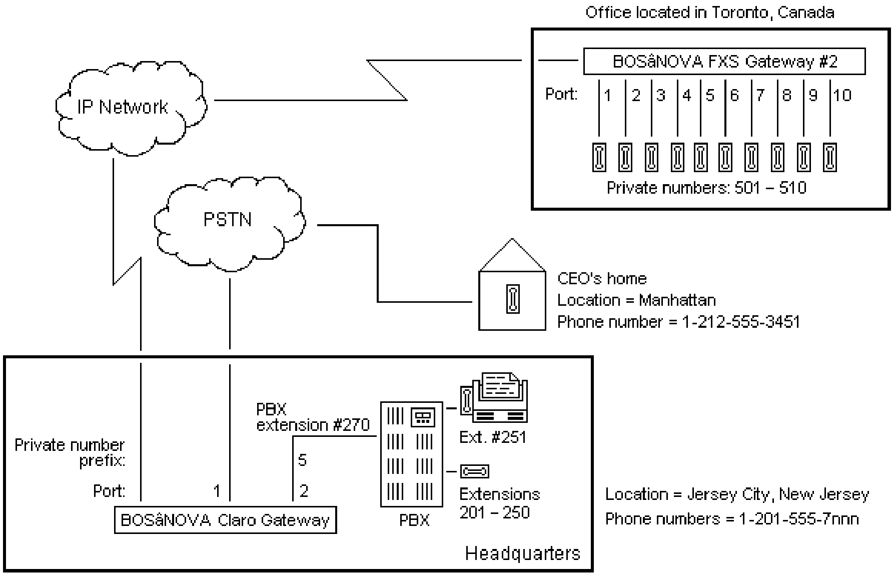
When an IP Telephony network includes Claro Gateways, the administrator must define one or more block of Public numbers. In addition, the administrator has the option to:

- allow users to use Private numbers
- associate a block of Private numbers with the block of Public numbers
- restrict outgoing calls to either the PSTN or the IP

Background

Claro Gateways are different because they are located between the PBX and ***both*** the PSTN and the Internet. In contrast, other Gateways are located between the PBX or the telephony equipment and ***only*** the connection to the Internet. Claro Gateways evaluate each call and, based upon various factors, determine whether the call should be forwarded to the IP or to the PSTN.

In the following diagram, notice that there is no line from the PBX to the PSTN. Rather, it is the Claro PRI Gateway that is connected to the PSTN.



Because of their location between the PBX and the PSTN, all Claro Gateways must accept Public numbers. The option is whether or not they can accept Private numbers, for example, a PBX extension.

Claro Analog and Port Grouping

The administrator must assign each port of a Claro Analog Gateway to a group. The choice of groups includes either a group with Claro functionality or a group with FXO/FXS functionality. Subsequent changes made to a group affect all ports belonging to that group.

The Numbering Plan Wizard displays the pages relevant to the grouping:

- If all ports are assigned Claro functionality, the Numbering Plan Wizard automatically skips the pages that are associated with FXO and FXS Gateways.
- If all ports are assigned FXO/FXS functionality, the Numbering Plan Wizard automatically skips the Group information page.
- If the grouping includes a mixture of both Claro functionality and FXO/FXS functionality, all the pages of the Numbering Plan Wizard are displayed.

The procedure for configuring Port Grouping begins on page 114.

Claro PRI and Public Number Blocks

The administrator must define one or more block of numbers that the Claro PRI accepts. A block of numbers is a set of consecutive numbers and is represented by the first number of, and the size of, the set.

In the case of a Claro Analog, the size of a block is always 1. Therefore, blocks are not defined in a Claro Analog Gateway.

In the preceding example, the Jersey City PBX supports a block of extensions from 201 to 251. Claro has to be configured to accept the same block. The administrator would enter for first Public number 5557201 and for Block Size he would enter 51.

Private Numbers and Associated Private Number Blocks

Claro PRI Gateways can be configured to accept Private numbers.

If the Claro is configured to accept Private numbers, the administrator also has the option of associating a block of Private numbers with the block of Public numbers. For example, instead of requiring that a user dial 2015557201 and so on, the administrator can associate a block of Private numbers starting with 201 and with Block Size of 51. Then, dialing only the Private number 201 would connect the user to the Public number 2015557201.

IP Bypass Numbers

The administrator can configure all Claro Gateways to direct specific phone numbers to the PSTN without allowing Claro to evaluate the number. Phone numbers listed in the IP Bypass tables are dialed directly to the PSTN. The Gateway does not attempt to place these calls as IP calls.

For example, police, fire department, and other emergency numbers should be configured to be dialed directly to the PSTN. Toll free numbers might also be dialed directly to the PSTN.

Claro can also be configured to direct to the PSTN ***all*** calls originating from a specific phone number. This feature is called Caller ID and is configured as part of IP Bypass.

The procedure for configuring IP Bypass numbers begins on page 196.

Force Dialout Direction

The administrator can configure all Claro Gateways to allow a user to limit the call direction of outgoing calls, ***per call***, to either the PSTN or the IP. The administrator assigns a prefix to both "PSTN only calls" and "IP only" calls. The user dials the prefix before dialing the phone number and thereby restricts the outgoing call to either the PSTN or the IP.

The procedure for configuring Force Dialout Direction begins on page 142.

IP Telephony...
Clear and Simple

SECTION 8:
NUMBERING PLAN WIZARD

This section details the procedures involved in configuring a Numbering Plan and displays the corresponding Numbering Plan Configurator tables.

Numbering Plan configuration is completed:

- 85% in the Numbering Plan Wizard, pages 108–142
- 10% in the Numbering Plan Configurator, pages 156–196
- Assigning an Officer in the Dialing Server, see page 218

*Following the initial setup, access to the Numbering Plan Wizard is **only** via the Numbering Plan Configurator.*

An overview of the BOSâNOVA Gateways Numbering Plan and in-depth explanations of each aspect of the numbering plan are provided in the section “Numbering Plan Overview” beginning on page 80.

*Before beginning, we recommend that, at the very least, you read **Basics of Configuration** on page 88.*

GUIDE TO THE PAGES OF THE NUMBERING PLAN WIZARD

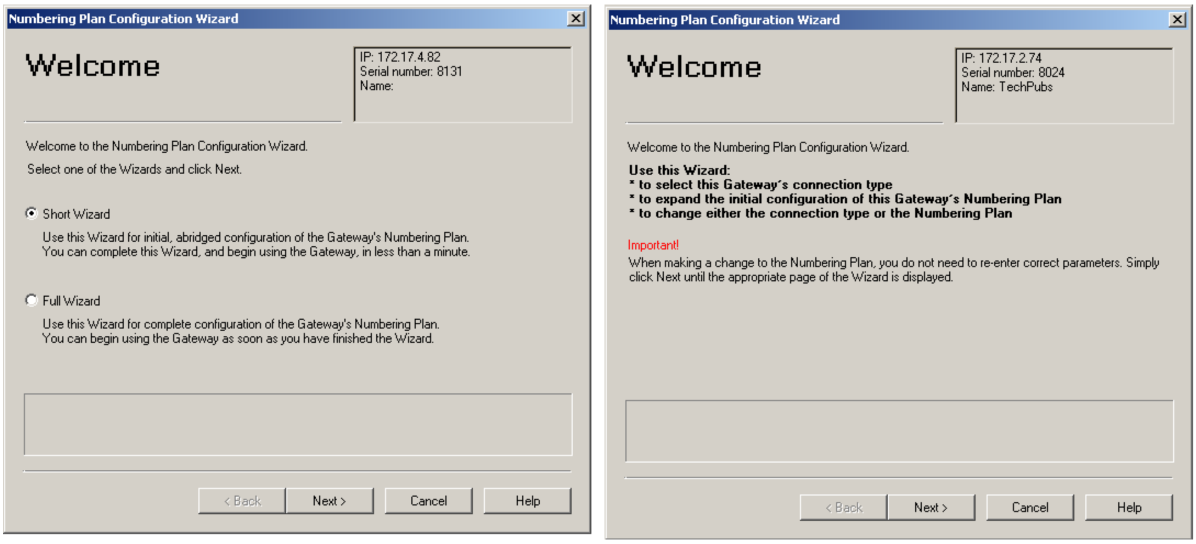
This table lists all the pages of the Numbering Plan Wizard ***potentially*** available. The pages actually displayed depend upon the Gateway type and Connection type. Click a page number to jump to the relevant topic.

Table 40: Guide to the Pages of the Numbering Plan Wizard

Subtitles of Pages of the Numbering Plan Wizard	see page #	Gateway Type				
		FXS	FXO	PRI	Claro PRI	Claro Analog
Welcome	109	✓	✓	✓	✓	✓
Descriptive name	111	✓	✓	✓	✓	✓
Connection type	112	✓	✓	✓	✓	✓
If Gatekeeper is selected as the Connection type, the Gatekeeper Parameters and Registration Parameters pages of the Wizard are displayed.						
Preferred protocol	113	✓	✓	✓	✓	✓
Port grouping	114					✓
Group information	116					✓
Phone number blocks	136				✓	
Termination of Hop-off	128				✓	
Port information	119	✓	✓	✓		✓
Phone numbers per port	139					✓
Private phone numbers	122	✓				
Private number prefixes	125	✓	✓	✓		
Hop-off prefixes	128		✓	✓	✓	✓
Hop-off prefixes for ports	129		✓	✓		✓
Access code	129		✓	✓		
Local PSTN parameters	130	✓	✓	✓	✓	✓
Dial public numbers?	132	✓	✓	✓		
Accept automatic dialing?	134	✓	✓			
Auto-dialing table	135	✓	✓			
Force dialout direction	142				✓	✓
Review configuration	143	✓	✓	✓	✓	✓

THE WELCOME PAGE

The first page of the Numbering Plan Wizard is a Welcome page. Depending upon the status of the Gateway’s numbering plan configuration, either the initial-configuration or reconfiguration Welcome page will be displayed.



Numbering Plan Configuration Wizard

Welcome

IP: 172.17.4.82
Serial number: 8131
Name:

Welcome to the Numbering Plan Configuration Wizard.

Select one of the Wizards and click Next.

● Short Wizard

Use this Wizard for initial, abridged configuration of the Gateway's Numbering Plan.
You can complete this Wizard, and begin using the Gateway, in less than a minute.

○ Full Wizard

Use this Wizard for complete configuration of the Gateway's Numbering Plan.
You can begin using the Gateway as soon as you have finished the Wizard.

Numbering Plan Configuration Wizard

Welcome

IP: 172.17.2.74
Serial number: 8024
Name: TechPubs

Welcome to the Numbering Plan Configuration Wizard.

Use this Wizard:
*** to select this Gateway's connection type**
*** to expand the initial configuration of this Gateway's Numbering Plan**
*** to change either the connection type or the Numbering Plan**

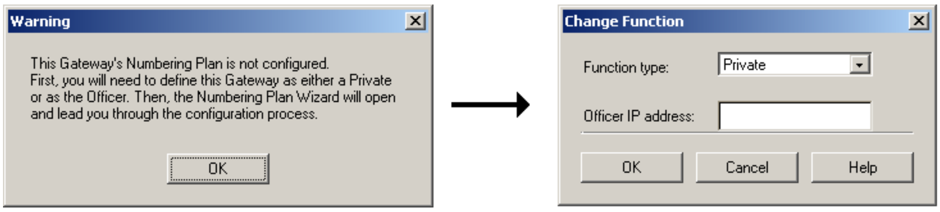
Important!
When making a change to the Numbering Plan, you do not need to re-enter correct parameters. Simply click Next until the appropriate page of the Wizard is displayed.

Figure 7: The Initial-Configuration and Reconfiguration Welcome pages

Initial Numbering Plan Configuration

If the Gateway’s numbering plan is not configured, initial configuration proceeds as follows:

1. From the Gateway Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Local Parameters**.
3. Click **Change**. The following sequence of screens is displayed.



Warning

This Gateway's Numbering Plan is not configured.
First, you will need to define this Gateway as either a Private or as the Officer. Then, the Numbering Plan Wizard will open and lead you through the configuration process.

Change Function

Function type: Private

Officer IP address:

4. Click **OK** on the message. The Change Function dialog box is displayed.

5. Enter the BOSâNOVA IP Telephony network's Officer Gateway's IP address. See "Using the Officer Gateway" on page 203 for information about the Officer Gateway.

6. Click **OK**. The pre-configuration Welcome screen is displayed. There are two possibilities:

   - Short Wizard:
     Use the Short Wizard to name the Gateway, assign a phone number to one or more port, and register the new Private Gateway with the Officer. This gets the Gateway "up and running" though the configuration may be incomplete.
   - Full Wizard:
     The Full Wizard provides access to all the pages relevant to the specific Gateway.

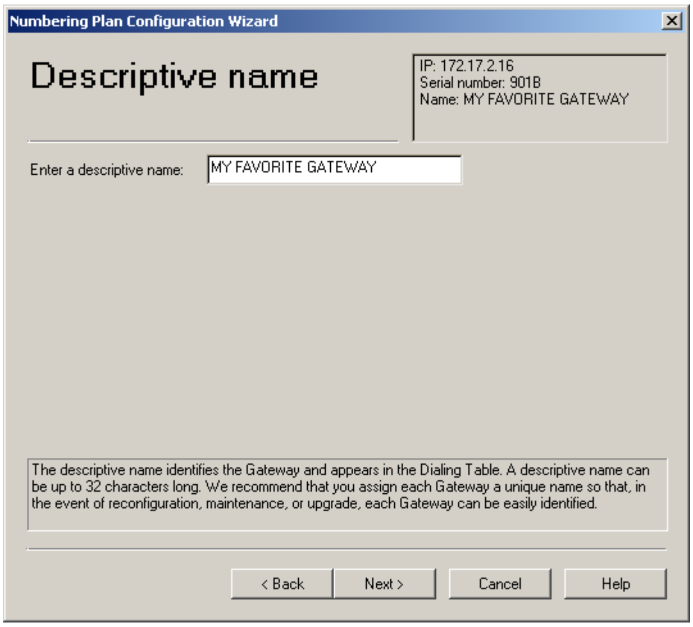
Reconfiguring the Numbering Plan

Reconfiguration of a Gateway's numbering plan proceeds as follows:

1. From the Gateway Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Local Parameters**.
3. Click **Change**. The reconfiguration Welcome page of the **Numbering Plan Wizard** opens. There are no options.

ASSIGNING A DESCRIPTIVE NAME

The second page of the Numbering Plan Wizard requests that you assign a descriptive name to the Gateway.

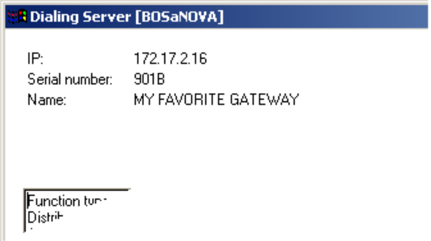


IP: 172.17.2.16
Serial number: 901B
Name: MY FAVORITE GATEWAY

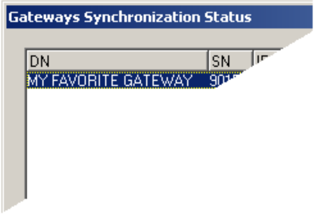
Enter a descriptive name: MY FAVORITE GATEWAY

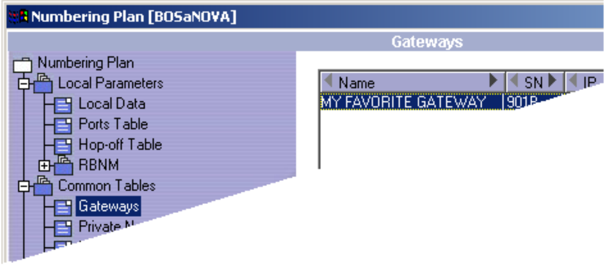
The descriptive name identifies the Gateway and appears in the Dialing Table. A descriptive name can be up to 32 characters long. We recommend that you assign each Gateway a unique name so that, in the event of reconfiguration, maintenance, or upgrade, each Gateway can be easily identified.

Assign a name that will assist with identification. Subsequently, the descriptive name appears in many locations, for example:



IP: 172.17.2.16
Serial number: 901B
Name: MY FAVORITE GATEWAY

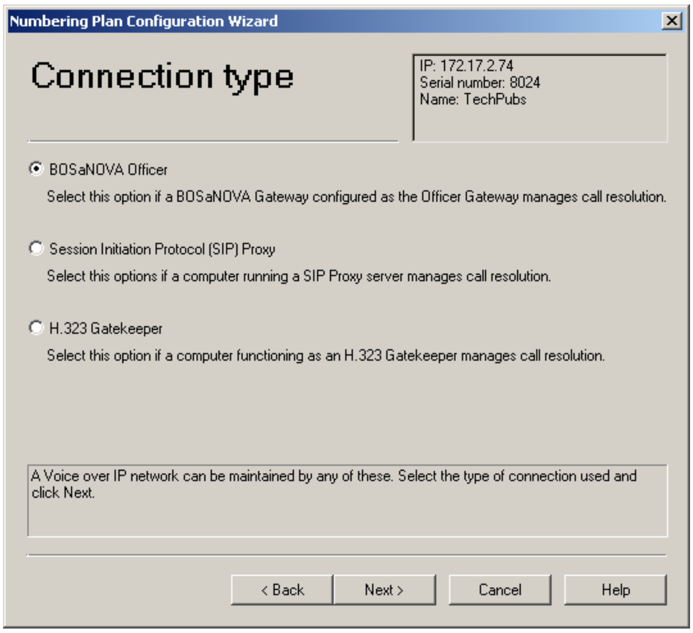




CONNECTION TYPE

The third page of the Numbering Plan Wizard requests that you select a Connection Type for this Gateway.

For explanations of the different Connection Type, and procedures related to configuring each of the Connection Types, see the following section beginning on page 145.



Connection type

IP: 172.17.2.74
Serial number: 8024
Name: TechPubs

● BOSaNOVA Officer

Select this option if a BOSaNOVA Gateway configured as the Officer Gateway manages call resolution.

○ Session Initiation Protocol (SIP) Proxy

Select this options if a computer running a SIP Proxy server manages call resolution.

○ H.323 Gatekeeper

Select this option if a computer functioning as an H.323 Gatekeeper manages call resolution.

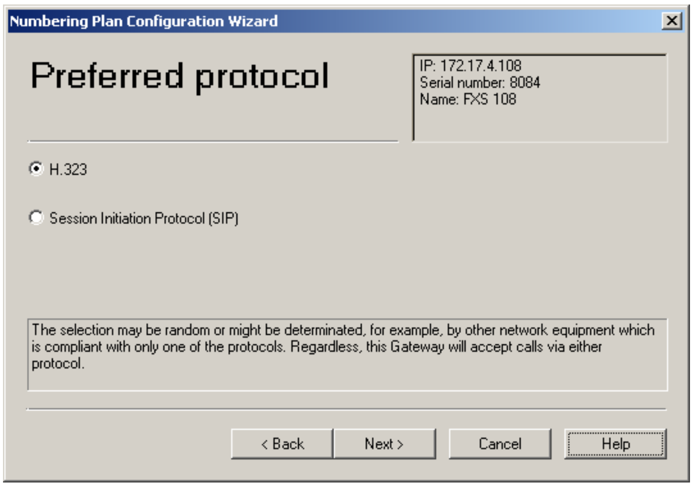
A Voice over IP network can be maintained by any of these. Select the type of connection used and click Next.

SELECTING H.323 OR SIP

This page of the Numbering Plan Wizard appears only if BOSâNOVA Officer Gateway is selected as the connection type.

BOSâNOVA Gateways work with both SIP and H.323 simultaneously. In other words, the Gateways are always ready to receive either an SIP or an H.323 call. The Gateway chooses the protocol for an outgoing call according to flag “Preferred protocol” that is set in the destination Gateway configuration or the same flag that is set for third-party gateway in the Officer configuration.

The selection of a protocol, therefore, might be random and the IP Telephony network will not suffer. However, as described below, the System Administrator might choose the protocol based on other reasons, in particular, other network equipment which is compliant with, or configured only for, one of the protocols.



Numbering Plan Configuration Wizard

Preferred protocol

IP: 172.17.4.108
Serial number: 8084
Name: FXS 108

● H.323

○ Session Initiation Protocol (SIP)

The selection may be random or might be determinated, for example, by other network equipment which is compliant with only one of the protocols. Regardless, this Gateway will accept calls via either protocol.

Session Initiation Protocol (SIP) is a standard introduced by the Internet Engineering Task Force (IETF) in 1999 to carry voice over IP. Since it was created by the IETF, it approaches voice and multimedia from the Internet, or IP, perspective.

H.323 emerged around 1996. As an International Telecommunication Union standard, H.323 was designed from a telecommunications perspective. Both standards have the same objective, that is, to enable voice and multimedia convergence with IP protocols.

The older H.323 standard has the advantage of having been implemented first. However, SIP more easily allows applications to be developed and has been gaining in popularity.

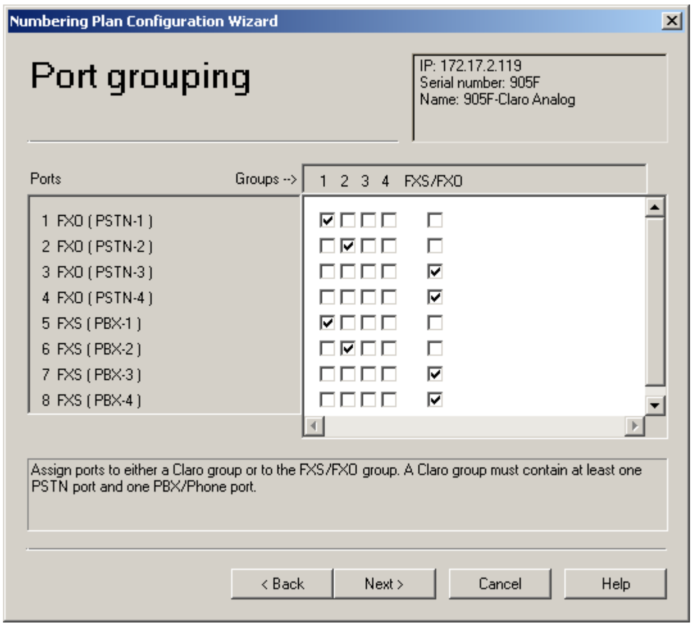
DEFINING CLARO ANALOG PORT GROUPING

Port grouping is defined in the Numbering Plan Wizard. For an explanation of Port grouping, see page 105.

This page is only relevant to Claro Analog Gateways and ROBO units.

Procedure

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Local Parameters**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the **Port Grouping** page.



Numbering Plan Configuration Wizard

Port grouping

IP: 172.17.2.119
Serial number: 905F
Name: 905F-Claro Analog

Ports	1	2	3	4	FXS/FXO
1 FXO (PSTN-1)	☑	□	□	□	□
2 FXO (PSTN-2)	□	☑	□	□	□
3 FXO (PSTN-3)	□	□	□	□	☑
4 FXO (PSTN-4)	□	□	□	□	☑
5 FXS (PBX-1)	☑	□	□	□	□
6 FXS (PBX-2)	□	☑	□	□	□
7 FXS (PBX-3)	□	□	□	□	☑
8 FXS (PBX-4)	□	□	□	□	☑

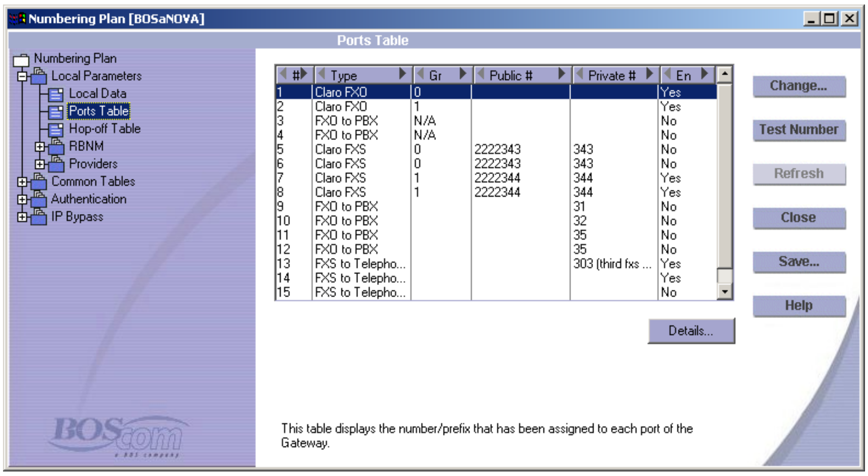
Assign ports to either a Claro group or to the FXS/FXO group. A Claro group must contain at least one PSTN port and one PBX/Phone port.

5. For each port, there are two possibilities:
   - To assign a port to a group and maintain the Claro functionality, select the group number.
   - To convert the port to FXS/FXO functionality, select the FXS/FXO checkbox.
6. Click **Next**. The Numbering Plan Wizard automatically displays the pages associated with the groups that have been assigned.

Associated Tables

Following configuration, port grouping information will appear in this table:

Local Parameters



#	Type	Gr	Public #	Private #	En
1	Claro FXO	0			Yes
2	Claro FXO	1			Yes
3	FXO to PBX	N/A			No
4	FXO to PBX	N/A			No
5	Claro FXS	0	2222343	343	No
6	Claro FXS	0	2222343	343	No
7	Claro FXS	1	2222344	344	Yes
8	Claro FXS	1	2222344	344	Yes
9	FXO to PBX			31	No
10	FXO to PBX			32	No
11	FXO to PBX			35	No
12	FXO to PBX			35	No
13	FXS to Telepho...			303 (third fxs ...	Yes
14	FXS to Telepho...				Yes
15	FXS to Telepho...				No

This table displays the number/prefix that has been assigned to each port of the Gateway.

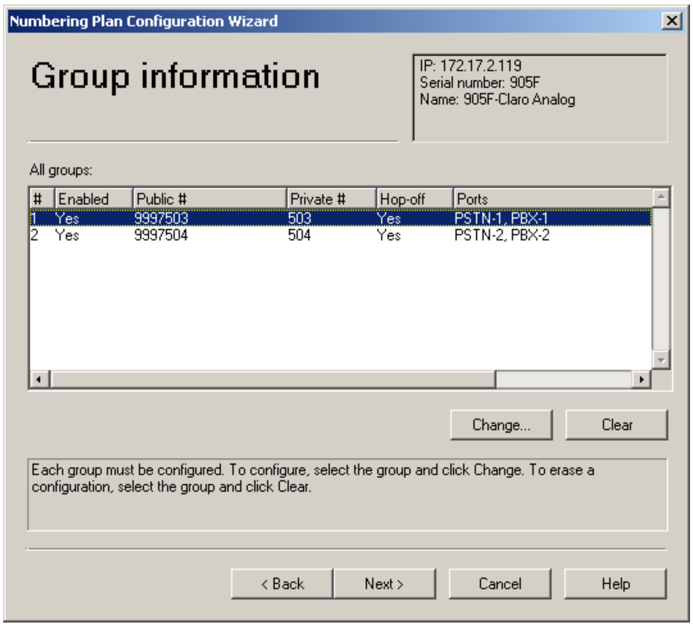
ENTERING CLARO ANALOG GROUP INFORMATION

Group information is defined in the Numbering Plan Wizard. For an explanation of Group information, see page 105.

This page is only relevant to Claro Analog Gateways and ROBO units.

Procedure

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Local Parameters**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the **Group information** page.



Group information

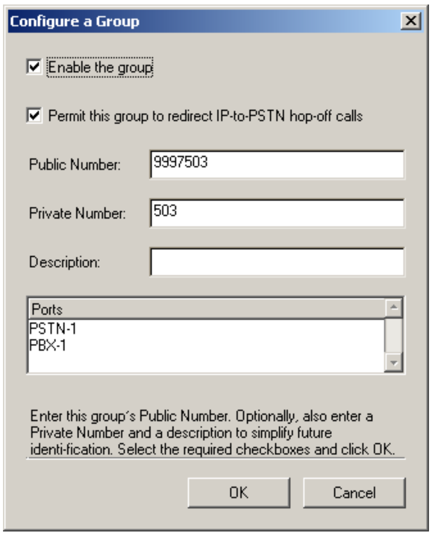
IP: 172.17.2.119
Serial number: 905F
Name: 905F-Claro Analog

All groups:

#	Enabled	Public #	Private #	Hop-off	Ports
1	Yes	9997503	503	Yes	PSTN-1, PBX-1
2	Yes	9997504	504	Yes	PSTN-2, PBX-2

Each group must be configured. To configure, select the group and click Change. To erase a configuration, select the group and click Clear.

5. Click **Change**. The Configure a Group dialog box is displayed.



Configure a Group

☑ Enable the group

☑ Permit this group to redirect IP-to-PSTN hop-off calls

Public Number: 9997503

Private Number: 503

Description:

Ports
PSTN-1
PBX-1

Enter this group's Public Number. Optionally, also enter a Private Number and a description to simplify future identi-fication. Select the required checkboxes and click OK.

6. Configure the group of ports:

   a. Select the first checkbox to enable the group.

   b. Select the second checkbox to enable each port within the group to redirect calls from the Internet to the PSTN.

   c. Enter the groups Public Number.

   d. Enter the groups Private Number.

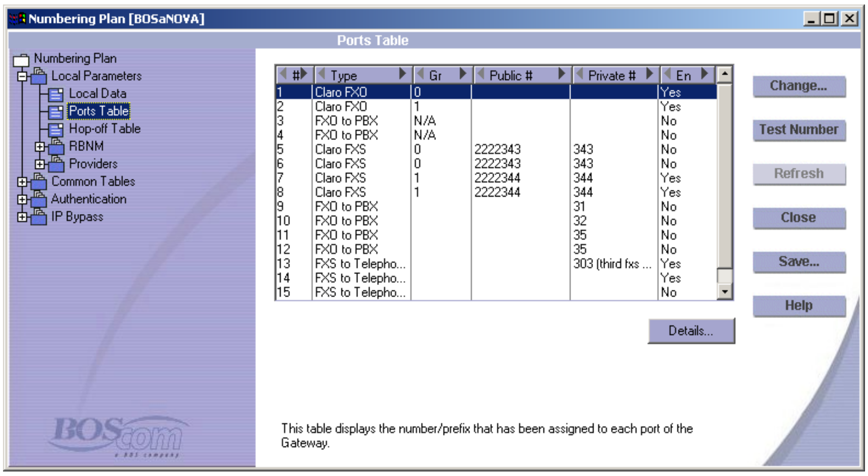
   e. Enter a group descriptive name that will assist with identification. Subsequently, the descriptive name appears in many locations

7. Click **OK**.

Associated Tables

Following configuration, group information will appear in this table:

Local Parameters



#	Type	Gr	Public #	Private #	En
1	Claro FXO	0			Yes
2	Claro FXO	1			Yes
3	FXO to PBX	N/A			No
4	FXO to PBX	N/A			No
5	Claro FXS	0	2222343	343	No
6	Claro FXS	0	2222343	343	No
7	Claro FXS	1	2222344	344	Yes
8	Claro FXS	1	2222344	344	Yes
9	FXO to PBX			31	No
10	FXO to PBX			32	No
11	FXO to PBX			35	No
12	FXO to PBX			35	No
13	FXS to Telepho...			303 (third fxs ...	Yes
14	FXS to Telepho...				Yes
15	FXS to Telepho...				No

This table displays the number/prefix that has been assigned to each port of the Gateway.

ASSIGNING PORT INFORMATION

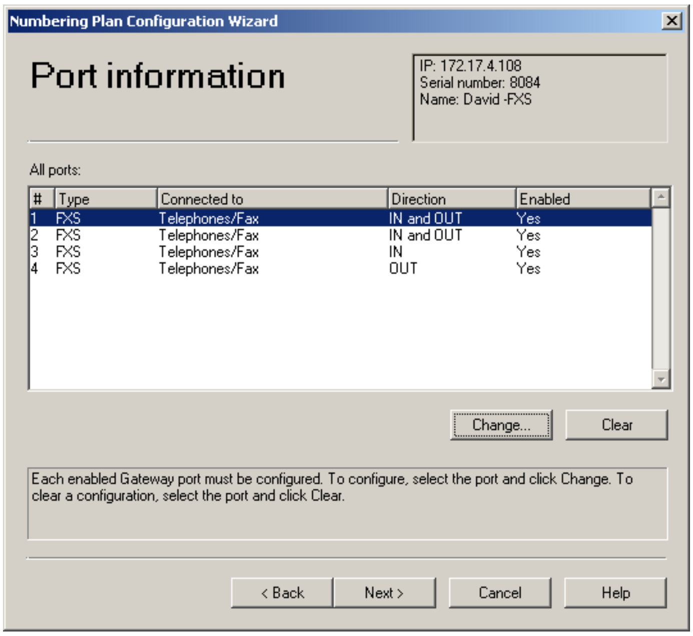
Port information is assigned in the Numbering Plan Wizard.

Port information is assigned for every active port of every Gateway except for the Claro PRI.

The information entered, and the number of columns displayed, varies according to Gateway type and per configuration.

Procedure

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Local Parameters**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the **Port information** page.



Numbering Plan Configuration Wizard

Port information

IP: 172.17.4.108
Serial number: 8084
Name: David -FXS

All ports:

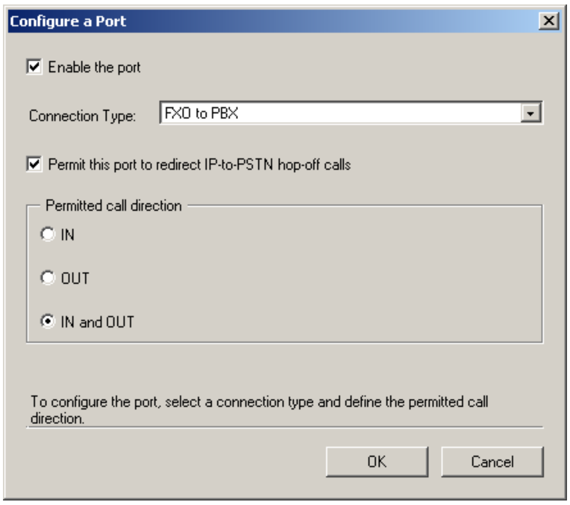
#	Type	Connected to	Direction	Enabled
1	FXS	Telephones/Fax	IN and OUT	Yes
2	FXS	Telephones/Fax	IN and OUT	Yes
3	FXS	Telephones/Fax	IN	Yes
4	FXS	Telephones/Fax	OUT	Yes

Each enabled Gateway port must be configured. To configure, select the port and click Change. To clear a configuration, select the port and click Clear.

Define information for each port before continuing to the next page.

5. Select a port. The row changes color when selected.

6. Click **Change**. The **Configure a Port** dialog box opens.



Configure a Port

☑ Enable the port

Connection Type: FXO to PBX

☑ Permit this port to redirect IP-to-PSTN hop-off calls

Permitted call direction

○ IN

○ OUT

● IN and OUT

To configure the port, select a connection type and define the permitted call direction.

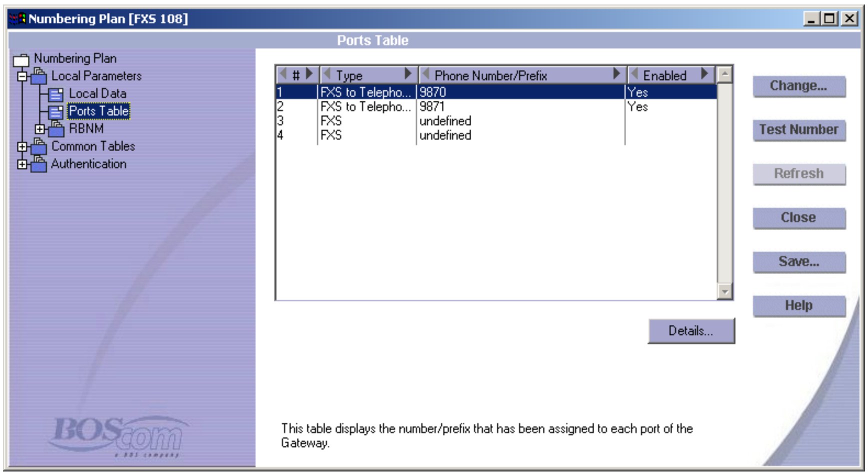
In an FXS Gateway, and when SIP Proxy is selected as the Connection Type, the "Permit this port to redirect IP to PSTN hop-off calls" checkbox does not appear.

7. Select **Enable the port**.
8. Select a **Connection type**.
9. For an FXO port connected to the PBX, decide whether or not to select **Permit this port to redirect IP to PSTN hop-off calls**.
10. Select a call direction and click OK. The **Configure a Port** dialog box closes.
11. Repeat steps 5–10 for each active port.
12. Click **Next** to open the next page of the Wizard.

Associated Tables

Following configuration, port information will appear in these tables:

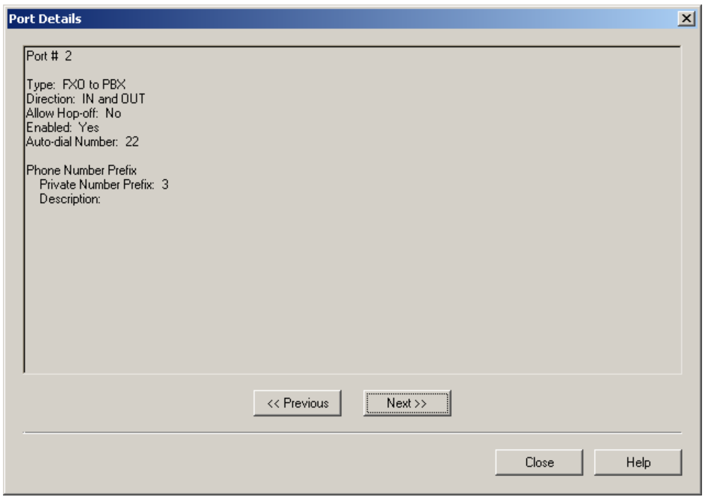
Local Parameters



#	Type	Phone Number/Prefix	Enabled
1	FXS to Telepho...	9870	Yes
2	FXS to Telepho...	9871	Yes
3	FXS	undefined	
4	FXS	undefined	

This table displays the number/prefix that has been assigned to each port of the Gateway.

Click **Details** to see a complete report of port information:



Port # 2

Type: FXO to PBX
Direction: IN and OUT
Allow Hop-off: No
Enabled: Yes
Auto-dial Number: 22

Phone Number Prefix
Private Number Prefix: 3
Description:

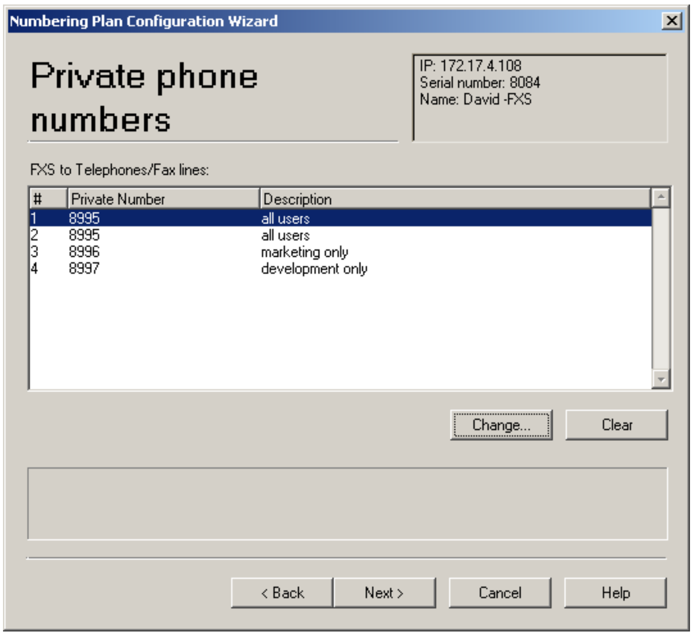
ASSIGNING PRIVATE-NUMBERS

Private-numbers are assigned in the Numbering Plan Wizard. For an explanation of private-numbers, see p. 91.

Private-numbers are assigned for FXS ports connected to telephony equipment, not for ports of a PRI or FXO Gateway.

Procedure

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Local Parameters**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the **Private phone numbers** page. (This assumes that Port information, discussed on page 119, is defined.)



Private phone numbers

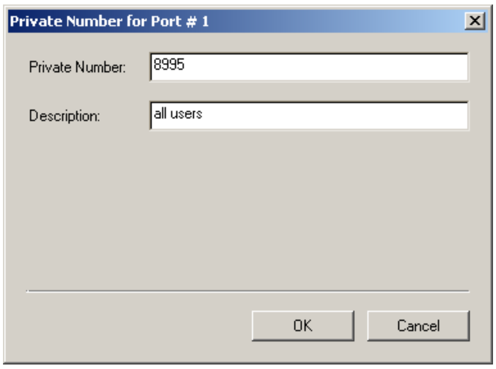
IP: 172.17.4.108
Serial number: 8084
Name: David -FXS

FXS to Telephones/Fax lines:

#	Private Number	Description
1	8995	all users
2	8995	all users
3	8996	marketing only
4	8997	development only

5. Select a port. The row changes color when selected.

6. Click **Change**. The Private Number for Port dialog box opens.



Private Number for Port # 1

Private Number: 8995

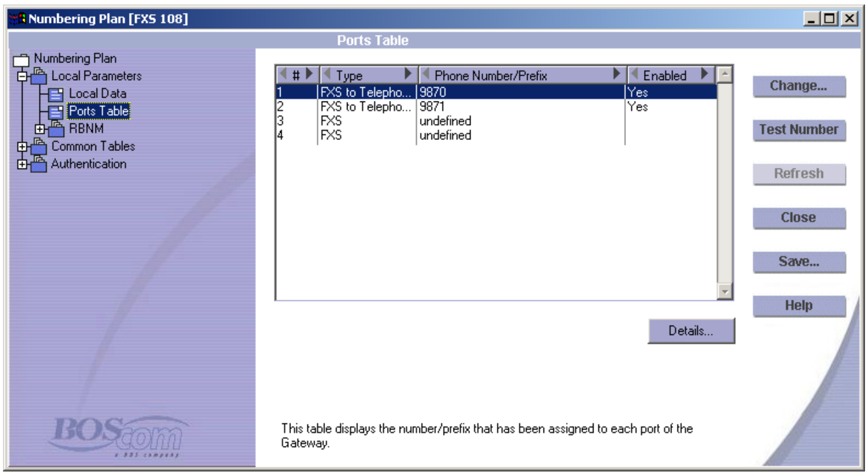
Description: all users

7. Enter the private-number and a description. The description is intended to make later identification easier.
8. Click **OK**.
9. Repeat steps 5 – 8 until all private-numbers are configured.
10. Complete the Wizard.

Associated Tables

Following configuration, private-numbers will appear in these tables:

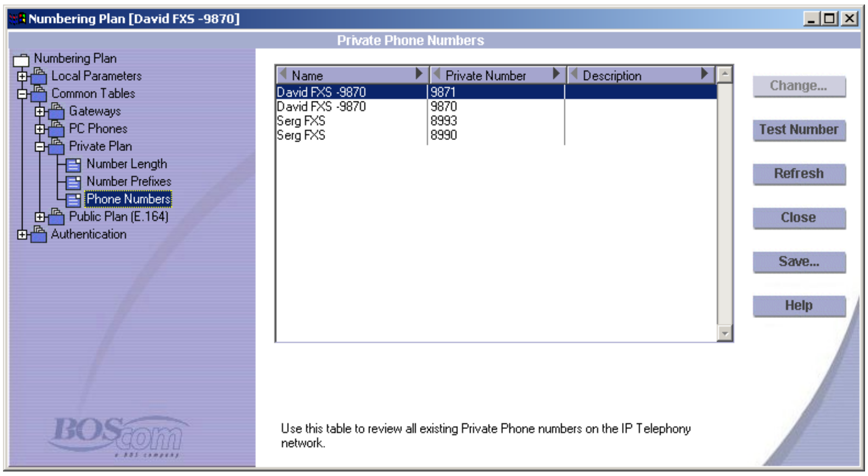
Local Parameters



#	Type	Phone Number/Prefix	Enabled
1	FXS to Telepho...	9870	Yes
2	FXS to Telepho...	9871	Yes
3	FXS	undefined	
4	FXS	undefined	

This table displays the number/prefix that has been assigned to each port of the Gateway.

Common Tables



Name	Private Number	Description
David FXS -9870	9871	
David FXS -9870	9870	
Serg FXS	8993	
Serg FXS	8990	

Use this table to review all existing Private Phone numbers on the IP Telephony network.

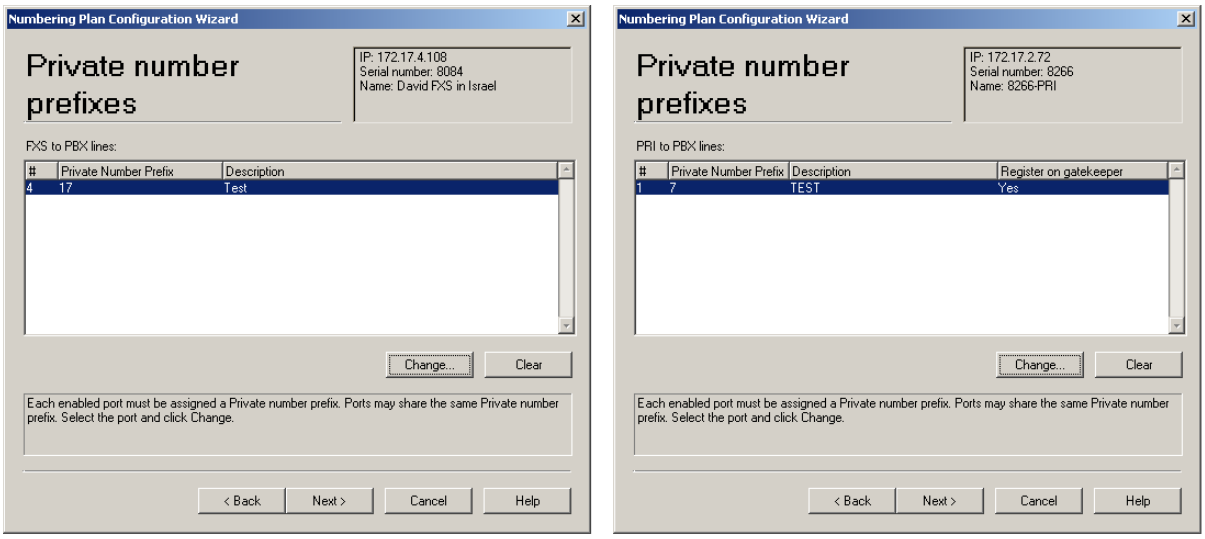
ASSIGNING PRIVATE-NUMBER PREFIXES

Private-number prefixes are assigned in the Numbering Plan Wizard. For an explanation of private-number prefixes, see page 91.

Private-number prefixes are assigned for PRI and FXO Gateways. Also, when an FXS port is connected to a PBX, a private-number prefix is assigned.

Procedure

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Local Parameters**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the **Private-number prefixes** page. (This assumes that Port information, discussed on page 119, is defined.)



Numbering Plan Configuration Wizard

Private number prefixes

IP: 172.17.4.108
Serial number: 8084
Name: David FXS in Israel

FXS to PBX lines:

#	Private Number Prefix	Description
4	17	Test

Each enabled port must be assigned a Private number prefix. Ports may share the same Private number prefix. Select the port and click Change.

Numbering Plan Configuration Wizard

Private number prefixes

IP: 172.17.2.72
Serial number: 8266
Name: 8266-PRI

PRI to PBX lines:

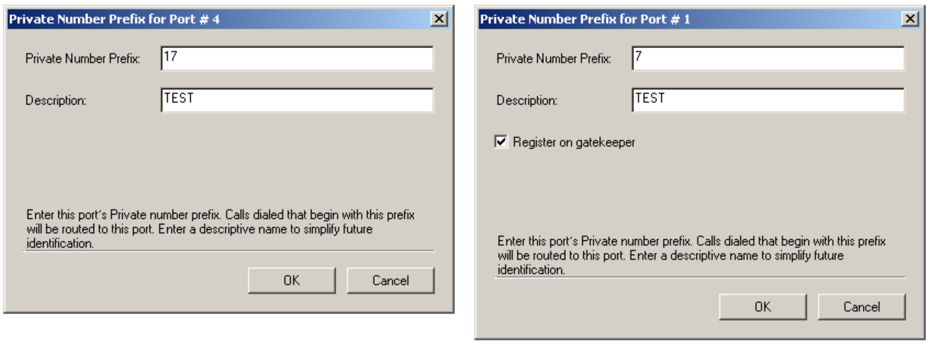
#	Private Number Prefix	Description	Register on gatekeeper
1	7	TEST	Yes

Each enabled port must be assigned a Private number prefix. Ports may share the same Private number prefix. Select the port and click Change.

Comparison of appearance in a Gateway using the BOSâNOVA Numbering Plan for call resolution as opposed to a Gateway using a gatekeeper.

When a Gateway is configured to work with a Gatekeeper, the Numbering Plan Wizard Private number prefixes page includes the Register on Gatekeeper option. When selected, the Private number prefix is sent to the Gatekeeper as an E.164 alias, that is, as a registration parameter. The Gatekeeper keeps track of these prefixes and directs matching calls to this Gateway. See also: "Configuring Gatekeeper as the Connection Type" on page 147.

5. Select a port. The row changes color when selected.
6. Click **Change**. The Private Number Prefix dialog box opens.



Private Number Prefix for Port # 4

Private Number Prefix: 17

Description: TEST

Enter this port's Private number prefix. Calls dialed that begin with this prefix will be routed to this port. Enter a descriptive name to simplify future identification.

Private Number Prefix for Port # 1

Private Number Prefix: 7

Description: TEST

☑ Register on gatekeeper

Enter this port's Private number prefix. Calls dialed that begin with this prefix will be routed to this port. Enter a descriptive name to simplify future identification.

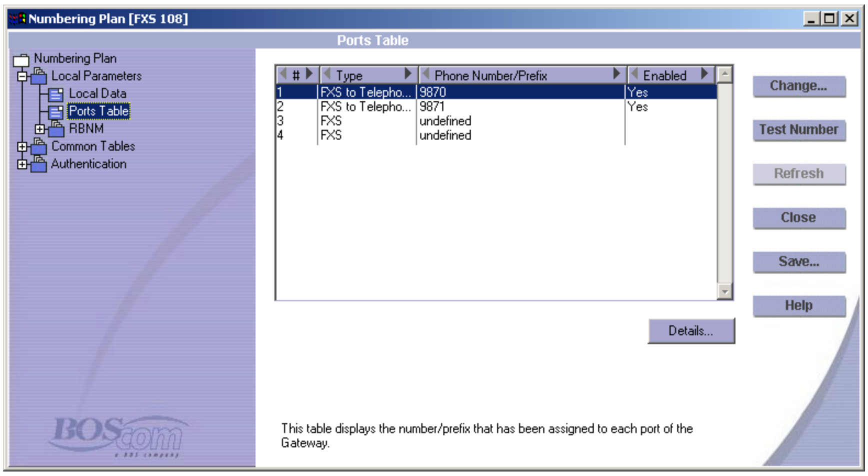
Comparison of appearance when using and not using a gatekeeper

7. Enter the private-number prefix and a description. The description simplifies later identification.
8. Select the Register on Gatekeeper checkbox when:
   - configuring a Gateway that will work with a Gatekeeper, and
   - the Private number prefix is to registered on the Gatekeeper as an E.164 alias.
9. Click **OK**.
10. Repeat steps 5 – 9 until all private-number prefixes are configured.
11. Complete the Wizard.

Associated Tables

Following configuration, private-number prefixes will appear in these tables:

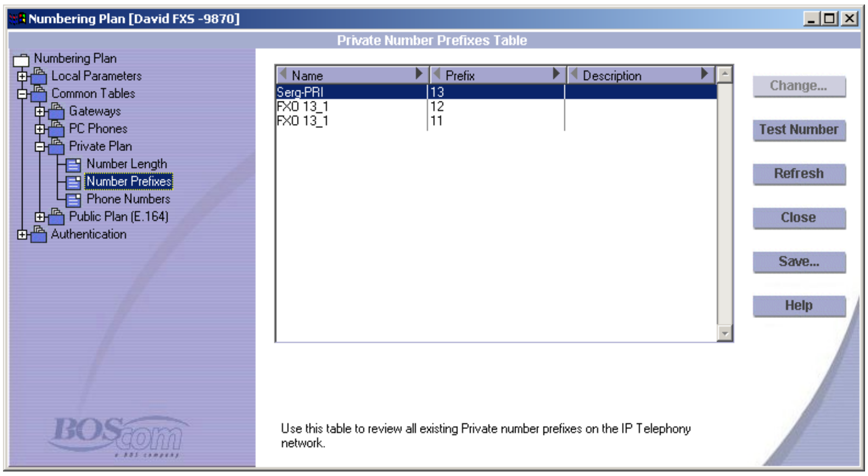
Local Parameters



#	Type	Phone Number/Prefix	Enabled
1	FXS to Telepho...	9870	Yes
2	FXS to Telepho...	9871	Yes
3	FXS	undefined	
4	FXS	undefined	

This table displays the number/prefix that has been assigned to each port of the Gateway.

Common Tables



Name	Prefix	Description
Serg-PRI	13	
FXO 13_1	12	
FXO 13_1	11	

Use this table to review all existing Private number prefixes on the IP Telephony network.

DEFINING AND APPLYING HOP-OFF PREFIXES

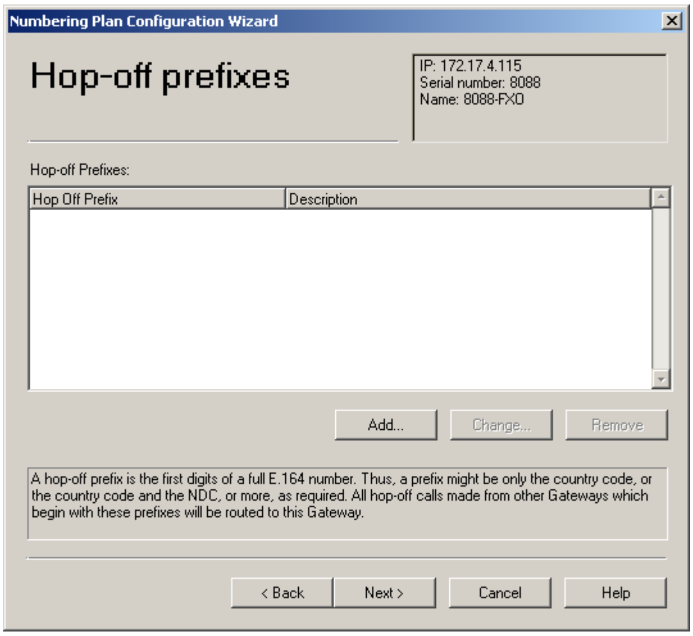
Terminate hop-off is enabled and configured in the Numbering Plan Wizard. For an explanation of hop-off calls, see page 96.

Procedure

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select L**ocal Parameters**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the **Ports information** page.
5. In the Hop-off column, **Yes** indicates that the port is hop-off enabled. Ensure that the appropriate ports are hop-off enabled. (If not, click **Change**, select **Permit this port to redirect IP to PSTN hop-off calls**, and click **OK**.)

In Claro PRI Gateways, hop-off dialing is enabled by selecting the checkbox in the "Termination of hop-off calls" page, not the "Ports information" page.

6. Click **Next** until arriving at the **Hop-off prefixes** page.



IP: 172.17.4.115
Serial number: 8088
Name: 8088-FXO

Hop-off Prefixes:

Hop Off Prefix	Description

A hop-off prefix is the first digits of a full E.164 number. Thus, a prefix might be only the country code, or the country code and the NDC, or more, as required. All hop-off calls made from other Gateways which begin with these prefixes will be routed to this Gateway.

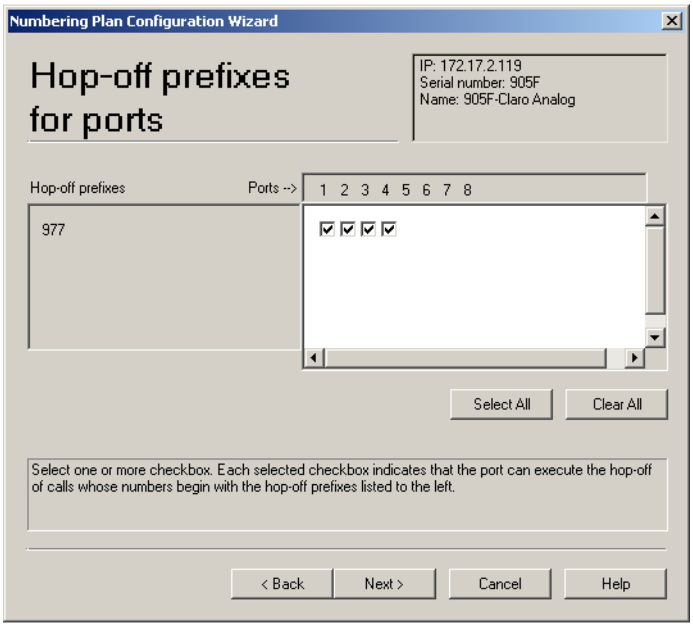
7. Click **Add**. The **Hop-off Prefix** dialog box appears.
8. Enter a hop-off prefix, that is, a sequence of numbers that appears at the beginning of a full public phone number (based on the E.164 standard as

explained on p. 83). Phone numbers starting with that sequence will be redirected to the PSTN.

9. Enter a description. The description simplifies later identification. Click **OK**.

10. Repeat steps 7–9 until all hop-off prefixes have been entered.

11. Click **Next**. The **Hop-off prefixes for ports** dialog box appears.



Numbering Plan Configuration Wizard

Hop-off prefixes for ports

IP: 172.17.2.119
Serial number: 905F
Name: 905F-Claro Analog

Hop-off prefixes	Ports --> 1 2 3 4 5 6 7 8
977	☑ ☑ ☑ ☑

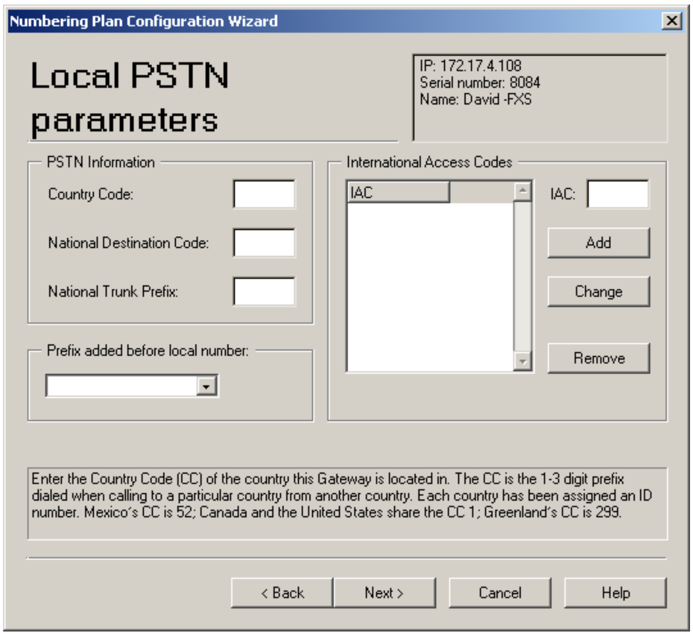
Select one or more checkbox. Each selected checkbox indicates that the port can execute the hop-off of calls whose numbers begin with the hop-off prefixes listed to the left.

12. Select one or more checkbox. Each selected checkbox indicates that the port can execute the hop-off of calls whose numbers begin with the listed hop-off prefixes.

13. Click **Next**. There are two possible scenarios:

    - If the telephony connection is to a PBX, the Access code page opens. Enter the access code that is dialed from PBX extensions to get an outside line. Click **Next**. The Local PSTN parameters page opens.
    - If the telephony connection is to the PSTN, the Local PSTN parameters page opens.

Figure 8: The Local PSTN Parameters Page



Numbering Plan Configuration Wizard

Local PSTN parameters

IP: 172.17.4.108
Serial number: 8084
Name: David -FXS

PSTN Information

Country Code:

National Destination Code:

National Trunk Prefix:

Prefix added before local number:

International Access Codes

IAC

IAC:

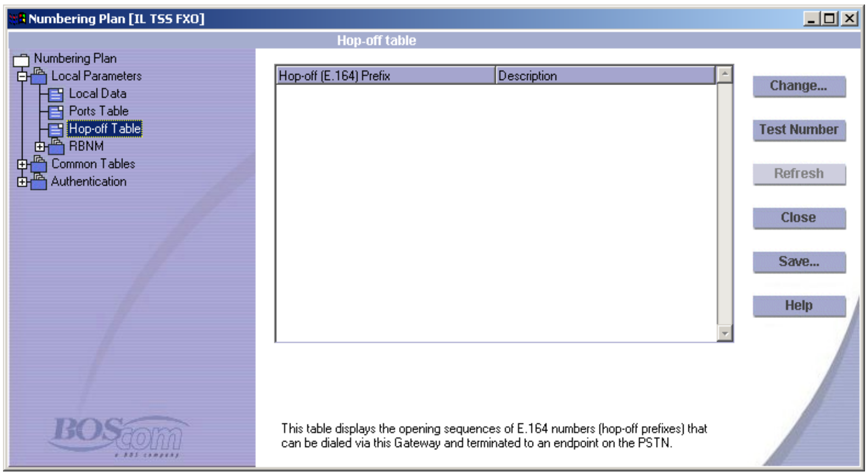
Enter the Country Code (CC) of the country this Gateway is located in. The CC is the 1-3 digit prefix dialed when calling to a particular country from another country. Each country has been assigned an ID number. Mexico's CC is 52; Canada and the United States share the CC 1; Greenland's CC is 299.

14. Enter this Gateway's full telephone number information (based on the E.164 standard as explained on p. 83) and click **Next**.
15. Complete the Wizard.

Associated Tables

Following configuration, hop-off prefixes appear in these tables:

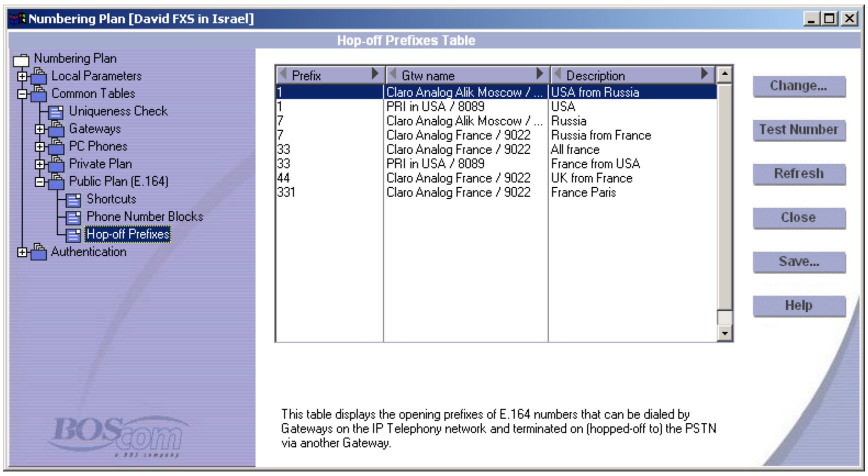
Local Parameters



Hop-off (E.164) Prefix	Description

This table displays the opening sequences of E.164 numbers (hop-off prefixes) that can be dialed via this Gateway and terminated to an endpoint on the PSTN.

Common Tables



Prefix	Gtw name	Description
1	Claro Analog Alik Moscow / ...	USA from Russia
1	PRI in USA / 8089	USA
7	Claro Analog Alik Moscow / ...	Russia
7	Claro Analog France / 9022	Russia from France
33	Claro Analog France / 9022	All france
33	PRI in USA / 8089	France from USA
44	Claro Analog France / 9022	UK from France
331	Claro Analog France / 9022	France Paris

This table displays the opening prefixes of E.164 numbers that can be dialed by Gateways on the IP Telephony network and terminated on (hopped-off to) the PSTN via another Gateway.

DIALING PUBLIC NUMBERS

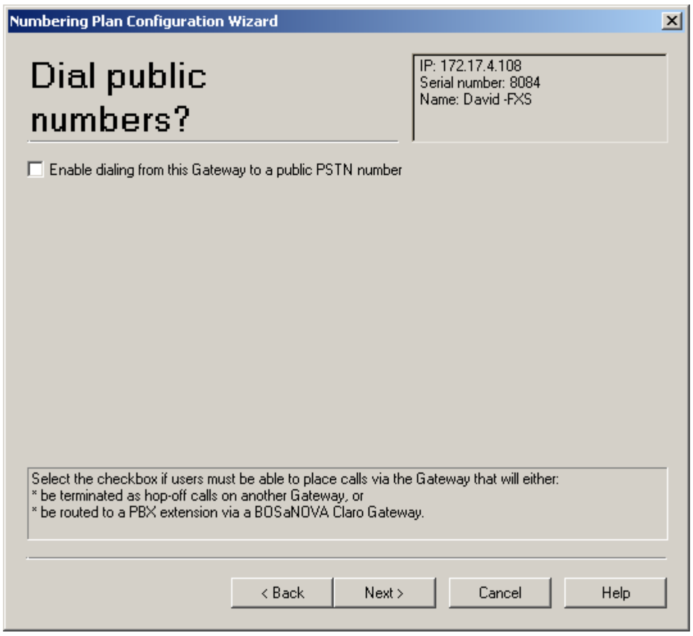
Dial public numbers is enabled in the Numbering Plan Wizard. For an explanation of dialing public numbers, see page 96.

*If **Hop-off calls** is enabled, the Wizard skips the Dial public numbers page. In that case, Dial public numbers* **is** *automatically enabled.*

Regarding Claro Gateways, Local PSTN parameters are always defined. Therefore, on Claro Gateways, the Wizard skips the Dial public numbers page.

Procedure

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Local Parameters**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the **Dial public numbers** page. (This assumes that the previous pages of the Wizard have been completed.)

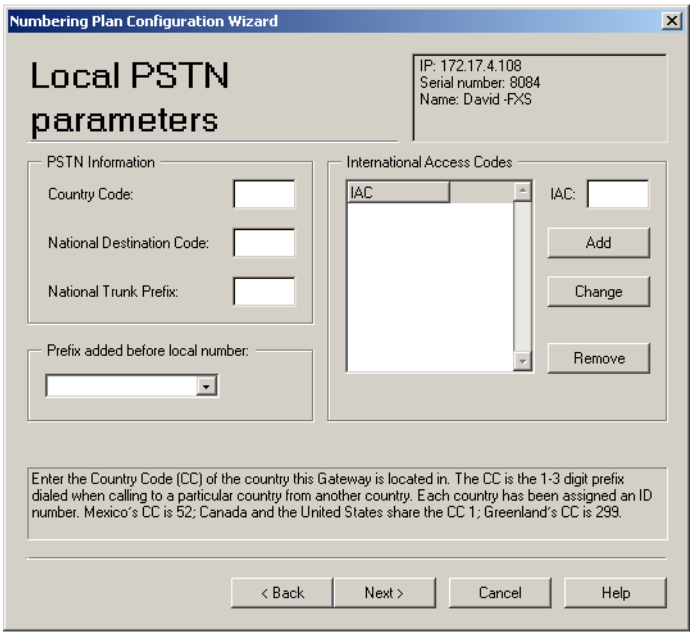


IP: 172.17.4.108
Serial number: 8084
Name: David -FXS

□ Enable dialing from this Gateway to a public PSTN number

Select the checkbox if users must be able to place calls via the Gateway that will either:
* be terminated as hop-off calls on another Gateway, or
* be routed to a PBX extension via a BOSaNOVA Claro Gateway.

5. Select the checkbox and click **Next**. The **Local PSTN parameters** page opens.


Numbering Plan Configuration Wizard
Local PSTN parameters
PSTN Information
Country Code:
National Destination Code:
National Trunk Prefix:
Prefix added before local number:
International Access Codes
IAC
IAC:
Add
Change
Remove
< Back
Next >
Cancel
Help

IP: 172.17.4.108
Serial number: 8084
Name: David -FXS

Enter the Country Code (CC) of the country this Gateway is located in. The CC is the 1-3 digit prefix dialed when calling to a particular country from another country. Each country has been assigned an ID number. Mexico's CC is 52; Canada and the United States share the CC 1; Greenland's CC is 299.

6. Enter this Gateway's full telephone number information (based on the E.164 standard as explained on p. 83) and click **Next**.

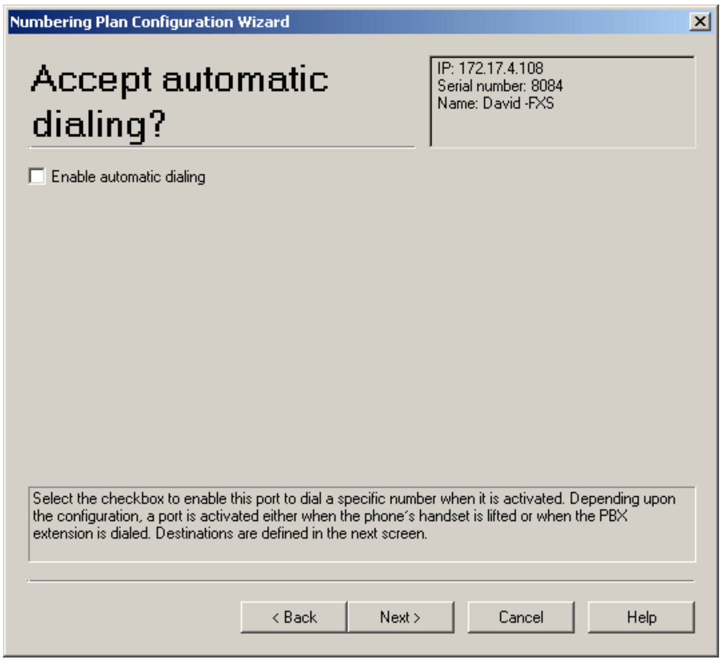
7. Complete the Wizard.

CONFIGURING AUTOMATIC DIALING

Configuring Automatic Dialing is done in the Numbering Plan Wizard of each Gateway. For an explanation of automatic dialing, see page 98.

Procedure

1. From the **Configurator main menu**, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Local Parameters**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the **Accept automatic dialing** page. (This assumes that the previous pages of the Wizard have been completed.)



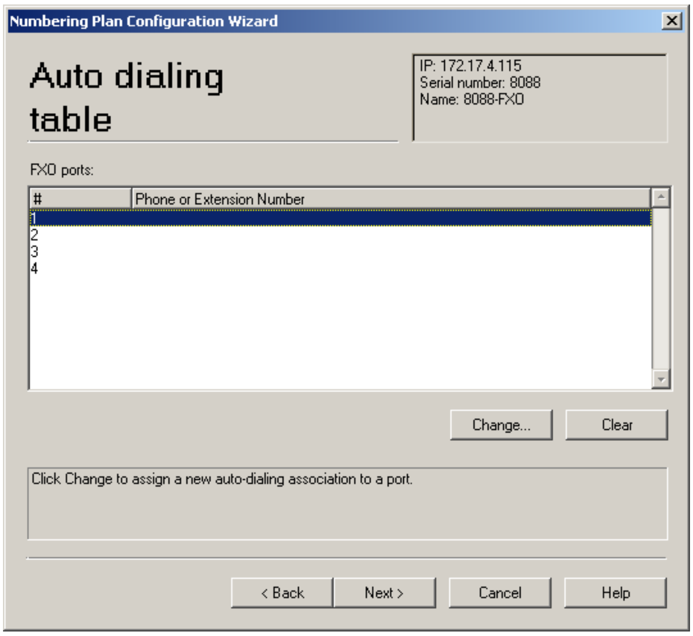
Accept automatic dialing?

IP: 172.17.4.108
Serial number: 8084
Name: David -FXS

□ Enable automatic dialing

Select the checkbox to enable this port to dial a specific number when it is activated. Depending upon the configuration, a port is activated either when the phone's handset is lifted or when the PBX extension is dialed. Destinations are defined in the next screen.

5. Select **Enable automatic dialing** and click **Next**. The **Auto dialing table** page opens.



Click Change to assign a new auto-dialing association to a port.

6. Select a port. The row changes color when selected.
7. Click **Change**. The **Number for Port** dialog box opens.
8. Enter the phone number or extension number that will be dialed when the port is activated and click **OK**.
9. Complete the Wizard.

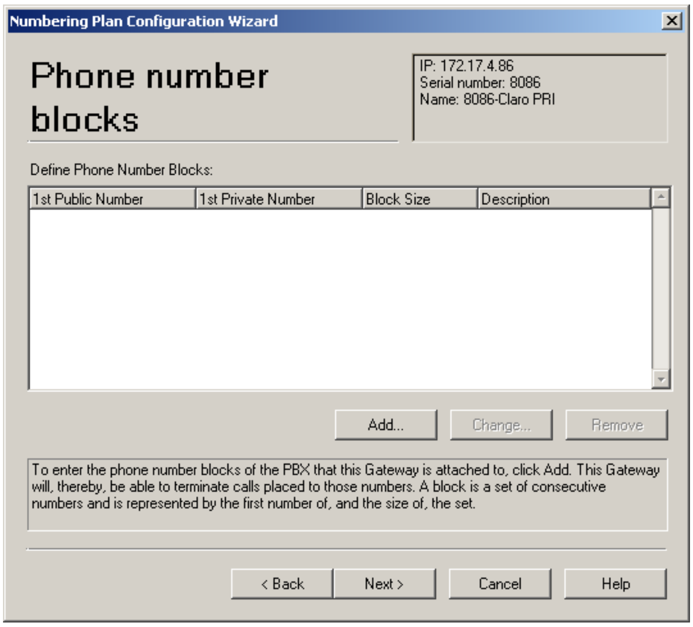
DEFINING CLARO PRI PHONE NUMBER BLOCKS

Phone number blocks are defined in the Numbering Plan Wizard. A block is a set of consecutive numbers and is represented by the first number of, and the size of, the set. For an explanation of Phone number blocks, see p. 105.

This topic is relevant to Claro PRI Gateways only.

Procedure

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Local Parameters**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the **Phone number blocks** page. (This assumes that the previous pages of the Wizard have been completed.)



Numbering Plan Configuration Wizard

Phone number blocks

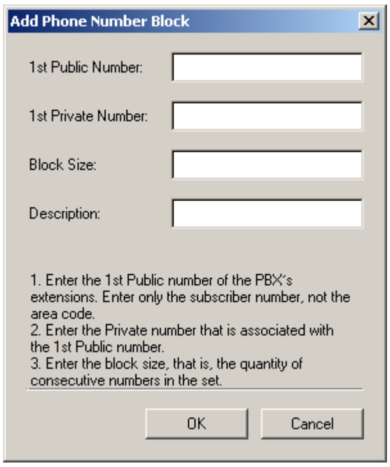
IP: 172.17.4.86
Serial number: 8086
Name: 8086-Claro PRI

Define Phone Number Blocks:

1st Public Number	1st Private Number	Block Size	Description

To enter the phone number blocks of the PBX that this Gateway is attached to, click Add. This Gateway will, thereby, be able to terminate calls placed to those numbers. A block is a set of consecutive numbers and is represented by the first number of, and the size of, the set.

5. Click **Add**. The **Add Phone Number Block** dialog box opens.



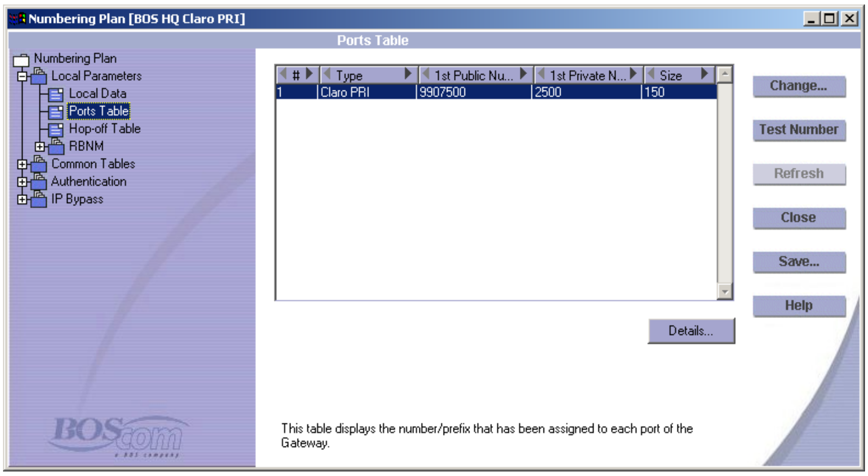
1. Enter the 1st Public number of the PBX's extensions. Enter only the subscriber number, not the area code.
2. Enter the Private number that is associated with the 1st Public number.
3. Enter the block size, that is, the quantity of consecutive numbers in the set.

6. In the **1st Public Number** field, enter the first number of the block.
7. In the **1st Private Number** field, enter the first number of the block. Assigning Private numbers is optional.
8. In the **Block Size** field, enter the quantity of phone numbers in the block.
9. Enter a description and click **OK**. The dialog box closes and the block definitions appear in the table.
10. Complete the Wizard.

Associated Tables

Following configuration, phone number blocks appear in these tables:

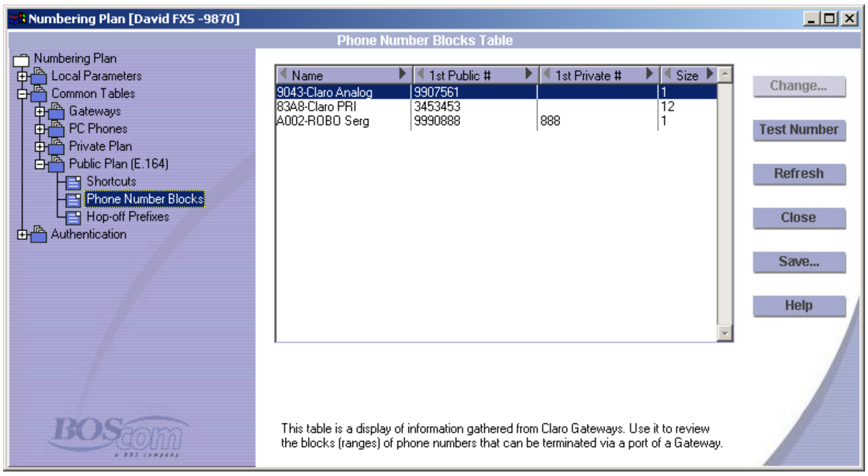
Local Parameters



#	Type	1st Public Nu...	1st Private N...	Size
1	Claro PRI	9907500	2500	150

This table displays the number/prefix that has been assigned to each port of the Gateway.

Common Tables



Name	1st Public #	1st Private #	Size
9043-Claro Analog	9907561		1
83A8-Claro PRI	3453453		12
A002-ROBO Serg	9990888	888	1

This table is a display of information gathered from Claro Gateways. Use it to review the blocks (ranges) of phone numbers that can be terminated via a port of a Gateway.

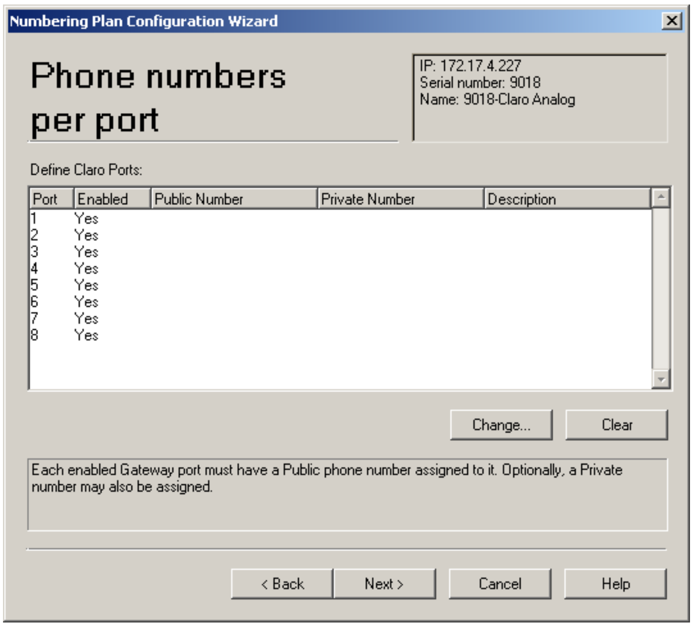
DEFINING CLARO ANALOG PHONE NUMBERS PER PORT

Public and Private numbers for a Claro Analog Gateway are defined in the Numbering Plan Wizard.

This topic is relevant to Claro Analog Gateways only.

Procedure

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Local Parameters**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the **Phone numbers per port** page. (This assumes that the previous pages of the Wizard have been completed.)



Numbering Plan Configuration Wizard

Phone numbers per port

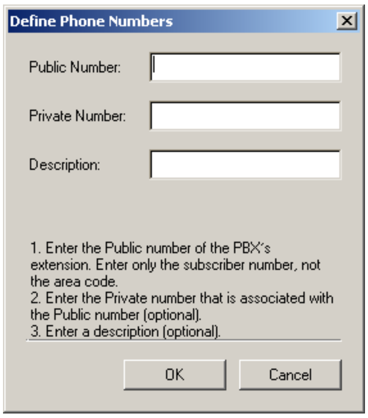
IP: 172.17.4.227
Serial number: 9018
Name: 9018-Claro Analog

Define Claro Ports:

Port	Enabled	Public Number	Private Number	Description
1	Yes			
2	Yes			
3	Yes			
4	Yes			
5	Yes			
6	Yes			
7	Yes			
8	Yes			

Each enabled Gateway port must have a Public phone number assigned to it. Optionally, a Private number may also be assigned.

5. Click **Change**. The Define Phone Numbers dialog box opens.



1. Enter the Public number of the PBX's extension. Enter only the subscriber number, not the area code.
2. Enter the Private number that is associated with the Public number (optional).
3. Enter a description (optional).

6. In the **Public Number** field, enter ***only*** the Subscriber Number portion of the end-point's E.164 number. Do not enter the National Destination Code or the Country Code.

7. Optionally, in the **Private Number** field, enter the Private number.

8. Optionally, enter a **Description** of the end-point, such as the user's name or the type of equipment. The description simplifies later identification.

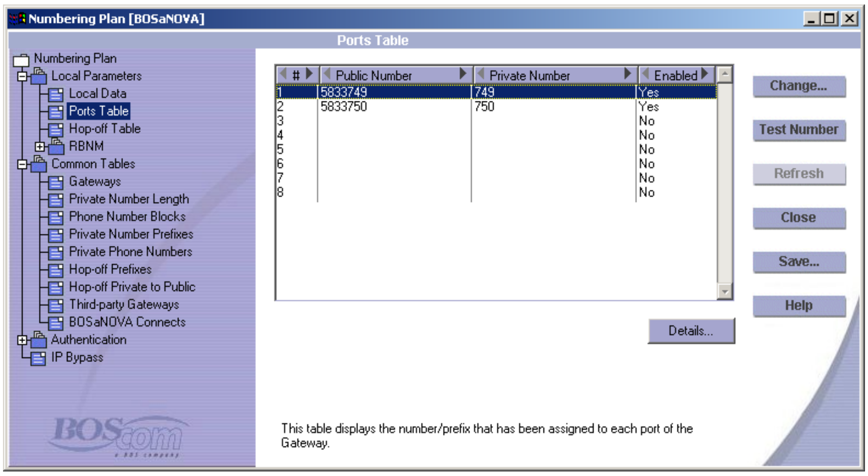
9. Click **OK**. The dialog box closes and the numbers appear in the table.

10. Complete the Wizard.

Associated Tables

Following configuration, port phone numbers appear in these tables:

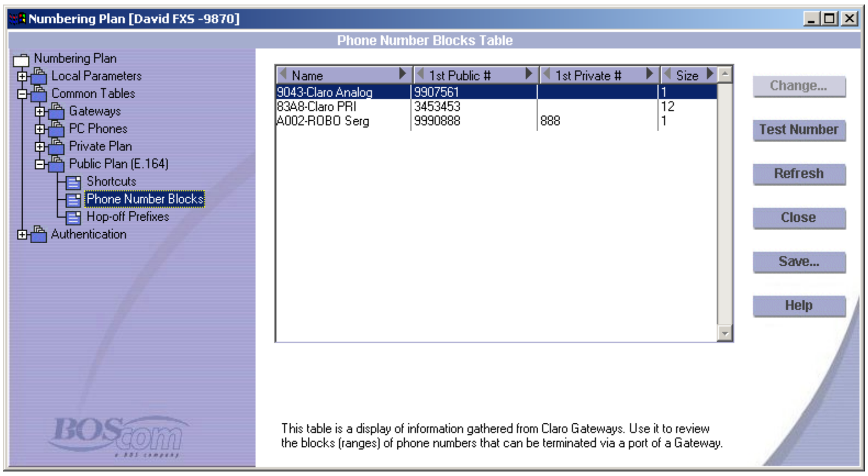
Local Parameters



#	Public Number	Private Number	Enabled
1	5833749	749	Yes
2	5833750	750	Yes
3			No
4			No
5			No
6			No
7			No
8			No

This table displays the number/prefix that has been assigned to each port of the Gateway.

Common Tables



Name	1st Public #	1st Private #	Size
9043-Claro Analog	9907561		1
83A8-Claro PRI	3453453		12
A002-ROBO Serg	9990888	888	1

This table is a display of information gathered from Claro Gateways. Use it to review the blocks (ranges) of phone numbers that can be terminated via a port of a Gateway.

The block size of a Claro Analog Gateway port is always 1.

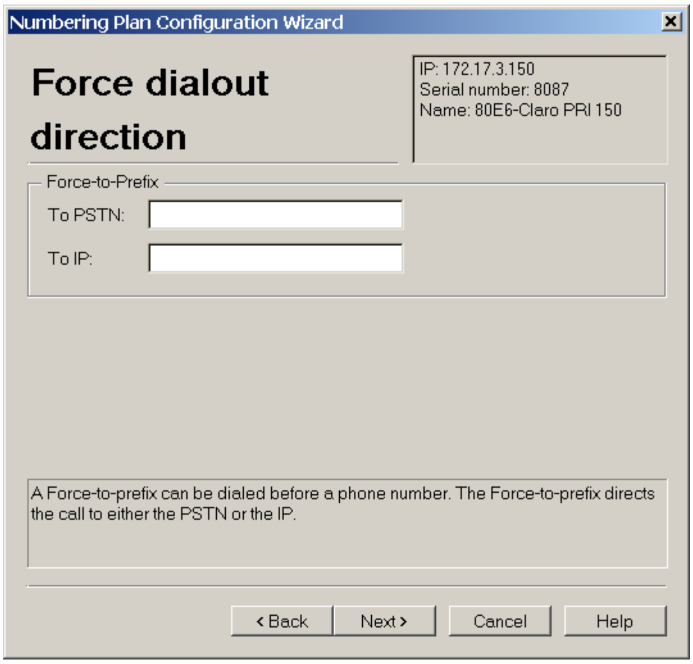
DEFINING FORCE DIALOUT DIRECTION

Force dialout direction is defined in the Numbering Plan Wizard. For an explanation of Force dialout direction, see p. 106.

This topic is relevant to Claro Gateways only.

Procedure

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Local Parameters**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the **Force dialout direction** page.



IP: 172.17.3.150
Serial number: 8087
Name: 80E6-Claro PRI 150

A Force-to-prefix can be dialed before a phone number. The Force-to-prefix directs the call to either the PSTN or the IP.

5. In the **To PSTN** field, enter the prefix that the user will dial to restrict a call to the PSTN.
6. In the **To IP** field, enter the prefix that the user will dial to restrict a call to the IP.
7. Click **Next** and complete the Wizard.

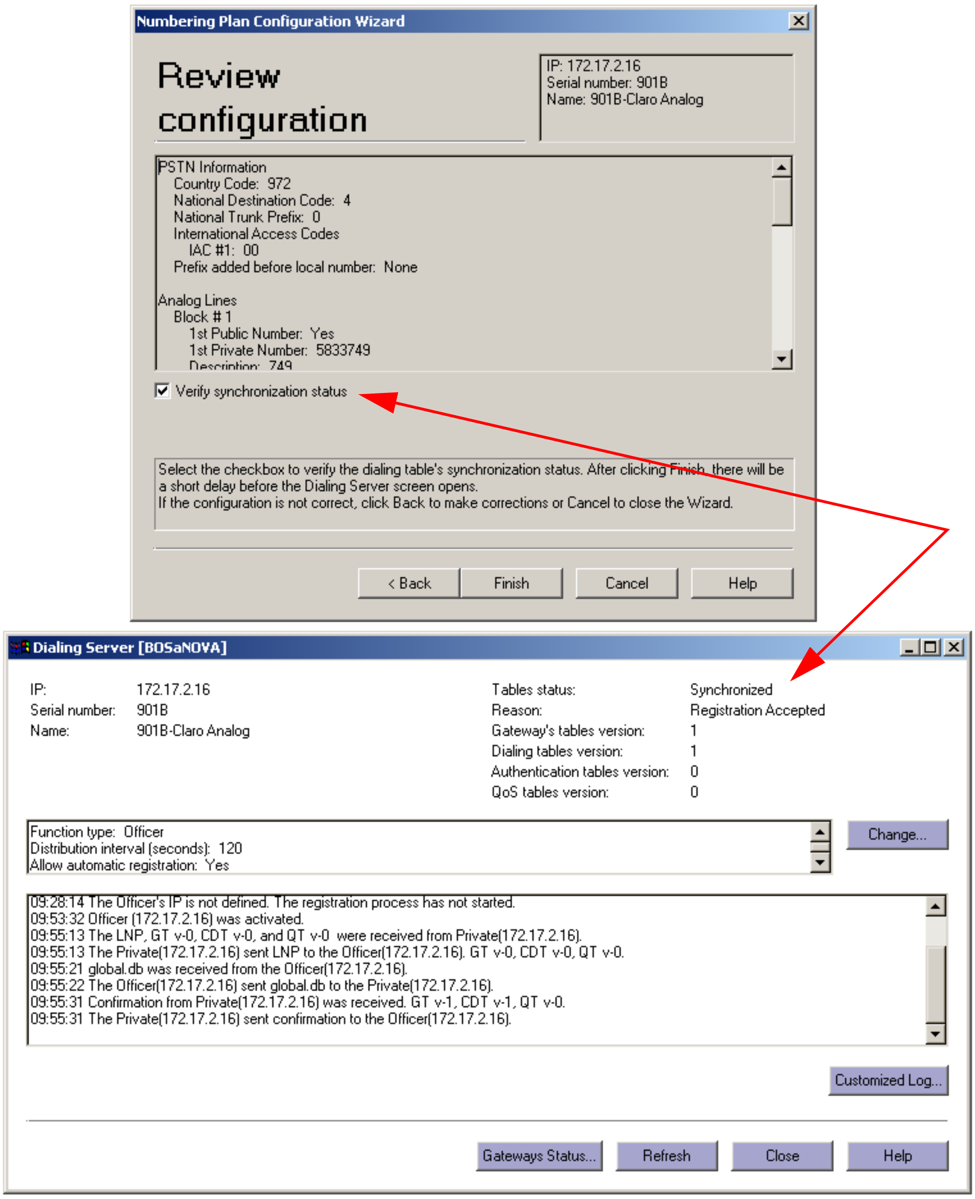
*Following configuration, the **Force to** information appears in the Numbering Plan Configurator > Local Parameters > Local Data table.*

REVIEW THE NUMBERING PLAN CONFIGURATION

Use the final page of the Numbering Plan Wizard to review the configuration. If the configuration is correct, select or clear the **Verify synchronization status** checkbox and click **Finish**.

When **Verify synchronization status** is selected:

1. the Numbering Plan Wizard closes;
2. there is a delay of a few seconds;
3. the Dialing Server opens. Whether or not the numbering plan tables are synchronized is displayed on the Dialing Server.



IP: 172.17.2.16
Serial number: 901B
Name: 901B-Claro Analog

```
PSTN Information
   Country Code:  972
   National Destination Code:  4
   National Trunk Prefix:  0
   International Access Codes
      IAC #1:  00
   Prefix added before local number:  None

Analog Lines
   Block # 1
      1st Public Number:  Yes
      1st Private Number:  5833749
      Description:  749
```

☑ Verify synchronization status

Select the checkbox to verify the dialing table's synchronization status. After clicking Finish, there will be a short delay before the Dialing Server screen opens.
If the configuration is not correct, click Back to make corrections or Cancel to close the Wizard.

IP: 172.17.2.16
Serial number: 901B
Name: 901B-Claro Analog

Tables status: Synchronized
Reason: Registration Accepted
Gateway's tables version: 1
Dialing tables version: 1
Authentication tables version: 0
QoS tables version: 0

Function type: Officer
Distribution interval (seconds): 120
Allow automatic registration: Yes

```
09:28:14 The Officer's IP is not defined. The registration process has not started.
09:53:32 Officer (172.17.2.16) was activated.
09:55:13 The LNP, GT v-0, CDT v-0, and QT v-0  were received from Private(172.17.2.16).
09:55:13 The Private(172.17.2.16) sent LNP to the Officer(172.17.2.16). GT v-0, CDT v-0, QT v-0.
09:55:21 global.db was received from the Officer(172.17.2.16).
09:55:22 The Officer(172.17.2.16) sent global.db to the Private(172.17.2.16).
09:55:31 Confirmation from Private(172.17.2.16) was received. GT v-1, CDT v-1, QT v-0.
09:55:31 The Private(172.17.2.16) sent confirmation to the Officer(172.17.2.16).
```

SECTION 9:
NUMBERING PLAN WIZARD—CONNECTION CONFIGURATION

The Numbering Plan Wizard is used both for configuring the connection type and for configuring the parameters and features of the numbering plan.

This section details the procedures involved in configuring the Gateway's connection type.

Numbering Plan configuration is completed:

- 85% in the Numbering Plan Wizard, pages 108–142
- 10% in the Numbering Plan Configurator, pages 156–196
- Assigning an Officer in the Dialing Server, see page 218

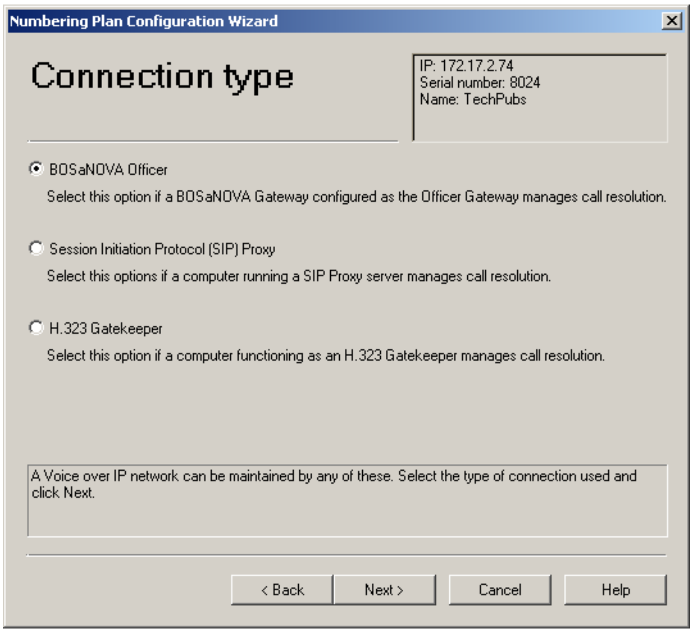
*Following the initial setup, access to the Numbering Plan Wizard is **only** via the Numbering Plan Configurator.*

An overview of the BOSâNOVA Gateways Numbering Plan and in-depth explanations of each aspect of the numbering plan are provided in the section "Numbering Plan Overview" beginning on page 80.

*Before beginning, we recommend that, at the very least, you read **Basics of Configuration** on page 88.*

CONNECTION TYPE

The third page of the Numbering Plan Wizard requests that you select a Connection Type for this Gateway.



Connection type

IP: 172.17.2.74
Serial number: 8024
Name: TechPubs

● BOSaNOVA Officer
Select this option if a BOSaNOVA Gateway configured as the Officer Gateway manages call resolution.

○ Session Initiation Protocol (SIP) Proxy
Select this options if a computer running a SIP Proxy server manages call resolution.

○ H.323 Gatekeeper
Select this option if a computer functioning as an H.323 Gatekeeper manages call resolution.

A Voice over IP network can be maintained by any of these. Select the type of connection used and click Next.

1. Select a connection type:
   - BOSâNOVA Officer
     The Officer Gateway is the Gateway on a BOSâNOVA IP Telephony network which compiles, maintains, and distributes a synthesis of all the other Gateway information. The section entitled *Using the Officer Gateway*, which begins on page 203, contains an overview of the responsibilities of, and procedures for configuring, the Officer Gateway.
   - Session Initiation Protocol (SIP) Proxy
     A SIP proxy is a computer running the Session Initiation Protocol (SIP). SIP is one of two protocols for carrying voice over IP. Procedures for configuring a SIP Proxy begin on page 183.
   - H.323 Gatekeeper
     A gatekeeper is a computer that performs address resolution and manages call control and network resources. It also provides call authorization and call accounting. Procedures for configuring an H.323 Gatekeeper begin on page 147.

See "Selecting H.323 or SIP" on page 113 for an overview of the SIP and H.323 protocols.

2. Click **Next**. The page displayed depends upon the selected connection type.

    - If you selected BOSâNOVA Officer, the Preferred protocol page of the Wizard is displayed. It is documented on page 113.
    - If you selected SIP Proxy, the Port information page of the Wizard is displayed. It is documented beginning on page 119.
    - If you selected H.323 Gatekeeper, the Gatekeeper parameters page of the Wizard is displayed. It is documented beginning on page 147.

CONFIGURING GATEKEEPER AS THE CONNECTION TYPE

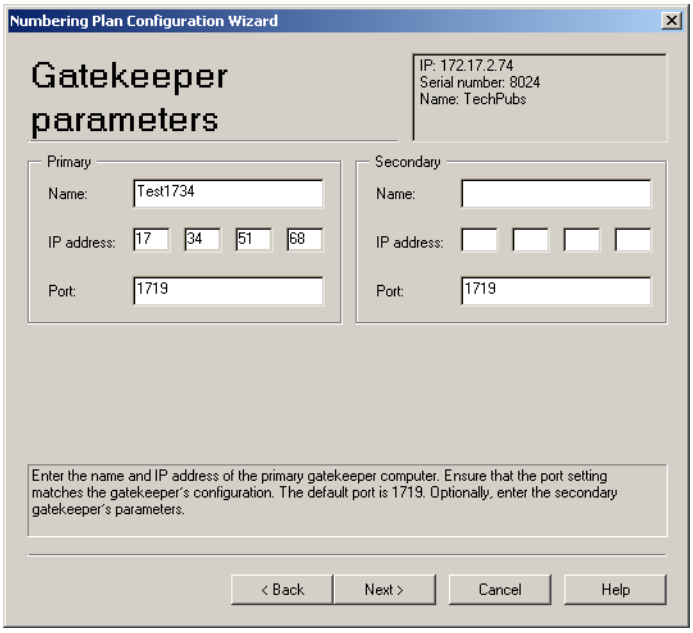
Gatekeeper parameters are assigned in the Numbering Plan Wizard.

The Gatekeeper parameters page only appears if H.323 Gatekeeper was selected as the Connection type. See “Connection Type” on page 145.

When a Gatekeeper is used, the BOSâNOVA Gateway Numbering Plan is not used. In addition, if the call cannot be resolved via the Gatekeeper, Claro Gateways (including the ROBO) reroute the call to the PSTN.

Procedure

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Connection Type**.
3. Click **Change**. The Numbering Plan Wizard opens.
4. Click **Next** until arriving at the **Connection Type** page.
5. Select **H.323 Gatekeeper** and click **Next**. The **Gatekeeper parameters** page is displayed.



Numbering Plan Configuration Wizard

Gatekeeper parameters

IP: 172.17.2.74
Serial number: 8024
Name: TechPubs

Primary

Name: Test1734

IP address: 17 34 51 68

Port: 1719

Secondary

Name:

IP address:

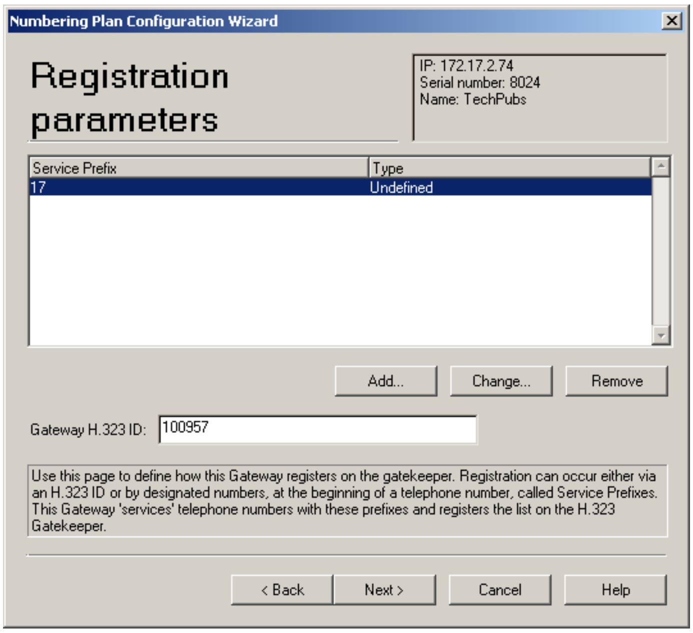
Port: 1719

Enter the name and IP address of the primary gatekeeper computer. Ensure that the port setting matches the gatekeeper's configuration. The default port is 1719. Optionally, enter the secondary gatekeeper's parameters.

6. Set the Primary Gatekeeper's three parameters:

   - **Name**
     Enter the name which identifies the Gatekeeper from which this Gateway obtains permission to register.
   - **IP address**
     Enter the IP address of the gatekeeper computer used to place calls.
   - **Port**
     Ensure that this setting matches the configuration of the gatekeeper computer used to place your calls. The default port is 1719.

7. If relevant, set the Secondary Gatekeeper's three parameters.
8. Click **Next**. The Registration Parameters page is displayed.



Registration parameters

IP: 172.17.2.74
Serial number: 8024
Name: TechPubs

Service Prefix	Type
17	Undefined

Gateway H.323 ID: 100957

Use this page to define how this Gateway registers on the gatekeeper. Registration can occur either via an H.323 ID or by designated numbers, at the beginning of a telephone number, called Service Prefixes. This Gateway 'services' telephone numbers with these prefixes and registers the list on the H.323 Gatekeeper.

9. Configure the Service Prefixes. Service Prefixes, and the procedure for configuring Service Prefixes, are documented beginning on page 150.
10. If required, enter an H.323 ID. This is the name this Gateway uses to identify itself to the Gatekeeper. Each Gateway must have a unique ID.

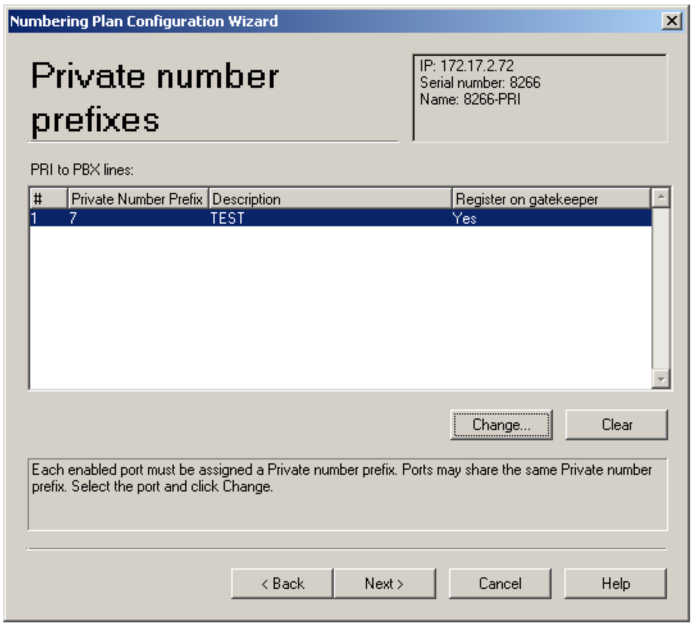
    The following issues affect the configuration of the H.323 ID:

    - The H.323 ID is an optional parameters.
    - When the H.323 ID is not configured, the Gateway identifies itself to the Gatekeeper using either E.164 aliases or services prefixes.

11. With the exception of the Private number prefixes page, and the Private phone numbers page, the remaining pages of the Wizard do not change when a Gatekeeper is used. The Numbering Plan pages of the Wizard are documented in the preceding section, beginning on page 108.

When a Gatekeeper is used, the **Register on Gatekeeper/Proxy** checkbox appears on the Private number prefixes page, and the Private phone numbers page, of the Wizard.

a. Display the Private number prefixes page or the Private phone numbers page for an FXS Gateway.



Numbering Plan Configuration Wizard

Private number prefixes

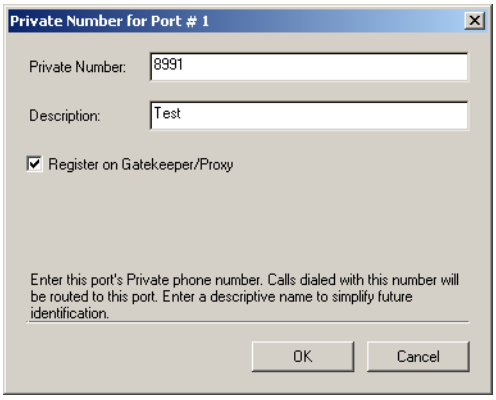
IP: 172.17.2.72
Serial number: 8266
Name: 8266-PRI

PRI to PBX lines:

#	Private Number Prefix	Description	Register on gatekeeper
1	7	TEST	Yes

Each enabled port must be assigned a Private number prefix. Ports may share the same Private number prefix. Select the port and click Change.

b. Click **Change**. The Private Number Prefix for Port dialog box is displayed.



Private Number for Port # 1

Private Number: 8991

Description: Test

☑ Register on Gatekeeper/Proxy

Enter this port's Private phone number. Calls dialed with this number will be routed to this port. Enter a descriptive name to simplify future identification.

c. Select **Register on Gatekeeper/Proxy** if the Private Number Prefix is to function as an E.164 alias and click **OK.**

d. Complete the Numbering Plan Wizard.

e. Close the Numbering Plan Configurator and reboot the Gateway.

Registration Parameters: Service Prefixes

The Service Prefix is one or more numbers added before the telephone number.

The Service Prefix Table is a list of all Service Prefixes supported by the local Gateway. The Gateway registers this list on the H.323 Gatekeeper.

During the registration process, each Gateway on the IP Telephony network sends its list of Service Prefixes to the H.323 Gatekeeper. When a service prefix precedes the phone number, the Gatekeeper uses this list to make decisions regarding termination of the call.

Uses of the Service Prefix

The Gatekeeper uses the list of Service Prefixes received from the Gateways for resolving the destination Gateway IP address.

- Example 1: BOSaNOVA Claro PRI should terminate calls for range of phone numbers: +44-116-2821-500 until +44-116-2821-699. Corresponding private numbers are 4500-4699. Also, this gateway is responsible for hop-off calls to France (33). In this case, it is possible to define the service prefixes as the following:

Prefix	Type
4411628215	Public
4411628215	Public
45	Private
46	Private
33	Hop-off

*For most Gatekeepers, the Type parameter can be left as **Undefined**. In limited cases, for purposes of interoperability, the type may need to be defined.*

- Example 2: Gateway A registered on the Gatekeeper with the Service Prefix list that consists of 33, 44 and 49. If a user, via Gateway B, dials 44.nn.n (where nn.n denotes any digits), Gateway B sends a request to the Gatekeeper to make a connection to the phone number 44nn.n. Then, the Gatekeeper routes this call to Gateway A.

A Service Prefix can identify a type of service.

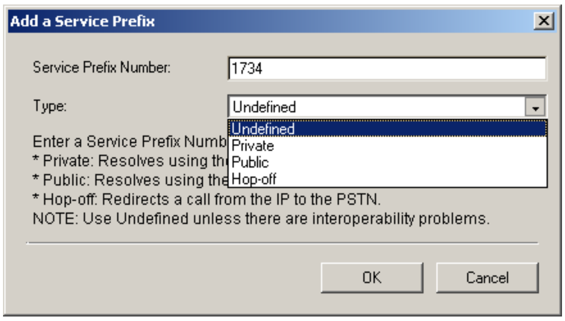
- For example, location B has three Gateways, two dedicated to voice (B1 and B2) and one dedicated to video conferencing (B3). The

System Administrator may assign the Service Prefix 20 for voice conversations and the Service Prefix 30 for video. In this case, Gateways B1 and B2 register on the Gatekeeper with the Service Prefix 20 and Gateway B3 with the Service Prefix 30. A VoIP Network user joining the video conference must dial Service Prefix 30 before dialing the phone number. To place a voice call, the user must dial 20.

In certain circumstances, the Service Prefixes may be used for advanced phone number manipulation.

Adding a Service Prefix

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Connection Type**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the Registration Parameters page.
5. Click **Add**. The Add a Service Prefix dialog box opens.


Add a Service Prefix

Service Prefix Number: 1734

Type: Undefined

Enter a Service Prefix Numb
* Private: Resolves using th
* Public: Resolves using the
* Hop-off: Redirects a call from the IP to the PSTN.
NOTE: Use Undefined unless there are interoperability problems.

6. Enter the service prefix number.
7. For most Gatekeepers, select **Type: Undefined**. In limited cases, for purposes of interoperability, the type may need to be defined.
8. Click **OK**. The Service Prefix dialog box closes.
9. Repeat steps 5–8 for each additional Service Prefix.
10. Complete the Numbering Plan Wizard.
11. Click **Apply**. The Reboot confirmation screen appears.
12. Select either **Reboot now** or **Reboot later**.

Changing a Service Prefix

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Connection Type**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the Registration Parameters page.
5. Select a line in the Service prefixes table.
6. Click **Change**. The Change a Service Prefix dialog box opens.
7. Make the changes.
8. Click **OK**. The Service Prefix dialog box closes.
9. Complete the Numbering Plan Wizard.
10. Click **Apply**. The Reboot confirmation screen appears.
11. Select either **Reboot now** or **Reboot later**.

Removing a Service Prefix

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Connection Type**.
3. Click **Change**. The **Numbering Plan Wizard** opens.
4. Click **Next** until arriving at the Registration Parameters page.
5. Select a line in the Service prefixes table.
6. Click **Remove**. A confirmation message is displayed.
7. Click **OK**. The Service Prefix dialog box closes.
8. Complete the Numbering Plan Wizard.
9. Click **Apply**. The Reboot confirmation screen appears.
10. Select either **Reboot now** or **Reboot later**.

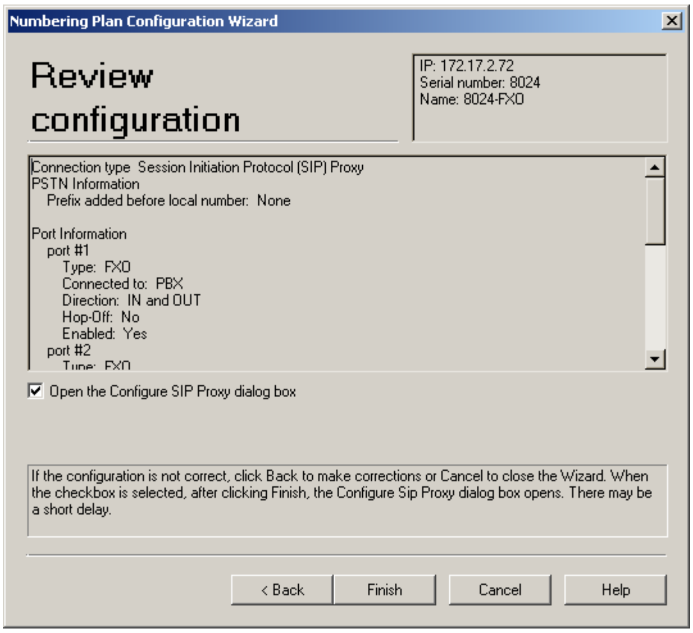
CONFIGURING SIP PROXY AS THE CONNECTION TYPE

SIP Proxy parameters are assigned upon completion of the Numbering Plan Wizard and, subsequently, from the Numbering Plan Configurator. (See “Configuring SIP Proxy Parameters” on page 184.)

However, SIP Proxy must first be selected as the Connection Type.

Procedure

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Connection Type**.
3. Click **Change**. The Numbering Plan Wizard opens.
4. Click **Next** until arriving at the **Connection Type** page.
5. Select **Session Initiation Protocol (SIP) Proxy**.
6. Proceed with the Numbering Plan Wizard until the **Review configuration** page is displayed. The remaining pages of the Numbering Plan Wizard are documented in the next section beginning on page 108.



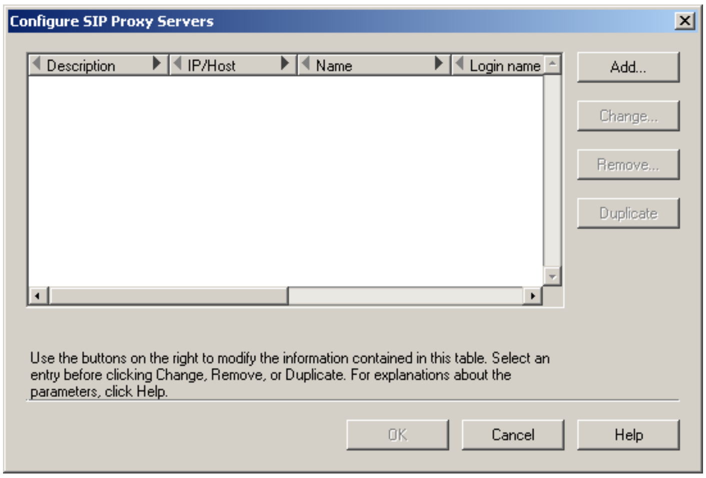
IP: 172.17.2.72
Serial number: 8024
Name: 8024-FXO

```
Connection type  Session Initiation Protocol (SIP) Proxy
PSTN Information
   Prefix added before local number:  None

Port Information
   port #1
      Type:  FXO
      Connected to:  PBX
      Direction:  IN and OUT
      Hop-Off:  No
      Enabled:  Yes
   port #2
      Type:  FXO
```

☑ Open the Configure SIP Proxy dialog box

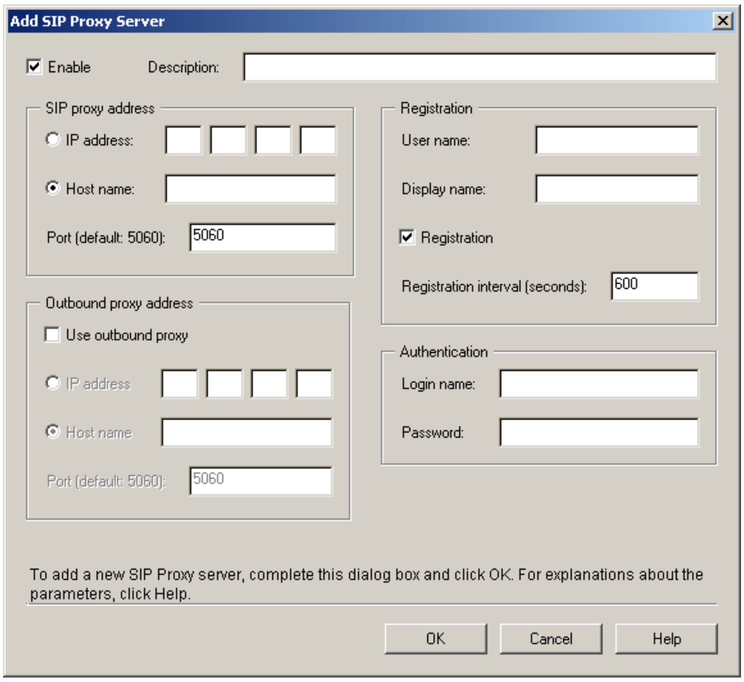
If the configuration is not correct, click Back to make corrections or Cancel to close the Wizard. When the checkbox is selected, after clicking Finish, the Configure Sip Proxy dialog box opens. There may be a short delay.

7. On the **Review configuration** page of the Numbering Plan Wizard, select the **Open the Configure SIP Proxy** dialog and click **Finish**. The Numbering Plan Wizard closes and the Configure SIP Proxy Servers page is displayed.



Use the buttons on the right to modify the information contained in this table. Select an entry before clicking Change, Remove, or Duplicate. For explanations about the parameters, click Help.

8. Click **Add**. The Add SIP Proxy dialog is displayed.



☑ Enable Description:

○ IP address:

● Host name:

Port (default: 5060): 5060

□ Use outbound proxy

○ IP address

● Host name

Port (default: 5060): 5060

User name:

Display name:

☑ Registration

Registration interval (seconds): 600

Login name:

Password:

To add a new SIP Proxy server, complete this dialog box and click OK. For explanations about the parameters, click Help.

9. Complete the fields. Depending upon the configuration determined by the IP Telephony network System Administrator, granting the BOSâNOVA Gateway permission to access the SIP proxy can be either a one-step or a two-step process. If it is a one-step process, only registration is required. If it is a two-step process, authentication is also required.

All of the following information must be obtained from the IP Telephony network System Administrator.

a. Enter the IP address, or the Host name, used to access the SIP proxy.

b. Confirm which UDP port is used. 5060 is the default UDP port used for SIP audio.

c. If an outbound proxy is used, select the checkbox and enter the IP address or the Host name.

d. In the Registration field, enter the User name and Display name.

e. Depending upon the SIP application for the local network architecture, either select or clear the Registration checkbox.

f. In the Registration interval field, enter a time less than the connection renewal time assigned by the IP Telephony Service Provider.

g. If authentication is required, enter the login name and the password assigned to you by the IP Telephony network System Administrator. This is the login name the SIP proxy server uses for authentication (via MD5 encryption).

10. Click **OK**. The Add SIP Proxy dialog box closes and the **Configured SIP Proxies** screen is displayed.
11. Click **OK**. The Numbering Plan Configurator is displayed.

The remaining branches of the SIP Proxy Connection Type are documented in the Numbering Plan Configurator section beginning on page 186.

SECTION 10:
NUMBERING PLAN CONFIGURATOR PROCEDURES

This section details the procedures involved in configuring a Numbering Plan which are completed in the Numbering Plan Configurator, that is, not via the Wizard. The corresponding Numbering Plan Configurator tables are displayed.

Numbering Plan configuration is completed:

- 85% in the Numbering Plan Wizard, pages 107–143
- 10% in the Numbering Plan Configurator, pages 174–196
  - Overview of the Numbering Plan Configurator, page 157
  - Completion Rule Mode, page 158
  - Forced Overlap Mode, page 159
  - Hop-on Number, adding, page 162
  - IP Bypass, configuring, page 196
  - Least Cost Routing, configuring, page 166
  - Maximum Private Number length, assigning, page 171
  - Private to Public Number associations, creating, page 172
  - Rule Based Number Management, page 174
  - Session Initiation Protocol, configuring, page 183
  - Third Party Gateways, configuring, page 189
  - Third-party IP Telephony Service Providers, page 193
- Assigning an Officer in the Dialing Server, see page 218

An overview of the BOSâNOVA Gateways Numbering Plan and in-depth explanations of each aspect of the numbering plan are provided in the section “Numbering Plan Overview” beginning on page 80.

*Before beginning, we recommend that, at the very least, you read **Basics of Configuration** on page 88.*

OVERVIEW OF THE NUMBERING PLAN CONFIGURATOR

The Numbering Plan Configurator is used:

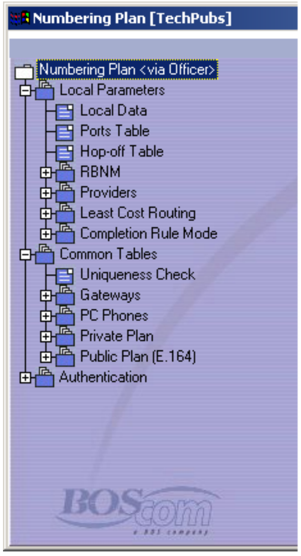
- to access and configure Connection Type ***or*** Numbering Plan parameters available only from the Numbering Plan Wizard
- to configure Connection Type ***or*** Numbering Plan parameters available in the Numbering Plan Configurator

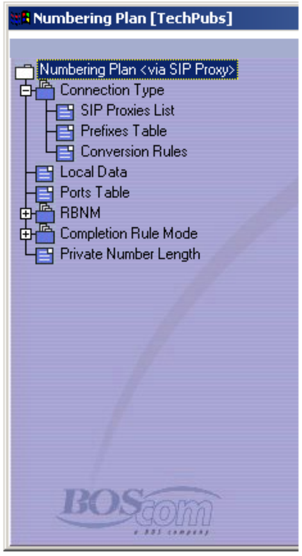
*Following the initial setup, access to the Numbering Plan Wizard is **only** via the Numbering Plan Configurator.*

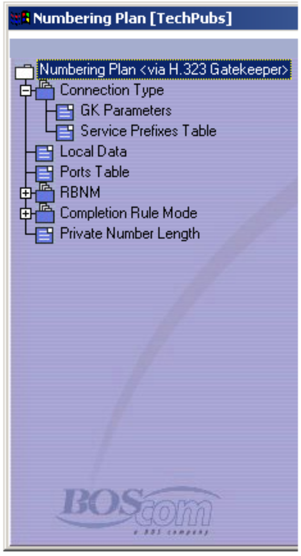
Which branches are displayed on the Numbering Plan Configurator is determined by:

- whether the Gateway is an Analog or a PRI Gateway
- the Connection Type used by the Gateway

The pictures below illustrate the difference between the Numbering Plan Configurators for an ***analog*** (FXO) Gateway. Similar differences exist for PRI Gateways.







The primary difference is that the Common Tables branch exists only when the BOSâNOVA Officer Gateway is used as the Connection Type.

COMPLETION RULE MODE

When the Completion Rule Mode is enabled, the Administrator can create rules that define when the dialing of a phone number is considered completed. These rules can accelerate call progress.

The Completion Rule Mode feature is relevant to Analog Gateways only.

Enabling Completion Rule Mode

To enable Completion Rule Mode:

1. From an Analog Gateway's Configurator main menu, select **Numbering Plan**.
2. Location of the Completion Rule Mode branch depends upon the Connection Type. If the Connection Type is:
   - Officer Gateway
     From the left pane of the Numbering Plan Configurator, expand the **Local Parameters** branch.
   - SIP Proxy or H.323 Gatekeeper
     The Completion Rule Mode branch appears at the root level.
3. Expand the **Completion Rule Mode** branch.
4. Select **Enable and Disable**. The current status is displayed in the right pane.
5. Click **Change**. The Change Completion Rule Mode Status dialog box is displayed.
6. Select the **Completion Rule Mode** checkbox and click **OK**.

Creating Rules for Completion Rule Mode

When Completion Rule Mode is enabled, there may be circumstances wherein it is necessary or preferable to configure the Gateway to proceed with call setup without waiting for the timeout. For example, a PBX might send three digits in the Call Setup message. If the three digits constitute an emergency number, a rule can be created directing the Gateway to proceed with the call immediately.

Similarly, there may be circumstances where the Gateway must be directed not to proceed with call setup.

All configuration processes and interface are the same as those in Forced Overlap Mode. See "Creating Rules for Forced Overlap Mode" on page 159.

FORCED OVERLAP MODE

When operating with most PBXs, the BOSâNOVA PRI Gateway automatically distinguishes between en bloc and overlap signaling. Call setup proceeds accordingly.

To operate with certain PBXs employing overlap signaling, a BOSâNOVA PRI Gateway can be forced to delay call setup until the sending of numbers by the PBX exceeds the timeout. In addition, rules can be created for exceptional circumstances.

The Forced Overlap Mode feature is relevant to PRI Gateways only.

Enabling Forced Overlap Mode

To enable Forced Overlap Mode:

1. From a PRI Gateway’s Configurator main menu, select **Numbering Plan**.
2. From the left pane of the Numbering Plan Configurator, expand the **Local Parameters** branch.
3. Expand the **Forced Overlap Mode** sub-branch.
4. Select **Enable and Disable**. The current status is displayed in the right pane.
5. Click **Change**. The Change Forced Overlap Mode Status dialog box is displayed.
6. Select the **Forced Overlap Mode** checkbox and click **OK**.

Creating Rules for Forced Overlap Mode

When Forced Overlap Mode is enabled, there may be circumstances wherein it is necessary or preferable to configure the Gateway to proceed with call setup without waiting for the timeout. For example, a PBX might send three digits in the Call Setup message. If the three digits constitute an emergency number, a rule can be created directing the Gateway to proceed with the call immediately.

Similarly, there may be circumstances where the Gateway must be directed not to proceed with call setup.

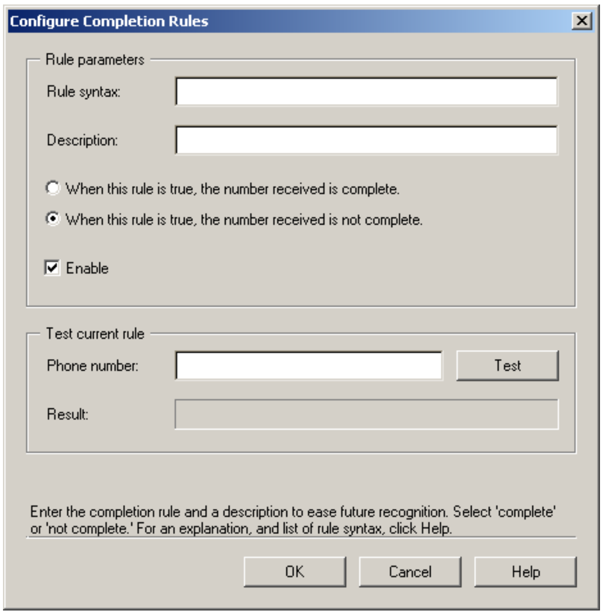
To create a rule to enable precise application of Forced Overlap Mode:

1. From a PRI Gateway’s Configurator main menu, select **Numbering Plan**.
2. From the left pane of the Numbering Plan Configurator, expand the **Local Parameters** branch.
3. Expand the **Forced Overlap Mode** sub-branch.

4. Select **Completion Rules**. The Completion Rules table appears in the right pane.

5. Click **Change**. The Completion Rules dialog box is displayed.

6. Click **Add**. The Configure Completion Rule dialog box is displayed.



Configure Completion Rules

Rule parameters

Rule syntax:

Description:

○ When this rule is true, the number received is complete.

● When this rule is true, the number received is not complete.

☑ Enable

Test current rule

Phone number:

Result:

Enter the completion rule and a description to ease future recognition. Select 'complete' or 'not complete.' For an explanation, and list of rule syntax, click Help.

7. Enter the Completion Rule syntax.

Syntax for rules is discussed in "Operation Code and Operands for RBNM" on page 180 and is available from the online Help.

8. Enter a description that will enable easy understanding of the rule.

9. Select one of the completion options:

   - When this rule is true, the number received is complete.
     When the rule is applied, the number to which it is applied is interpreted as a complete number. The Gateway responds with *Proceeding*.
   - When this rule is true, the number received is ***not*** complete.
     When the rule is applied, the number to which it is applied is interpreted as an incomplete number. The Gateway awaits additional called-party information elements arriving in succeeding messages.

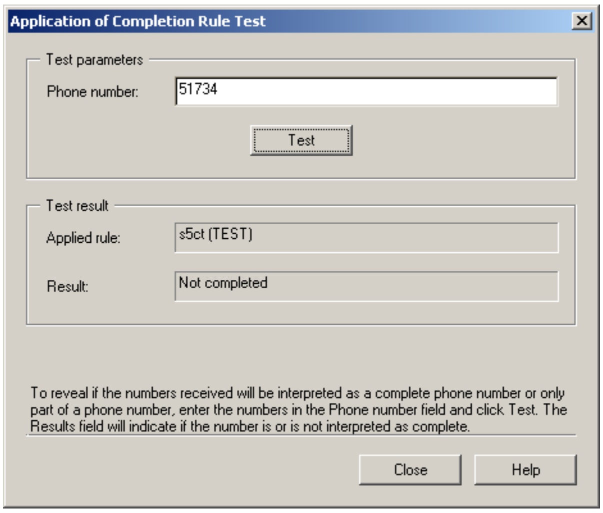
10. Select **Enable** and click **OK**. The new rule appears in the Completion Rules table.

11. To change the order the rules are applied, select the rule and use the Up and Down buttons.

Testing the Application of Completion Rules

When more than one rule exists, the outcome of their application may not be as anticipated. To test the application of all rules to a number:

1. From a PRI Gateway's Configurator main menu, select **Numbering Plan**.
2. From the left pane of the Numbering Plan Configurator, expand the **Local Parameters** branch.
3. Expand the **Forced Overlap Mode** sub-branch.
4. Select **Completion Rules**. The Completion Rules table appears in the right pane.
5. Click **Test**. The Application of Completion Rules Test dialog box is displayed.



Phone number: 51734

Applied rule: s5ct (TEST)

Result: Not completed

To reveal if the numbers received will be interpreted as a complete phone number or only part of a phone number, enter the numbers in the Phone number field and click Test. The Results field will indicate if the number is or is not interpreted as complete.

6. In the phone number field, enter a number.
7. Click **Test**. The results of the test will be indicated in the Result field.

HOP-ON NUMBERS

A BOSâNOVA Claro Gateway can be configured to reroute calls from designated Subscriber numbers off of the PSTN and onto the BOSâNOVA IP Telephony network. This feature is called Hop-on.

Hop-on numbers are entered in the Numbering Plan Configurator's Local Parameters branch of the specific Claro Gateway that will receive the call.

This topic is relevant to Claro Gateways only.

To add a Hop-on number:

1. From a Claro Gateway's Configurator main menu, select **Numbering Plan**.
2. From the left pane of the Numbering Plan Configurator, expand the **Local Parameters** branch.
3. Select **Hop-on**. The Hop-on table is displayed.
4. Select **Change**. The Hop-on dialog table is displayed.
5. Click **Add**. The Add Hop-on dialog box is displayed.
6. Enter the Subscriber number that will be rerouted off of the PSTN and onto the BOSâNOVA IP Telephony network.

A Hop-on number may be a number that is included in the phone number range assigned to the Claro Gateway. However, in this case the calls will always be terminated on the Claro Gateway.

7. If required, from the Authentication dropdown menu, select an Authentication method. (See "Authentication" on page 210.)
8. If required, configure Automatic Dialing.
   a. Select the **Enable** checkbox.
   b. Enter the phone number on the IP Telephony network to be dialed each time the Hop-on number is rerouted off of the PSTN.
   c. Enter a description of the Automatic Dialing number.
9. Click **OK**. The Hop-on dialog table is displayed.
10. Repeat steps 5–9 for each Hop-on number.
11. Click **OK**. The Hop-on table is displayed.

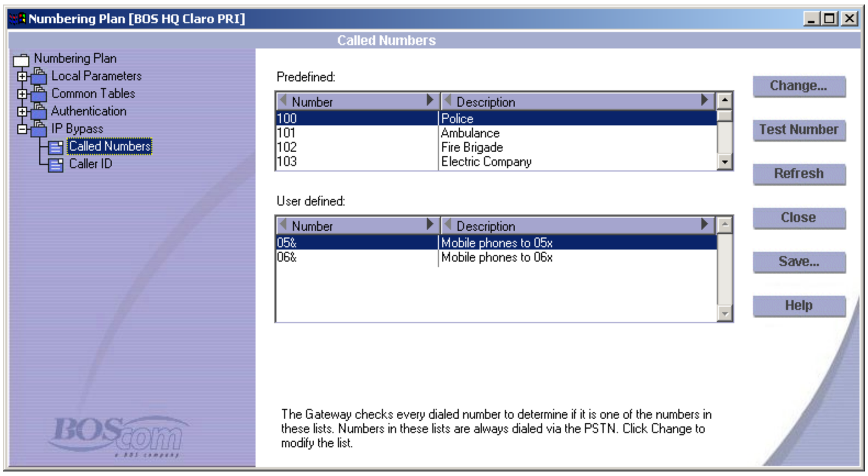
IP BYPASS

IP Bypass numbers and callers are defined in the Claro Gateway's Numbering Plan Configurator. For an explanation of IP Bypass, see p. 106.

This topic is relevant to Claro Gateways only.

Adding an Phone Number to the IP Bypass List

1. In the left pane of the **Numbering Plan Configurator**, expand the **IP Bypass** branch.
2. Select **Called Number**. The **Called Numbers** tables appear.



Predefined:

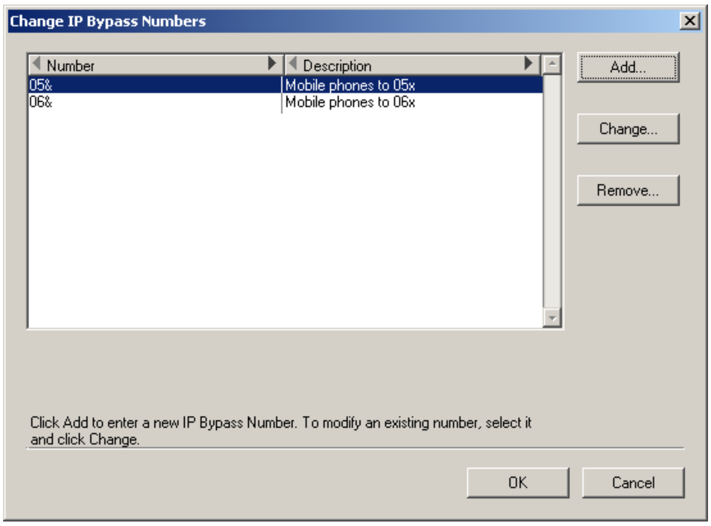
Number	Description
100	Police
101	Ambulance
102	Fire Brigade
103	Electric Company

User defined:

Number	Description
05&	Mobile phones to 05x
06&	Mobile phones to 06x

The Gateway checks every dialed number to determine if it is one of the numbers in these lists. Numbers in these lists are always dialed via the PSTN. Click Change to modify the list.

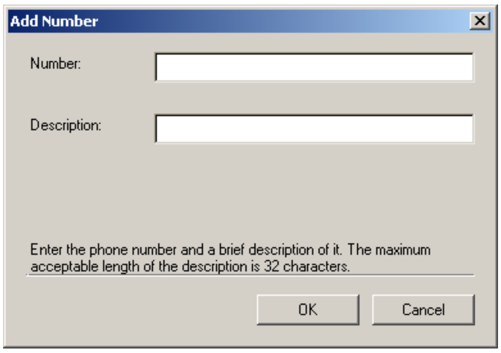
3. Click **Change**. The **Change IP Bypass Numbers** dialog box is displayed.



Number	Description
05&	Mobile phones to 05x
06&	Mobile phones to 06x

Click Add to enter a new IP Bypass Number. To modify an existing number, select it and click Change.

4. Click **Add**. The **Add Number** dialog box is displayed.



Enter the phone number and a brief description of it. The maximum acceptable length of the description is 32 characters.

5. Enter the phone number that will ***never*** be dialed to the IP.

Emergency phone numbers, such as police, fire, and ambulance, are typically included in the IP Bypass Called Numbers list.

6. Enter a description of the IP Bypass phone number. The description can be up to 32 characters in length.
7. Click **OK** twice to return to the Numbering Plan Configurator main screen.

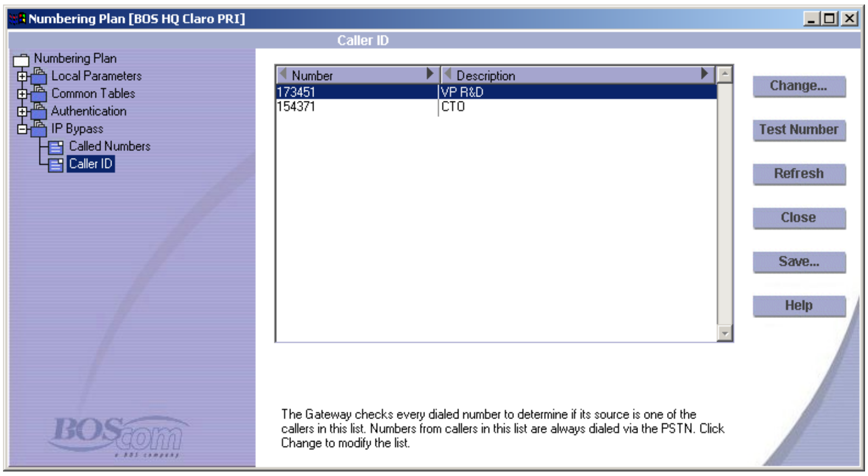
Adding a Caller ID to the IP Bypass List

1. Determine whether the PBX sends extension numbers or Subscriber Numbers to the Claro Gateway. This information should be available from both the PBX manufacturer's technical support department and from the PBX's documentation.

The IP Bypass Caller ID that is entered in step 6 is the user's phone number the Claro Gateway receives from the PBX. Depending on the PBX, this might be only an extension number or might be the complete Subscriber Number.

2. In the left pane of the **Numbering Plan Configurator**, expand the **IP Bypass** branch.

3. Select **Caller ID**. The Caller ID table is displayed.



Number	Description
173451	VP R&D
154371	CTO

The Gateway checks every dialed number to determine if its source is one of the callers in this list. Numbers from callers in this list are always dialed via the PSTN. Click Change to modify the list.

4. Click **Change**. The **Change Caller ID** dialog box is displayed.
5. Click **Add**. The **Add Number** dialog box is displayed.
6. Enter the IP Bypass Caller ID phone number.
7. Enter a description of the IP Bypass Caller ID number. The description can be up to 32 characters in length.
8. Click **OK** twice to return to the Numbering Plan Configurator main screen.

Changing an IP Bypass Phone Number or Caller ID

1. In the left pane of the Numbering Plan Configurator, expand the **IP Bypass** branch.
2. Select either Called Number or Caller ID.
3. Click **Change**. The **Change IP Bypass** dialog box is displayed.
4. Select an IP Bypass phone number or Caller ID from the list.
5. Click **Change**. The **Change Number** dialog box is displayed.
6. Change the IP Bypass phone number or Caller ID.
7. Change the description of the IP Bypass phone number or Caller ID. The description can be up to 50 characters in length.
8. Click **OK** twice to return to the Numbering Plan Configurator main screen.

LEAST COST ROUTING (LCR)

For LCR to function, Uniqueness Check must be disabled. See "Enabling and Disabling the Uniqueness Check" on page 205.

BOSâNOVA Gateways can be configured to route calls:

- only through selected, enabled Gateways, *and*
- only in the order those selected Gateways are listed.

This feature is called Least Cost Routing (LCR). IP Telephony network-wide LCR is configured in the Officer Gateway. For instructions, see "Network-wide Multi-path Priorities" on page 206.

LCR can be implemented per BOSâNOVA Gateway. Configuration is assigned in the Local Parameters branch of each Gateway's Numbering Plan Configurator.

When LCR is implemented locally, the Local Parameters take precedence over the Common Tables. Warnings are posted in the Common Tables of Gateways when LCR is implemented locally.

Configuring LCR per BOSâNOVA Gateway

To configure LCR such that the local Gateway interacts only with selected BOSâNOVA Gateways and only in a specific order:

1. From the Configurator main menu, select **Numbering Plan**.
2. From the left pane of the Numbering Plan Configurator, expand the **Local Parameters** branch.
3. Expand the **Least Cost Routing** sub-branch.
4. Select **BOSâNOVA Hop-off**. The table displays the other Gateways through which the local Gateway can route calls.
5. Click **Change**. The LCR Available Gateway List screen is displayed.

Configuration involves two steps:

a. Import the Gateways.

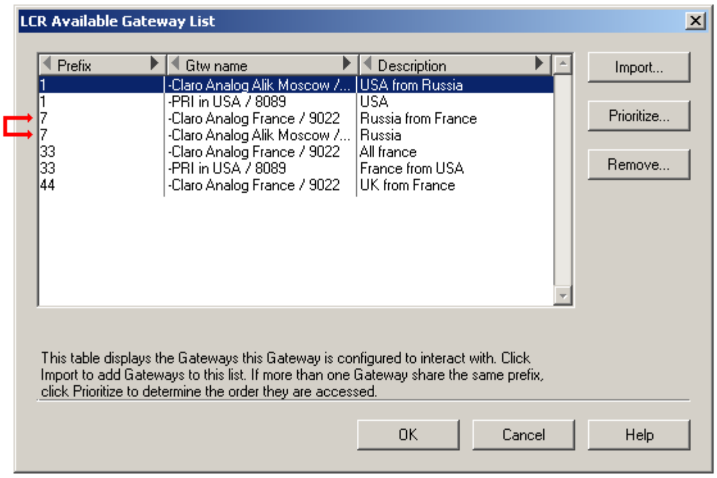
i. From the LCR Available Gateway List screen, click **Import**. The LCR Gateway Import screen is displayed.

ii. Select the Gateways to be imported.

iii. Click **OK**. The LCR Available Gateway List screen is displayed.

b. Prioritize the Gateways.

i. Note which Gateways share the same prefix. Prioritization of Gateways is necessary only for Gateways that share the same prefix.



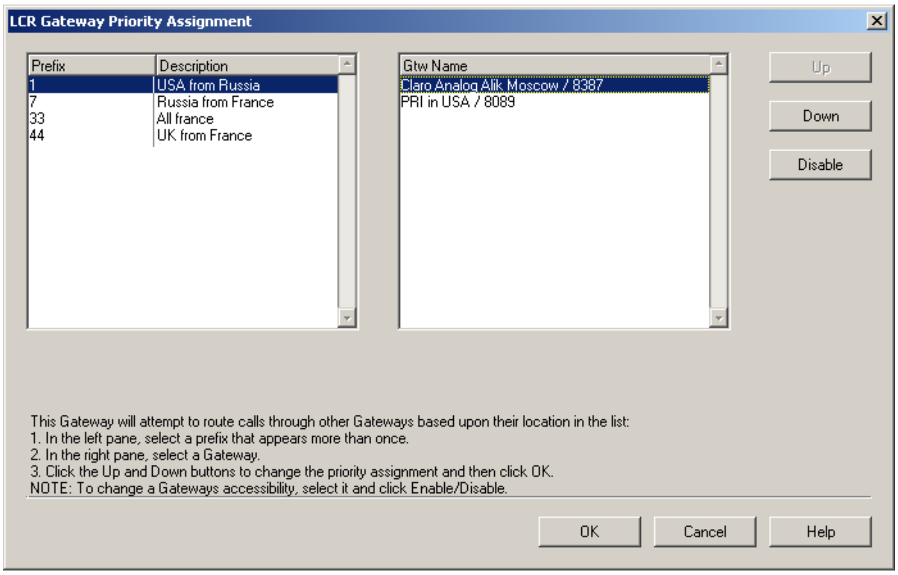
Shared prefix

LCR Available Gateway List

Prefix	Gtw name	Description
1	-Claro Analog Alik Moscow /...	USA from Russia
1	-PRI in USA / 8089	USA
7	-Claro Analog France / 9022	Russia from France
7	-Claro Analog Alik Moscow /...	Russia
33	-Claro Analog France / 9022	All france
33	-PRI in USA / 8089	France from USA
44	-Claro Analog France / 9022	UK from France

This table displays the Gateways this Gateway is configured to interact with. Click Import to add Gateways to this list. If more than one Gateway share the same prefix, click Prioritize to determine the order they are accessed.

ii. From the LCR Available Gateway List screen, click **Prioritize**. The LCR Gateway Priority Assignment screen is displayed.



LCR Gateway Priority Assignment

Prefix	Description
1	USA from Russia
7	Russia from France
33	All france
44	UK from France

Gtw Name
Claro Analog Alik Moscow / 8387
PRI in USA / 8089

This Gateway will attempt to route calls through other Gateways based upon their location in the list:
1. In the left pane, select a prefix that appears more than once.
2. In the right pane, select a Gateway.
3. Click the Up and Down buttons to change the priority assignment and then click OK.
NOTE: To change a Gateways accessibility, select it and click Enable/Disable.

iii. From the left pane, select a hop-off prefix that appears more than once.

iv. In the right pane, select a Gateway.

If the Up and Down buttons are grayed out, the Gateway is not enabled. Click Enable first and then continue with prioritization.

v. Use the Up and Down buttons to assign a position to the selected Gateway.

vi. Click **OK**. The LCR Available Gateway List screen is displayed.

Enabling and Disabling BOSâNOVA Gateways for LCR

To achieve Least Cost Routing, a Gateway may need to be temporarily disabled and, subsequently, enabled.

To disable a Gateway:

1. From the Configurator main menu, select **Numbering Plan**.
2. From the left pane of the Numbering Plan Configurator, expand the **Local Parameters** branch.
3. Expand the **Least Cost Routing** sub-branch.
4. Select **BOSâNOVA Hop-off**. The table displays the other Gateways through which the local Gateway can route calls.
5. Click **Change**. The LCR Available Gateway List screen is displayed.
6. Click **Prioritize**. The LCR Gateway Priority Assignment screen is displayed.
7. From the left pane, select a hop-off prefix that appears more than once.
8. In the right pane, select a Gateway.
9. Click **Disable**.
10. Click **OK**.

Configuring LCR for Third-Party Gateways

To configure LCR such that the local Gateway interacts only with selected third-party Gateways and only in a specific order:

1. From the Configurator main menu, select **Numbering Plan**.
2. From the left pane of the Numbering Plan Configurator, expand the **Local Parameters** branch.
3. Expand the **Least Cost Routing** sub-branch.
4. Select **Third-party Gateways**. The table displays information about the other third-party Gateways through which the local Gateway can route calls.
5. Click **Change**. The LCR Third-party Gateways Tables screen is displayed. Configuration involves the following steps:

   a. Add, or import, the Gateways.

For instructions regarding adding third-party gateways, see "Third Party Gateways" on page 189.

To import third-party gateways that are already configured on the IP Telephony network:

i. Click **Import**. The LCR Third-party Gateway Import screen is displayed.

ii. Select the Gateways to be imported.

iii. Click **OK**. The LCR Third-party Gateways Tables screen is displayed.

b. Configure the masks. For an explanation of masks, see "What is a Mask?" on page 191.

c. Prioritize the Gateways.

i. From the LCR Third-party Gateways Tables screen, click **Prioritize**. The LCR Third-party Gateway Priority Assignment screen is displayed.

ii. From the left pane, select a mask. The gateways sharing that mask are displayed in the right pane.

iii. In the right pane, select a gateway.

iv. Use the Up and Down buttons to assign a position to the selected Gateway.

v. Click **OK**. The LCR Third-party Gateways Tables screen is displayed.

Enabling and Disabling Third-party Gateways for LCR

To achieve Least Cost Routing, a Gateway may need to be temporarily disabled and, subsequently, enabled.

To disable a Gateway:

1. From the Configurator main menu, select **Numbering Plan**.
2. From the left pane of the Numbering Plan Configurator, expand the **Local Parameters** branch.
3. Expand the **Least Cost Routing** sub-branch.
4. Select **Third-party Gateways**.
5. Click **Change**.
6. Click **Prioritize**.
7. From the left pane, select a mask.
8. In the right pane, select a Gateway.
9. Click **Disable**.
10. Click **OK**.

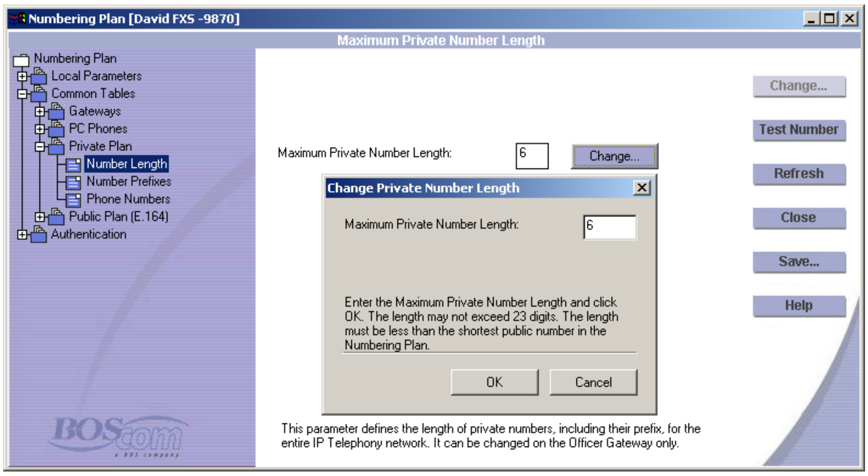
MAXIMUM PRIVATE-NUMBER LENGTH

Maximum private-number length is assigned in the Officer’s Numbering Plan Configurator. For an explanation of maximum private-number length, see page 94.

Maximum private-number length must be shorter than the length of the shortest public number. Length determines whether the Gateways relate to the number as a private-number or as a public-number.

Procedure

1. On the Officer Gateway, from the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, expand the **Common Tables** branch.
3. Select **Private Plan > Number Length**. The **Maximum Private Number Length** field appears in the right pane.



Numbering Plan [David FXS -9870]

Maximum Private Number Length

Maximum Private Number Length: 6

Change Private Number Length

Maximum Private Number Length: 6

Enter the Maximum Private Number Length and click OK. The length may not exceed 23 digits. The length must be less than the shortest public number in the Numbering Plan.

This parameter defines the length of private numbers, including their prefix, for the entire IP Telephony network. It can be changed on the Officer Gateway only.

4. Click **Change**. The **Change Private Number Length** dialog box appears.

If the Change button does not appear, the Gateway is a Private, not an Officer.

5. Enter the maximum private-number length and click **OK**.

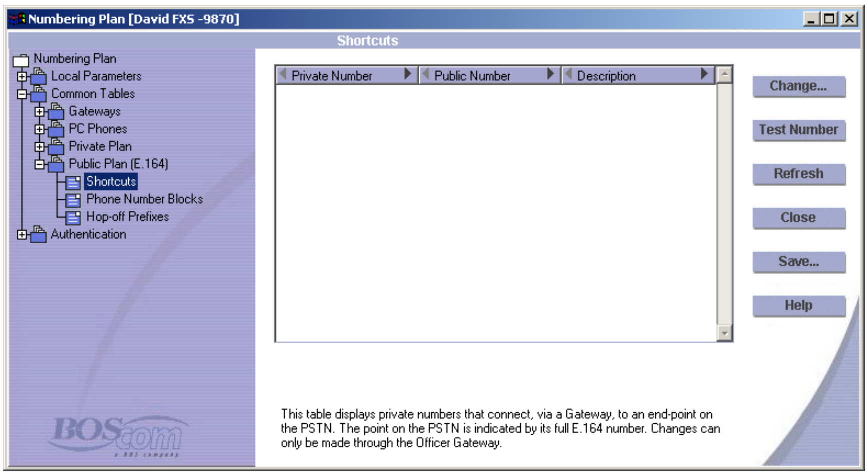
Maximum private-number length is applied when the Gateways receive the updated common dialing table from the Officer.

PRIVATE TO PUBLIC NUMBER ASSOCIATIONS

Private to public number associations are created in the Officer's Numbering Plan Configurator. For an explanation of private to public number associations, see page 103.

Procedure

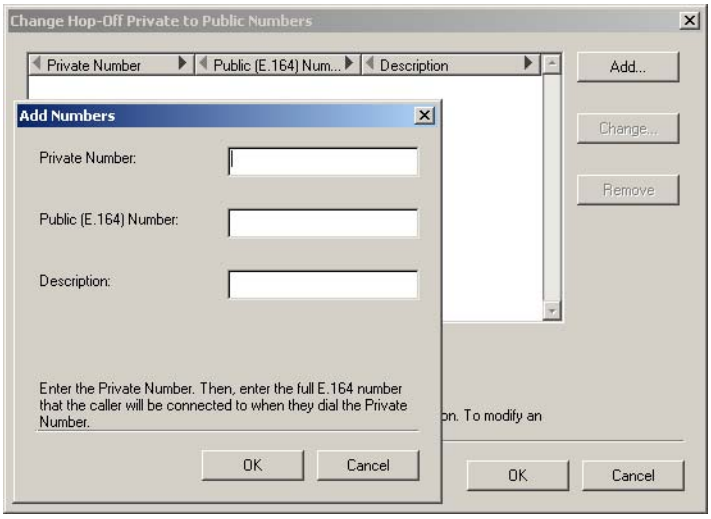
1. On the Officer Gateway, from the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, expand the **Common Tables** branch.
3. Select **Public Plan > Shortcuts**. The **Hop-off Private to Public** table appears.



This table displays private numbers that connect, via a Gateway, to an end-point on the PSTN. The point on the PSTN is indicated by its full E.164 number. Changes can only be made through the Officer Gateway.

4. Click **Change**. The **Change Hop-off Private to Public Numbers** dialog box appears.

5. Click **Add**. The **Add Numbers** dialog box appears.



Enter the Private Number. Then, enter the full E.164 number that the caller will be connected to when they dial the Private Number.

6. Enter the Private Number. This is the number callers will dial.
7. Enter the Public Number, that is, the full public telephone number (based upon the E.164 structure, see p. 83) that will be associated with the private number.
8. Enter a description. The description simplifies later identification. Click **OK**
9. Repeat steps 5–8 until all Private to Public Number associations are entered.
10. Click **OK** to return to the **Numbering Plan Configurator**.

All BOSâNOVA Gateways will be updated when the Officer distributes the updated common dialing table.

RULE BASED NUMBER MANAGEMENT

Rule Based Number Management is configured in the Local Parameters branch of each Gateway's Numbering Plan Configurator. After defining a set of rules, the rules are applied to each port as required.

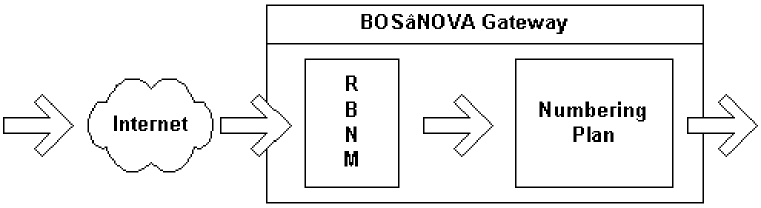
General Comments

The Gateway may need to change numbers in a phone number before forwarding the phone number. Rule Based Number Management (RBNM) is used to change a telephone number into a different number before the call is matched to an inbound destination or before the call is forwarded to an outbound destination. RBNM (also called digit manipulation, number manipulation, digit translation, number transposition) determines the phone number that the Gateway forwards.

Depending upon the type of Gateway, there are either four, six, or eight applications of RBNM. Following are definitions accompanied by an illustration.

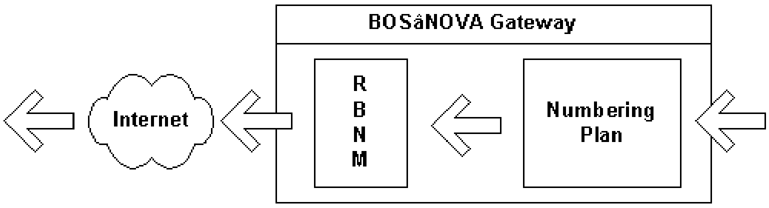
IP to Gateway

These rules convert phone numbers coming from the IP prior to their resolution by the Numbering Plan.



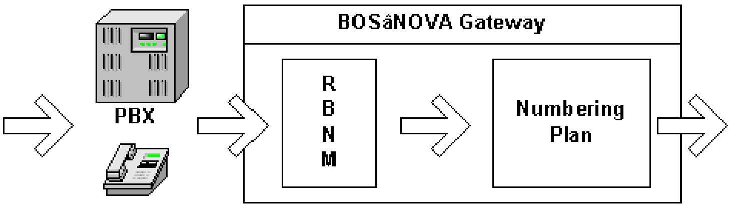
Gateway to IP

These rules convert phone numbers coming from the Gateway prior to their termination elsewhere on the IP.



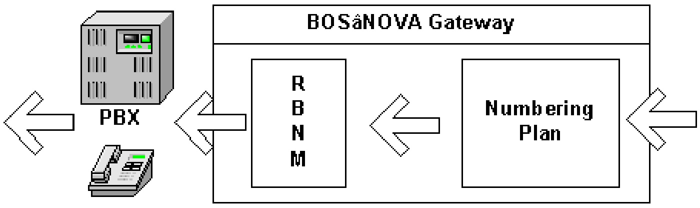
PBX and Phones to Gateway

These rules convert phone numbers coming either from the PBX or telephones prior to their resolution by the Numbering Plan.



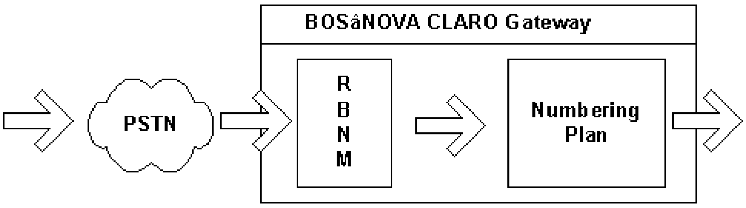
Gateway to PBX and Phones

These rules convert phone numbers coming from the Gateway prior to their termination either by a PBX or a telephone.



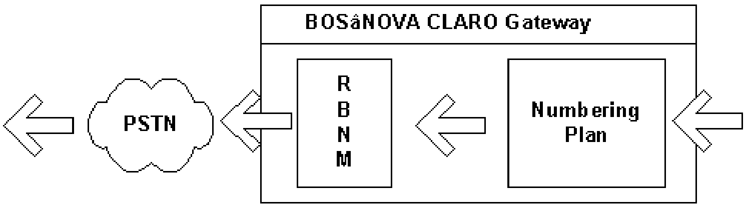
PSTN to Gateway

These rules convert phone numbers coming from the PSTN prior to their resolution by the Numbering Plan of a Claro Gateway.



Gateway to PSTN

These rules convert phone numbers coming from the Claro Gateway prior to their termination on the PSTN.



Examples of RBNM

RBNM would be applied in the following examples:

Gtw-to-PBX Rule

A PBX might be configured to accept only the three last digits of a phone number it receives via the PRI line. In this case, the system administrator must define a rule that will strip the first several digits from the subscriber number that, by default, is dialed by the originating BOSâNOVA Claro Gateway.

The rule "copy only the last three digits of the phone number" is written as: **c-3**

IP-to-Gtw Rule

If the IP call is received from a third-party gateway, it may be necessary to remove a phone number prefix. In the following example, the prefix 1102 is removed from the phone number.

The rule "if the number starts with 1102 then skip 1102 and copy rest of the number" is written as: **s1102ct**

Gtw-to-IP Rule

It may be necessary to add a prefix to a phone number before it is sent to the IP. In the following example, the prefix 1102 is added to the beginning of the phone-number.

The rule "add 1102 to the beginning of the number and copy the rest of the number" is written as: **a1102ct**

PBX-to-Gtw Rule

Background:

In countries with decentralized telecommunication systems, such as the USA and the UK, long distance calls can be placed via different carriers and the carrier can be selected on a per-call base. Each carrier is assigned an identification number. A prefix is dialed before the carrier identification number. That prefix is called the Carrier Selection prefix. In the USA, the carrier selection prefix is 101.

It may be necessary to remove the carrier selection prefix, and associated carrier identification number, from a phone number received from the PBX. In the following example, the carrier selection prefix 101 and associated 4 digit carrier number are removed before the Gateway forwards the call.

The rule "if a number starts with carrier selection prefix 101 then skip it and skip the next 4 digits which are the carrier number, and copy the rest of the number" is written as: **s101s+4ct**

PSTN-to-Gtw Rule

In some cases, the PSTN does not send the complete Subscriber Number to the PBX. For example, if a company has leased a block of phone numbers from the Central Office, beginning with 9907500 and ending with 9907699, the Central Office might send only the last 4 digits to the company's PBX.

Claro Gateways require a complete E.164 number. In this case, the numbers 990 must be added to every call received from the PSTN before the numbering plan can resolve the call.

The rule "add 990 to the beginning of every number received from the PSTN" is written as: **a990ct**

Gtw-to-PSTN Rule

Some countries have more than one International Access Code (IAC), with each IAC being used by a different long-distance carrier. It may be necessary to route calls to specific countries via a specific long-distance carrier. However, users behind the PBX might dial only the default IAC.

The default IAC—for example 00—must be replaced with the IAC of a specific long-distance carrier. In the following example, the IAC of the specific long-distance carrier is 012 and all calls going to the UK are routed through this long-distance carrier. The Country Code of the UK is 44.

The rule "if a number begins with 0044 then skip those numbers, add the number 01244, and copy the rest of the phone number" is written as: **s0044a01244ct**

Caller ID PBX-to-Gateway

To apply Caller ID Authentication, it may be necessary to convert Caller IDs received from a PBX into full E.164 numbers. (See "Authentication for Caller ID Numbers" on page 213.) First, verify the length of the received Caller ID.

The rule "if the Caller ID received from the PBX is three digits long, convert it to the full E.164 number 97249907*nnn*" is written as: **d=3a97249907ct**

Caller ID PSTN-to-Gateway

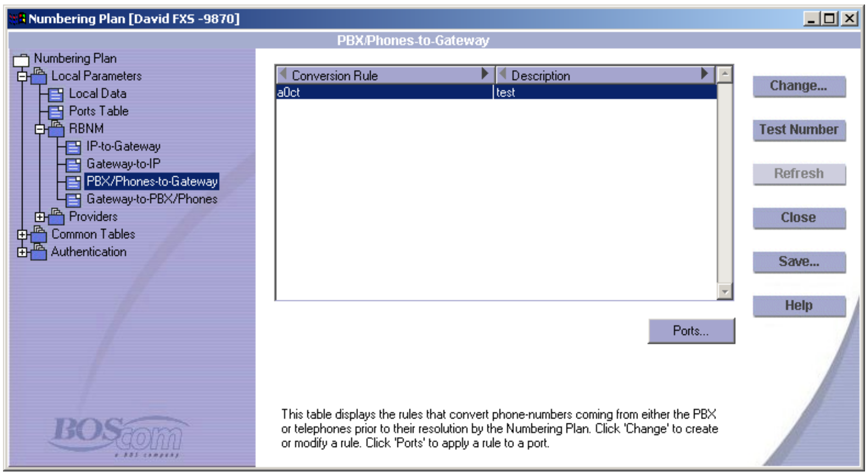
To apply Caller ID Authentication, it may be necessary to convert Caller IDs received from the PSTN into full E.164 numbers. (See "Authentication for Caller ID Numbers" on page 213.) First, verify the length of the received Caller ID.

The rule "if the Caller ID received from the PSTN includes a National Trunk Prefix—for example, 049907510—convert it to the full E.164 number 97249907510" is written as: **d+7s0a972ct**

Creating and Applying RBNM

To create a rule for number management:

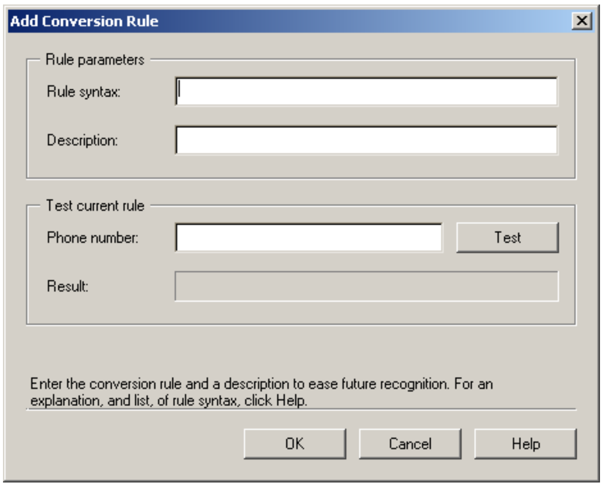
1. Open the Gateway's Configurator.
2. From the Configurator main menu, select **Numbering Plan**.
3. From the Parameters field, expand the Local Parameters branch.
4. From the Parameters field, expand the Rule Based Number Management branch.
5. From the Parameters field, select a call direction relative to the Gateway. The corresponding table appears in the Configuration Field.



Conversion Rule	Description
a0ct	test

This table displays the rules that convert phone-numbers coming from either the PBX or telephones prior to their resolution by the Numbering Plan. Click 'Change' to create or modify a rule. Click 'Ports' to apply a rule to a port.

6. To add a RBNM rule, or to view existing RBNM rules, click **Change**. The corresponding dialog box is displayed.
7. To add a RBNM rule, click **Add**. The Add Conversion Rule dialog box is displayed.



Enter the conversion rule and a description to ease future recognition. For an explanation, and list, of rule syntax, click Help.

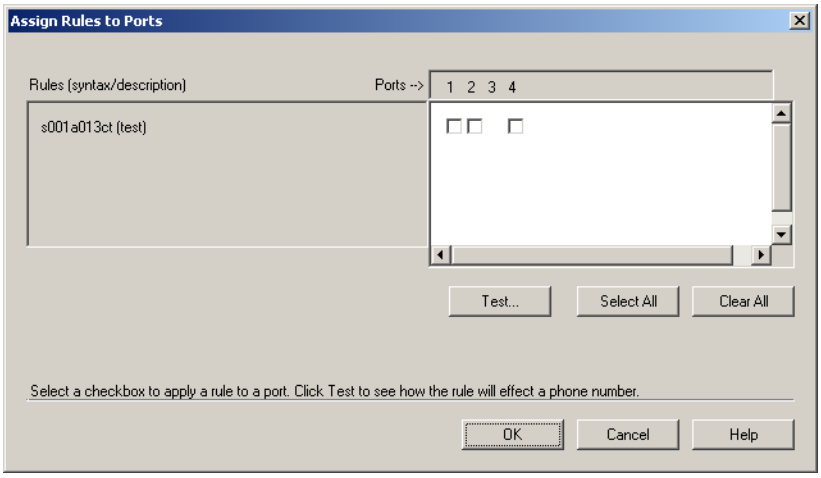
8. Enter the Conversion syntax. For instructions regarding syntax, see Operation Code and Operands.

9. Enter a description that will enable easy identification of the rule.
10. Optionally, test the rule by entering a phone-number in the test field and clicking **Test**. Results are displayed in the Results field.
11. Click **OK**. The RBNM rule appears in the Conversion Rule table.
12. Click **OK**. The corresponding table appears in the Configuration Field.

In some cases, the rule must be applied to specific ports before it takes effect.

To apply a rule:

1. Select **Ports**. The Assign Rules to Ports dialog box is displayed.



Select a checkbox to apply a rule to a port. Click Test to see how the rule will effect a phone number.

2. For each rule that is to be applied to a port, select the corresponding checkbox.
3. Optionally, test the rule by clicking **Test** and entering a number in the phone-number field.
4. Click **OK**. The corresponding table appears in the Configuration Field.

Operation Code and Operands for RBNM

Rule Based Number Management (RBNM) is a Boolean function that transforms the source number, designated as <SN>, into the resulting number, designated as <RN>. In this section, originally written by the programmer, RBNM is called Number Transformation and is abbreviated as NT.

NT consists of a series of conversions. The conversions are performed one after the other until the entire series is exhausted. NT returns true if all conversions are returned true. When NT returns false, it means that the source number did not match the current NT.

Use the following operation code when configuring RBNM.   Operands are described in the following subsection.

SKIP

SKIP, indicated with a lower-case **s**, moves the pointer in the <SN> ahead according to the operand. Thus, the <RN> remains unchanged during this conversion.

Following is the behavior of SKIP per operand specified:

- If the operand is <Number> and the <Number> is first sub-string of the <SN>, then the pointer in the <SN> is moved ahead for string length <Number>.
- If the operand is <Wild Number> and <SN> starts with digits that respectively match the symbols of the <Wild Number>, then the pointer in the <SN> is moved ahead for string length <Wild Number>.
- If the operand is <Number of digits>, then the pointer in the <SN> is moved ahead that number.   In this case, the <Number of digits> must be positive.
- If the operand is <Tail>, then the pointer in the <SN> is moved to the end of the string.

COPY

COPY, indicated with a lower-case **c**, copies the specified number of digits from the <SN> to the <RN>. The pointer in the <SN> is moved ahead depending on the operand.

Following is the behavior of COPY per operand specified:

- If the operand is <Number> and the <Number> is the first sub-string of the <SN>, then it is copied from the <SN> and appended to the <RN>. In this case, the return value is true.   However, if the <Number> is not the first sub-string of the <SN>, then the return value is false.

- If the operand is <Wild Number> and the <SN> starts with digits that respectively match the symbols of the <Wild Number>, then the corresponding part of <SN> is appended to the <RN> and the return value is true. If the <SN> does not start with the <Wild Number>, then the return value is false.
- If the operand is <Number of digits> and it is positive, then the first <Number of digits> of the <SN> are appended to <RN> and the return value is true. If the <Number of digits> is longer than the string length of the <SN>, then the return value is false.
- If the operand is <Number of digits> and it is negative, then the last <Number of digits> of the <SN> are appended to the <RN> and the return value is true. If the <Number of digits> is longer than the string length of the <SN>, then the return value is false.
- If the operand is <Tail>, then the remaining part of the <SN> is appended to the <RN>. The return value is true.

ADD

ADD, indicated with a lower-case **a**, appends the <Number> specified to the <RN>. The pointer in the <SN> is not moved. No other operands are applicable to this operation code. The return value is true.

DIGITS COUNT

DIGITS COUNT, indicated with a lower-case **d**, restricts the application of the rule to a <SN> with a *specific*, *greater than*, or *less than* number of digits.

- If the return value is true, the rule is applied.
- If the return value is false, the rule is not applied.
- DIGITS COUNT, and the operand following it, must appear as follows:

d+*n*	greater than	If there are more than ***n*** digits in the <SN>, apply the rule which follows
d–*n*	less than	If there are less than ***n*** digits in the <SN>, apply the rule which follows
d=*n*	exactly	If the <SN> is exactly ***n*** digits, apply the rule which follows

Formal Operand Definition for RBNM

Conversion is a Boolean function that receives 3 parameters:
* *the Conversion operand*
* *the current pointer of the <SN>*
* *the <RN>*
Conversion returns true on success and false on failure. It also returns the new pointer of <SN>.

Operand definitions are included in the following formal definition. The formal definition is explained in two additional tables found in the online Help.

<NT> ::= <Conversion> | <NT>

<Conversion> ::= <OpCode> <Operand>

<OpCode> ::= S[KIP] | C[OPY] | A[DD] | D[IGIT COUNT]

<Operand> ::= <Number> | <Wild Number> | <Number of digits> | <Tail>

<Number> ::= <digit> | <Special symbol> | <Number><digit> | <Number> <Special symbol>

<Wild Number> ::= <digit> | <?> | <Wild Number> <digit> | <Wild Number><?>

<Number of digits> ::= <+ | –><digit> | <Number of digits><digit>

<Tail> ::= t

<digit> ::= 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9

<Special symbol> ::= A | B | C | D | P(pause) | F(flash) | * | #

<?> ::= question mark means any digit at that place

SESSION INITIATION PROTOCOL (SIP)

In most cases, initial SIP Proxy configuration occurs upon completion of the Numbering Plan Wizard. See “Configuring SIP Proxy as the Connection Type” on page 153.

Subsequent SIP Proxy configuration, as well as configuration of phone-number Prefixes and Conversion Rules, is performed in the Numbering Plan Configurator.

Designating a SIP Proxy as the Connection Type

To designate that a BOSâNOVA Gateway’s Connection Type will be via a computer running the Session Initiation Protocol:

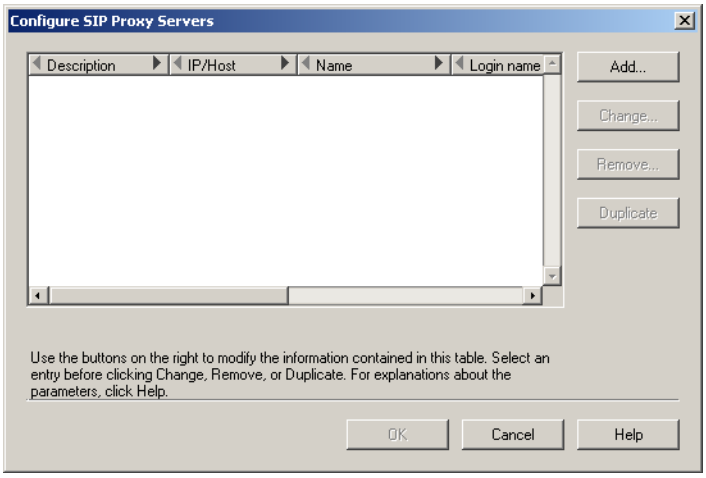
1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, select **Connection Type**.
3. Click **Change**. The Numbering Plan Wizard opens.
4. Click **Next** until arriving at the **Connection Type** page.
5. Select **Session Initiation Protocol (SIP) Proxy**.
6. Complete the Numbering Plan Wizard.
7. On the Review page of the Numbering Plan Wizard, select the **Open the Configure SIP Proxy Configuration dialog box** checkbox.
8. Click **Finish**. The dialog box opens.
9. Continue by defining the parameters of one or more SIP Proxy with which the Gateway will be associated. The procedure is identical to the procedure found on the next page, beginning with step #5.

Configuring SIP Proxy Parameters

Complete this procedure to configure a BOSâNOVA Gateway to operate with one or more SIP Proxies.

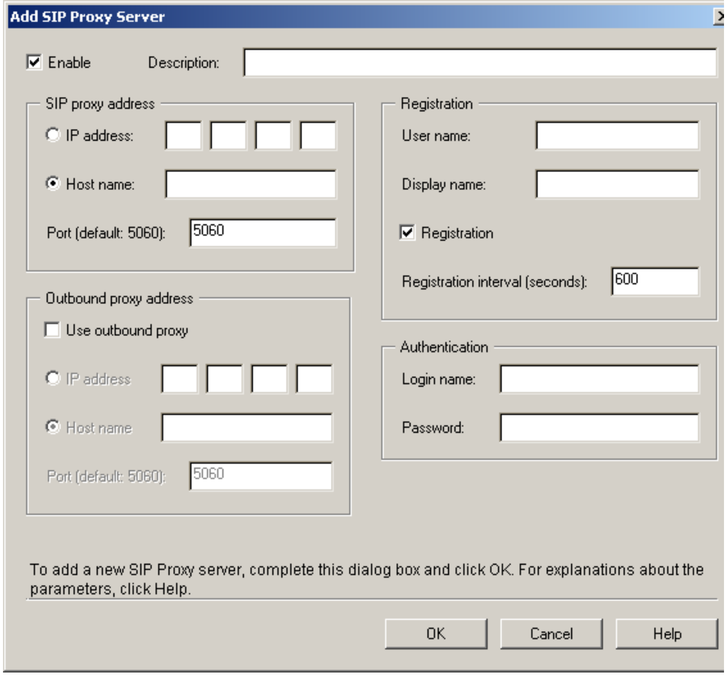
Initial definition of SIP Proxy parameters can occur upon completion of the Numbering Plan Wizard. See step 7 on page 154.

1. From the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, expand the **Connection Type** branch.
3. Select **SIP Proxies List**. The table of configured SIP Proxies appears in the right pane.
4. Click **Change**. The Configure SIP Proxy Servers dialog box is displayed.



Use the buttons on the right to modify the information contained in this table. Select an entry before clicking Change, Remove, or Duplicate. For explanations about the parameters, click Help.

5. Click **Add**. The Add SIP Proxy Server dialog box is displayed.



Add SIP Proxy Server

☑ Enable Description:

SIP proxy address
○ IP address:
● Host name:
Port (default: 5060): 5060

Outbound proxy address
□ Use outbound proxy
○ IP address
● Host name
Port (default: 5060): 5060

Registration
User name:
Display name:
☑ Registration
Registration interval (seconds): 600

Authentication
Login name:
Password:

To add a new SIP Proxy server, complete this dialog box and click OK. For explanations about the parameters, click Help.

6. Complete the fields. Depending upon the configuration determined by the IP Telephony network System Administrator, granting the BOSâNOVA Gateway permission to access the SIP proxy can be either a one-step or a two-step process. If it is a one-step process, only registration is required. If it is a two-step process, authentication is also required.

   All of the following information must be obtained from the IP Telephony network System Administrator.

   a. Enter the IP address, or the Host name, used to access the SIP proxy.

   b. Confirm which UDP port is used. 5060 is the default UDP port used for SIP audio.

   c. If an outbound proxy is used, select the checkbox and enter the IP address or the Host name.

   d. In the Registration field, enter the User name and Display name.

   e. Depending upon the SIP application for the local network architecture, either select or clear the Registration checkbox.

   f. In the Registration interval field, enter a time less than the connection renewal time assigned by the IP Telephony Service Provider.

   g. If authentication is required, enter the login name and the password assigned to you by the IP Telephony network System Administrator. This is the login name the SIP proxy server uses for authentication (via MD5 encryption).

7. Click **OK**. The Add SIP Proxy dialog box closes and the **SIP Proxy Server** dialog box is redisplayed.

8. Repeat steps 5–7 for each SIP Proxy with which this Gateway is to be associated.

9. Click **OK**. The SIP Proxy Server dialog box closes and the Numbering Plan Configurator is displayed.

Adding and Associating Phone Number Prefixes

If there is more than one SIP Proxy associated with the Gateway, calls can be forwarded randomly or can be forwarded to one specific SIP Proxy.

Alternately, calls can be associated with several SIP Proxies and the SIP Proxies can be ranked in order of preference.

The Phone Number Prefix is used to determine which SIP Proxy the Gateway forwards the call to. A phone number prefix can be:

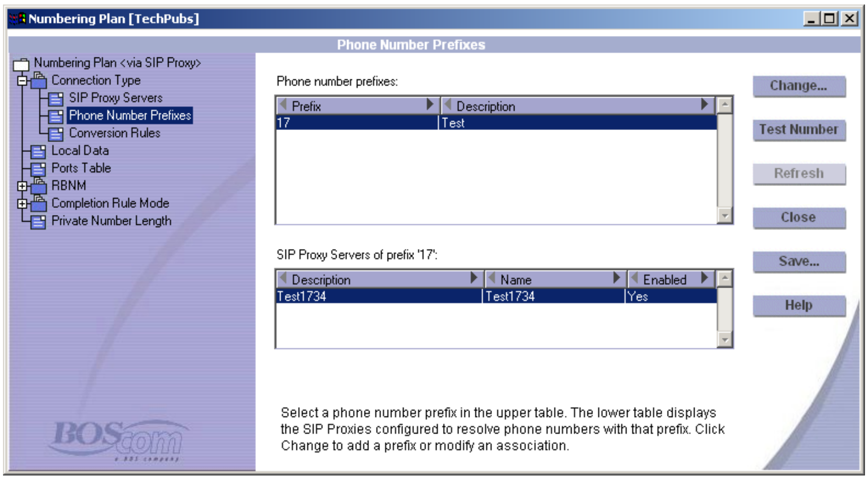
- one or more number appearing at the beginning of a phone number
- additional numbers appended at the beginning of a phone number

To add and associate Phone Number Prefixes:

1. From the Configurator main menu, select **Numbering Plan**.

2. In the left pane of the **Numbering Plan Configurator**, expand the **Connection Type** branch.

3. Select **Phone Number Prefixes**. Two tables are displayed in the Configuration pane. The upper table lists Phone Number Prefixes already defined. The lower table indicates which SIP Proxy the Phone Number Prefix is associated with.



Phone number prefixes:

Prefix	Description
17	Test

SIP Proxy Servers of prefix '17':

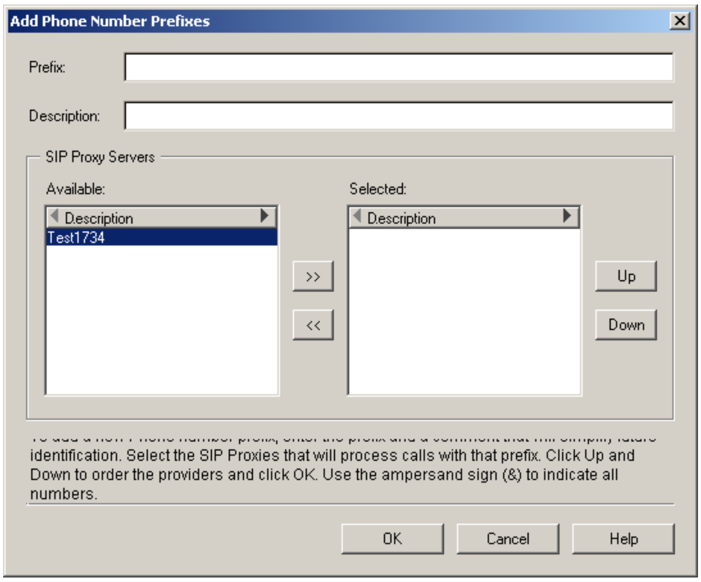
Description	Name	Enabled
Test1734	Test1734	Yes

Select a phone number prefix in the upper table. The lower table displays the SIP Proxies configured to resolve phone numbers with that prefix. Click Change to add a prefix or modify an association.

4. Click **Change**. The Phone Number Prefixes dialog box is displayed. There are three possibilities:

   - To add a prefix:

     i. Click **Add**. The Add Phone Number Prefix dialog box is displayed.



To add a new Phone number prefix, enter the prefix and a comment that will simplify future identification. Select the SIP Proxies that will process calls with that prefix. Click Up and Down to order the providers and click OK. Use the ampersand sign (&) to indicate all numbers.

     ii. Enter the first digits of the telephone number that will be routed via a SIP Proxy. Enter an ampersand (&) if all numbers are to be routed via the SIP Proxy.

     iii. Enter a description of the prefix.

     iv. Select a SIP Proxy from the list of available SIP Proxies.

     v. Click the double-arrows to add the SIP Proxy to the Selected list.

     vi. If necessary, sort the list.

     vii.To finish, click **OK**.

   - To change a prefix, select the prefix, click **Change**, change any of the parameters and click **OK**.

   - To delete a prefix, select the prefix, click **Remove**, and click **Yes** to confirm the decision.

Conversion Rules

Conversion Rules modify specific phone numbers after the GW to IP rules are applied and before the number is sent to the SIP Proxy.

For an overview and instructions regarding Conversion Rule syntax, see "Rule Based Number Management" on page 174.

To add a rule:

1. From the left pane of the Numbering Plan Configurator, expand the Connection Type branch.
2. Select **Conversion Rules**.
3. Click **Change**. The Conversion Rules dialog box is displayed. There are three possibilities:
   - To add a rule:

     i. Click **Add**. The Add SIP Proxy Conversion Rule dialog box opens.

     ii. Enter the rule syntax.

     iii. Enter a description of the rule.

     iv. Select a SIP Proxy from the list of available SIP Proxies.

     v. Click the double-arrows to add the SIP Proxy to the Selected list.

     vi. To finish, click **OK**.
   - To change a rule:

     i. Select the rule.

     ii. Click **Change**.

     iii. Change any of the parameters and click **OK**.
   - To delete a rule:

     i. Select the rule.

     ii. Click **Remove**.
4. Click **Yes** to confirm the decision.

THIRD PARTY GATEWAYS

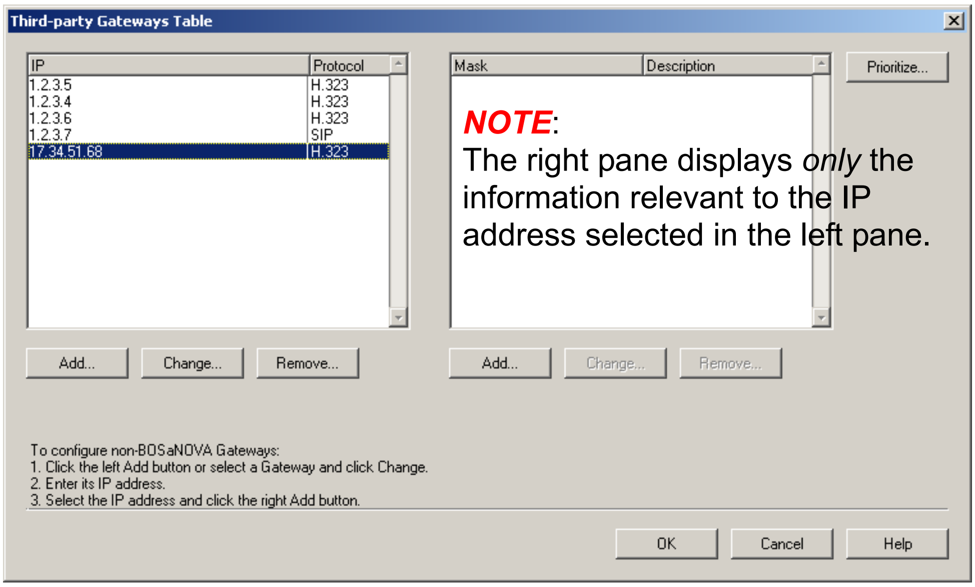
Third-party gateways can be integrated into a BOSâNOVA IP Telephony network. Using the Officer's Numbering Plan Configurator, configure the Officer Gateway to interact with the third party Gateway.

Configure the third-party gateway according to the directions supplied by the manufacturer.

Procedure

To configure the Officer Gateway to interact with the third party gateway:

1. On the Officer Gateway, from the Configurator main menu, select **Numbering Plan**.
2. In the left pane of the **Numbering Plan Configurator**, expand the **Common Tables** branch.
3. Select **Gateways > Third-party Gateways**. The Third-party Gateways table appears in the right pane.
4. Click **Change**. The **Third-party Gateways Table** dialog box opens.



IP	Protocol
1.2.3.5	H.323
1.2.3.4	H.323
1.2.3.6	H.323
1.2.3.7	SIP
17.34.51.68	H.323

Mask	Description

NOTE:
The right pane displays *only* the information relevant to the IP address selected in the left pane.

To configure non-BOSaNOVA Gateways:
1. Click the left Add button or select a Gateway and click Change.
2. Enter its IP address.
3. Select the IP address and click the right Add button.

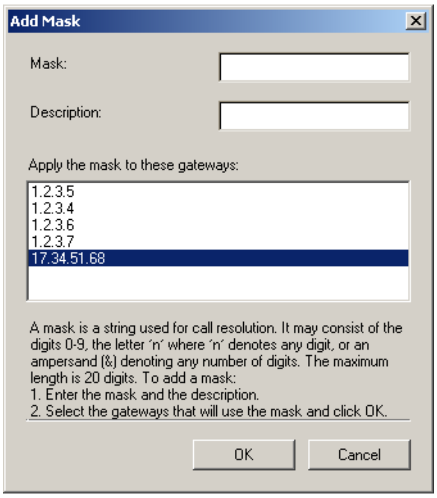
5. Click the left **Add** button. The **Add Gateway** dialog box opens.
6. Enter the IP address of the third-party gateway.
7. Select a preferred protocol, either H.323 or SIP, and click **OK**. (For information on Preferred Protocol, see "Selecting H.323 or SIP" on page 113.)

8. Repeat steps 5–7 for each third-party gateway. Up to 100 third-party gateways can be supported.

When third party gateways are configured ***with*** *masks, complete steps 9–15. When they are configured* ***without*** *masks—for example, when Numbering Plan Authentication is used (see p. 210)—click OK to complete the procedure.*

9. From the left pane, select an IP address. The row changes color when selected.

10. Click the right **Add** button. The **Add Mask** dialog box opens. (See “What is a Mask?” on page 191 for an explanation of masks.)



1.2.3.5
1.2.3.4
1.2.3.6
1.2.3.7
17.34.51.68

A mask is a string used for call resolution. It may consist of the digits 0-9, the letter 'n' where 'n' denotes any digit, or an ampersand (&) denoting any number of digits. The maximum length is 20 digits. To add a mask:
1. Enter the mask and the description.
2. Select the gateways that will use the mask and click OK.

11. Enter the mask and a description. The description simplifies later identification.

12. When required, select the Gateways that will share the mask and click **OK**. The **Third-party Gateways Table** dialog box is displayed.

To prioritize the use of a mask that is shared by more than one third-party gateway, click ***Prioritize****. For more information, see “Network-wide Multi-path Priorities” on page 206.*

13. Repeat steps 10–12 for each mask. Up to 100 masks can be assigned for each third-party gateway.

14. As required, select another IP address and repeat steps 10–13.

15. Click **OK**. The **Third-party Gateways Table** dialog box closes. All BOSâNOVA Gateways will be updated when the Officer distributes the updated common dialing table.

What is a Mask?

The mask can be either:

- Any string of numbers that is assigned to an IP address. The length of a mask must be between 1 and 20 digits. You may assign masks according to any organizational plan you desire. You will receive an error message if there is a conflict between the mask and an existing number.

  When the mask is dialed, the caller will be connected to the recipient available from the gateway at the assigned IP address.
- One or several digits identifying a gateway followed by the letter “n” recurring as often as there are digits in the extensions accessible via that gateway. The letter “n” denotes any number 0, 1, ..., 9. The combined length of the number and the recurrences of the letter “n” cannot exceed 20 characters.
- One or several digits identifying a gateway followed by an ampersand. The ampersand indicates a variable quantity of digits.

  When the mask is dialed, the caller will be connected to the recipient via the gateway at the assigned IP address. The call may progress through either a PBX or the PSTN.

BOSâNOVA Gateways support “best-match” dialing. The Gateway reviews the existing masks and forwards the call via the mask which closest reflects the number dialed.

In the table below, the mask 510 translates directly to the IP address 172.17.2.80. This is the IP address of the gateway of the call recipient.

Mask	IP Address
510	172.17.2.80
21nnn	172.21.45.995
99nnnnnnn	172.17.4.108

In contrast, the mask needed to access a PBX extension via a third-party gateway with the IP address 172.21.45.995 includes:

- The number 21. This indicates the specific gateway with the IP address 172.21.45.995.
- The variables nnn which represent the 3 digit extensions of the parties available via this gateway.

Similarly, the mask needed to access numbers on the PSTN via a third-party gateway able to hop-off calls includes:

- The number 99. This indicates the specific gateway with the IP address 172.17.4.108.
- Seven (7) occasions of the variable n, which represent the seven digits of the public numbers available via this gateway.

THIRD PARTY IP TELEPHONY SERVICE PROVIDERS

A BOSâNOVA Gateway can be configured to route calls to a third party IP Telephony Service Provider. When this is done, the BOSâNOVA Gateway operates behind the scenes and the IP Telephony Service Provider maintains all services, most typically, billing.

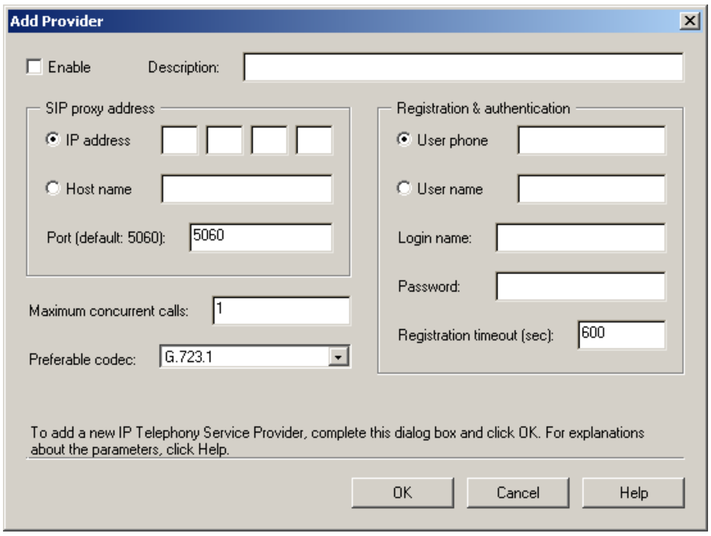
Third Party IP Telephony Service Providers are configured in the Local Parameters branch of each Gateway's Numbering Plan Configurator.

Most of the parameters necessary for configuration must be assigned by the IP Telephony Service Provider.

Adding an IP Telephony Service Provider

IP Telephony Service Providers are implemented per Gateway. To add an IP Telephony Service Providers on a Gateway:

1. From the Configurator main menu, select **Numbering Plan**.
2. From the left pane of the Numbering Plan Configurator, expand the **Local Parameters** branch.
3. Expand the **Providers** sub-branch.
4. Select **Parameters**.
5. Click **Change**. The IP Telephony Service Providers dialog box is displayed. There are four possibilities:
   - To add a new IP Telephony Service Provider, click **Add**. The Add Provider dialog box opens.



Add Provider

☐ Enable Description:

SIP proxy address

● IP address

○ Host name

Port (default: 5060): 5060

Maximum concurrent calls: 1

Preferable codec: G.723.1

Registration & authentication

● User phone

○ User name

Login name:

Password:

Registration timeout (sec): 600

To add a new IP Telephony Service Provider, complete this dialog box and click OK. For explanations about the parameters, click Help.

Table 41: Add IP Telephony Service Provider Parameters

Parameter	Definition
Enable	When selected, this Gateway can route calls to this IP Telephony Service Provider.
Description	Enter the name or a description of the IP Telephony Service Provider.
SIP Proxy* - IP address	When selected, the IP Telephony Service Provider is accessed via this IP address. Enter the IP address.
SIP Proxy* - Host name	When selected, the IP Telephony Service Provider is accessed via this Host name. Enter the Host name.
Port	5060 is the default UDP IP port number used for SIP audio and video.
Maximum concurrent calls	Enter the maximum number of calls the Gateway, using this account, is allowed to route to the IP Telephony Service Provider.
Preferable codec	Select the codec this Gateway prefers to use when sending IP packets to the IP Telephony Service Provider.
User phone	When selected, this Gateway registers with the IP Telephony Service Provider using this phone number. Enter the phone number.
User name	When selected, this Gateway registers with the IP Telephony Service Provider using this assigned name. Enter the name.
Login name	Enter the assigned login name the Gateway uses to identify itself to the SIP Proxy server.
Password	Enter the assigned password the Gateway uses to identify itself to the SIP Proxy server.
Registration timeout	Enter a time **less than** the connection renewal time assigned by the IP Telephony Service Provider.
* A Session Initiation Protocol (SIP) proxy server is an intermediate component usually located between a SIP enabled IP Telephony Service Provider and the Internet. The SIP proxy is responsible for routing and delivering all calls to the SIP IP Telephony Service Provider.	

- To change an IP Telephony Service Provider, first select the IP Telephony Service Provider and then click Change.
- To delete an IP Telephony Service Provider, first select the IP Telephony Service Provider and then click Remove.
- To duplicate an IP Telephony Service Provider, first select the IP Telephony Service Provider and then click Duplicate.

6. Click **OK**. The IP Telephony Service Providers dialog box is displayed.
7. To finish, click **OK**.

Adding a Prefix

A prefix can be any number of digits from the beginning of an E.164 telephone number. When a prefix is associated with a third party IP Telephony Service Provider, the Gateway routes all calls beginning with the prefix to that Provider.

To add a prefix:

1. From the left pane of the Numbering Plan Configurator, expand the Local Parameters branch.
2. Expand the Provider sub-branch.
3. Select **Prefixes**.
4. Click **Change**. The Provider Prefixes dialog box is displayed. There are three possibilities:
   - To add a prefix:
     i. Click **Add**. The Add Provider Prefix dialog box opens.
     ii. Enter the first digits of the E.164 telephone number that will be routed via a third party IP Telephony Service Provider. Enter an ampersand (&) if all numbers are to be routed via the provider.
     iii. Enter a description of the prefix.
     iv. Select an IP Telephony Service Provider from the list of available providers.
     v. Click the double-arrows to add the provider to the Selected list and, if necessary, sort the list.
     vi. To finish, click **OK**.
   - To change a prefix, select the prefix, click **Change**, change any of the parameters and click **OK**.
   - To delete a prefix, select the prefix, click **Remove**, and click **Yes** to confirm the decision.

Adding a RBNM Rule

Rule Based Number Management (RBNM) modifies specific phone numbers before they are sent to the Provider. For an overview and instructions regarding RBNM syntax, see “Rule Based Number Management” on page 174.

To add a rule:

1. From the left pane of the Numbering Plan Configurator, expand the Local Parameters branch.
2. Expand the Provider sub-branch.
3. Select **Rules**.
4. Click **Change**. The Provider Rules dialog box is displayed. There are three possibilities:
    - To add a rule:
        i. Click **Add**. The Add Provider Rule dialog box opens.
        ii. Enter the rule syntax.
        iii. Enter a description of the rule.
        iv. Select an IP Telephony Service Provider from the list of available providers.
        v. Click the double-arrows to add the provider to the Selected list.
        vi. To finish, click **OK**.
    - To change a rule:
        i. Select the rule.
        ii. Click **Change**.
        iii. Change any of the parameters and click **OK**.
    - To delete a rule:
        i. Select the rule.
        ii. Click **Remove**.
        iii. Click **Yes** to confirm the decision.

IP Telephony...
Clear and Simple

SECTION 11: MISCELLANEOUS ASPECTS OF THE NUMBERING PLAN MODULE

This section explains aspects of the numbering plan module that are not directly related to numbering plan configuration. These include:

- Verifying changes to the Numbering Plan, see p. 198
- Using the **Test** button to review the Numbering Plan, see p. 200
- How the Gateways accept phone-numbers, see p. 201

An overview of the BOSâNOVA Gateways Numbering Plan and in-depth explanations of each aspect of the numbering plan are provided in the section "Numbering Plan Overview" beginning on page 80.

Procedures begin on page 108.

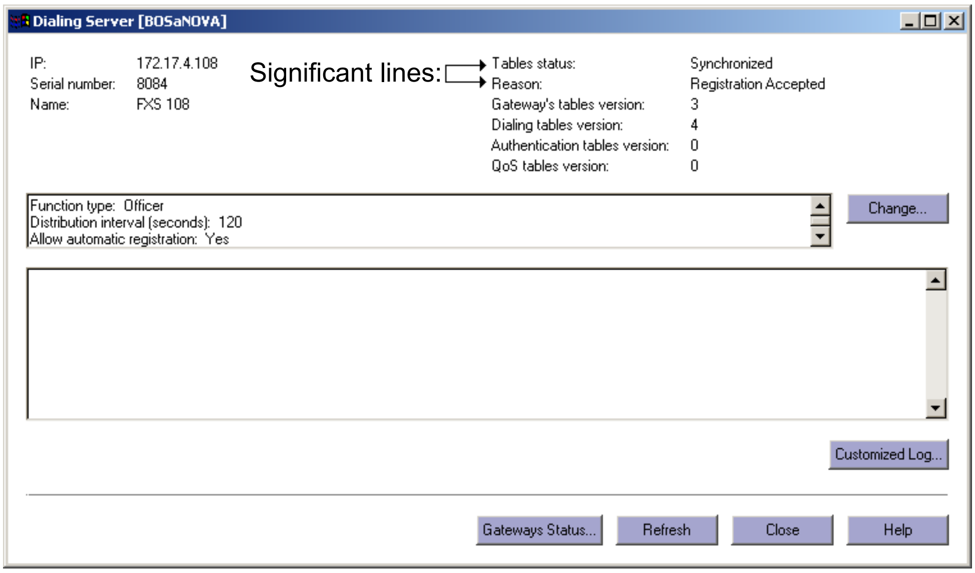
VERIFYING A NUMBERING PLAN

A new Gateway's numbering plan, and changes to an existing numbering plan, must be validated by the Officer. The Gateway's Dialing Server displays whether the changes are accepted or rejected.

A summary of all Gateways is displayed only in the Officer's Dialing Server.

To determine whether numbering plan changes were accepted or rejected:

1. Open the BOSâNOVA Gateway Configurator.
2. From the main menu, select **Dialing Server**. The **Dialing Server** opens.
3. Locate **Dialing tables status** and **Reason** in the upper right of the **Dialing Server** screen.



Dialing Server [BOSaNOVA]

IP: 172.17.4.108
Serial number: 8084
Name: FXS 108

Significant lines:

Tables status: Synchronized
Reason: Registration Accepted
Gateway's tables version: 3
Dialing tables version: 4
Authentication tables version: 0
QoS tables version: 0

Function type: Officer
Distribution interval (seconds): 120
Allow automatic registration: Yes

If the changes were accepted, the Dialing tables status will be **Synchronized** and the Reason status will be **Registration accepted**.

If the status is **Not synchronized** and the Reason status is **Registrations rejected**, a detailed explanation will appear in the log messages. Possibilities include:

- If the log message indicates that the rejection was due to a phone number conflict, then the user must correct the numbering plan configuration and eliminate the conflict.
- If the log message indicates that the rejection was due to a software version mismatch, then the user must update the software version on either the Officer or the Private Gateway.

The following two tables list the possible status messages:

Table 42: Dialing Tables Status

Not Configured	The Gateway's dialing table is not complete
Synchronized	The Gateway's local dialing table matches the common dialing table distributed by the Officer
Not Synchronized	The Gateway's local dialing table does not match the common dialing table distributed by the Officer. This commonly occurs after changes are made to the local dialing table but before registration with the Officer.
Invalid Configuration	This may occur at startup when changes were made manually to a Gateway's configuration files. It indicates a conflict between the Gateway's local dialing table and the information contained in the common dialing table. This status is not a result of negotiation with the Officer. The administrator should manually correct the settings that he never should have touched in the first place.

Table 43: Reasons

Registration sent	This message appears after changes to a numbering plan are sent to the Officer but before the Gateway receives a response from the Officer.
Registration rejected	The Gateway's local dialing table was rejected by the Officer.
Officer is off-line	The Gateway could not connect to the Officer.
Invalid Officer IP	The Officer IP address listed by the Gateway does not correspond with the actual network Officer IP address.
Registration accepted	The Gateway's local dialing table was accepted by the Officer and incorporated into the common dialing table.
Officer IP undefined	An Officer IP address has not been entered for this Gateway.

USING THE TEST BUTTON

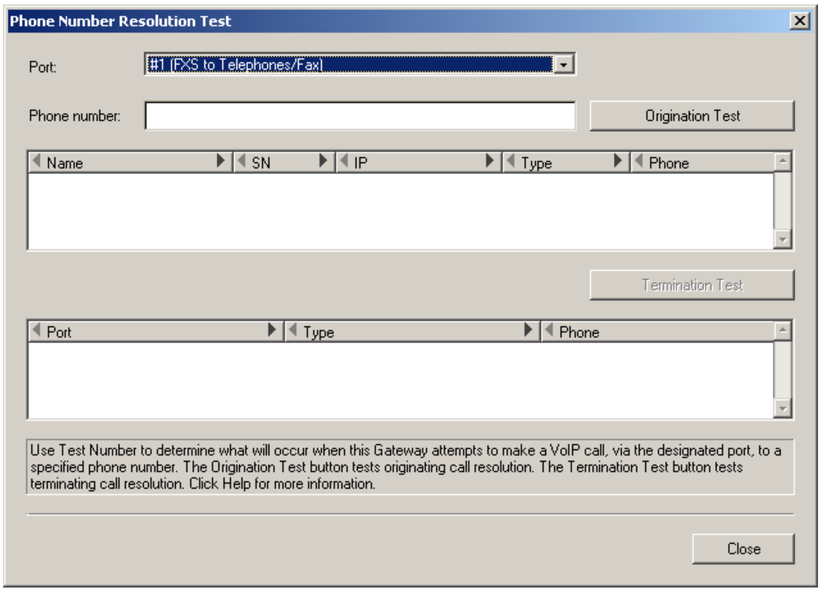
The **Test** button is a Gateway tool that can be used to ascertain what occurs after dialing a specific phone number via a specific port of the Gateway. Amongst other things, the readout reveals:

- IP Telephony network Gateways that could receive the call
- The actual number sent after the originating Gateway applies any relevant rules
- Whether the received number would be understood as a Hop-off call or a Private Number
- The actual number dialed by the terminating Gateway after it applies any relevant rules

The test simulates what occurs when the number is dialed from the specific Gateway, that is, the Gateway whose Configurator is open. The same number, when dialed from another Gateway, may produce different results.

To test a number:

1. Open the BOSâNOVA Gateway Configurator.
2. From the main menu, select **Numbering Plan**.
3. Click **Test Number**. The **Phone Number Resolution Test** dialog box opens.



Port: #1 (FXS to Telephones/Fax)

Use Test Number to determine what will occur when this Gateway attempts to make a VoIP call, via the designated port, to a specified phone number. The Origination Test button tests originating call resolution. The Termination Test button tests terminating call resolution. Click Help for more information.

4. From the dropdown list, choose the specific port that is to be tested.
5. In the Phone number field, enter the phone number that is to be tested.

6. Click **Origination Test**. The results of this test reveal:
   - the IP Telephony network Gateways that can receive the call
   - information about those Gateways
   - the phone number those Gateways would receive after all rules have been applied
7. Choose one of the Gateways. The results of the second test will reveal how the ***selected*** Gateway resolves the phone number.

Ensure that the selected Gateway is accessible—via the IP network—from the computer on which the Gateway Configurator is running. The Destination Test will not work if the Gateway is not accessible.

8. Click **Destination Test**. The results of this test reveal:
   - the Gateway port that the call would pass through
   - whether the number received is understood to be a Hop-off Number (and, therefore, will be redirected onto the PSTN) or if it is considered a Private Number
   - the phone number dialed after all rules have been applied
9. Click **Close**.

HOW GATEWAYS ACCEPT PHONE NUMBERS

The phrase "accepting a phone number" refers to the process whereby the Gateway determines that the user has finished dialing the phone number. Once the Gateway determines that the user has finished dialing the phone number, it accepts the number and begins to analyze it.

Gateways accept phone numbers either:

- automatically, via inter-digit time-out, or
- manually, by pressing # (the pound key).

Inter-digit Time-out

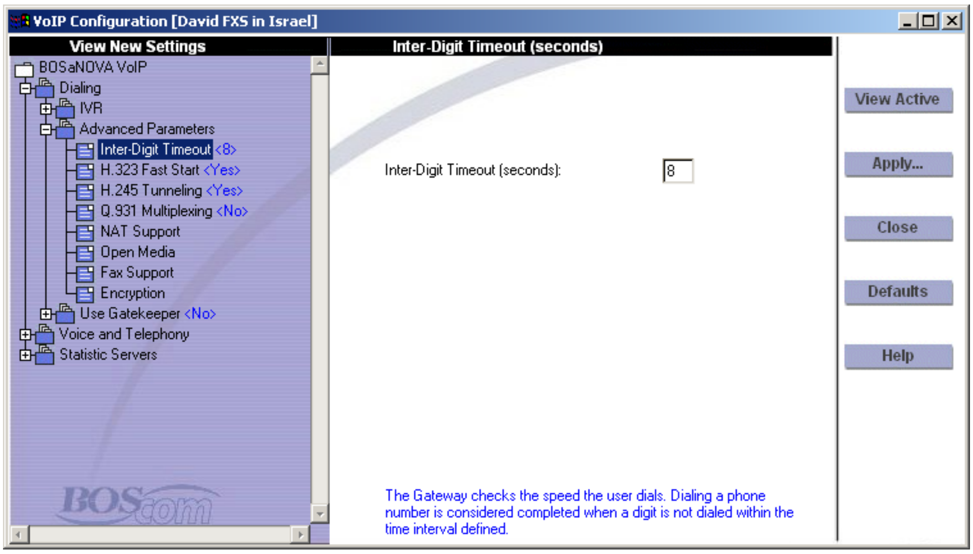
Inter-digit time-out is the maximum period of seconds a user can delay between each of the digits of a phone number. The Gateway waits that period before concluding that the user has finished dialing and accepting the number.

By default, Inter-Digit Time-out is set at 5 seconds.

If the user dials quickly, BOSâNOVA Gateways automatically reduce the inter-digit time-out. For example, if Inter-Digit Time-out is set at 5 seconds, the actual delay can be as short as 3 seconds.

To set the inter-digit time-out:

1. Open the BOSâNOVA Gateway Configurator.
2. From the main menu, select **VoIP Configuration**.
3. Expand the **Dialing** branch.
4. Expand the **Advanced Parameters** branch.
5. Select **Inter-Digit Time-out**. The Inter-Digit Time-out screen appears.



VoIP Configuration [David FXS in Israel]

Inter-Digit Timeout (seconds)

Inter-Digit Timeout (seconds): 8

The Gateway checks the speed the user dials. Dialing a phone number is considered completed when a digit is not dialed within the time interval defined.

6. Enter the period of seconds that the Gateway will wait. The shortest period is 1 second; the longest period is 20 seconds.
7. Click **Apply**. The Gateway does not need to be rebooted.

SECTION 12:
USING THE OFFICER GATEWAY

If a Gatekeeper is not used, one Gateway on a BOSâNOVA IP Telephony network is designated “Officer.” This section describes:

- Responsibilities of the Officer, see p. 204
- Configuring Uniqueness Check and Multi-path routing, see p. 205
- Configuring Private Number Length, see p. 210
- Configuring Authentication, see p. 210
- Dialing Server Functions
    - Assigning a Gateway the Officer function, see p. 218
    - Changing Officers, see p. 219
    - Adding a new Private, see p. 220
    - Reviewing Gateways Synchronization Status from the Officer, see p. 221
    - Explanations of Synchronization Status screen Legend Entries, see Table 44 on page 222
    - Updating Common Dialing Tables, see p. 224
    - Customize Log, see p. 225

An overview of the BOSâNOVA Gateways Numbering Plan and in-depth explanations of each aspect of the numbering plan are provided in the section “Numbering Plan Overview” beginning on page 80.
Procedures begin on page 108.

RESPONSIBILITIES OF THE OFFICER

The Officer fulfills these functions:

- **Numbering Plan Update**
  All Gateways on the IP Telephony network keep an up-to-date version of the entire numbering plan. The Officer maintains the numbering plan and, periodically, distributes it to the other Gateways. If the Officer cannot connect to a Gateway, it retries according to the following schedule:
  - three attempts with a 2 minute interval
  - three attempts with a 5 minutes interval
  - three attempts with a 1 hour interval
  - unrestricted number of attempts with a one day interval
- **Validation**
  The Officer validates changes or additions to the numbering plan. Changes or additions that would cause a conflict are rejected and returned to the originating Gateway.
- **Uniqueness Check and Multi-path Routing**
  A BOSâNOVA IP Telephony network can be configured to route calls either through unique, designated paths or be designed to allow the routing of calls through a number of available paths. Uniqueness Check, available only from the Officer Gateway, must be disabled before multi-route and least cost routing can function. Network applied, general, multi-path routing priorities are also set in the Officer.
- **Maximum Private Number Length**
  Maximum Private number length for the entire IP Telephony network is set by the Officer. The Officer distributes the maximum Private number length to all the other Gateways.
- **Integrating BOSâNOVA Connects**
  BOSâNOVA Connects can be added to an IP Telephony network only via the Officer Gateway. See “Configuring a BOSâNOVA Connect with an Officer” on page 246.
- **Integrating BOSâNOVA Link & Talks**
  BOSâNOVA Link & Talks can be added to an IP Telephony network only via the Officer Gateway. See “Link & Talk and the Officer Gateway” on page 252.
- **Authentication**
  Numbering Plan and Hop-off ID Authentication are managed by the Officer Gateway. The Officer distributes these rules to all Private Gateways on the IP Telephony network via the Common dialing tables. See p. 210.

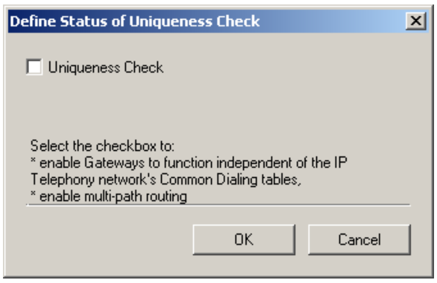
ENABLING AND DISABLING THE UNIQUENESS CHECK

When Uniqueness Check is disabled:

- individual Gateways can be configured to function independent of the IP Telephony network's Common Dialing Tables.
- more than one Gateway can be assigned the same hop-off prefix or, in the case of third-party gateways, the same mask.

To disable or enable Uniqueness Check:

1. Connect and login to the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan**. The Officer's Numbering Plan Configurator is displayed.
3. Expand the Common Tables branch.
4. In the left pane, select **Uniqueness Check**. The message in the right pane indicates if it is enabled or disabled.
5. To change the status, click **Change**. The Define Status of Uniqueness Check dialog box is displayed.



Define Status of Uniqueness Check

□ Uniqueness Check

Select the checkbox to:
* enable Gateways to function independent of the IP Telephony network's Common Dialing tables,
* enable multi-path routing

6. Select or clear the checkbox and click **OK**. The Officer Gateway does not need to be rebooted.

NETWORK-WIDE MULTI-PATH PRIORITIES

If Uniqueness Check is disabled, Gateways can be configured such that they share the same Hop-off Prefix or, in the case of third-party gateways, the same mask (see “Enabling and Disabling the Uniqueness Check” on page 205). When this occurs, it may be advantageous to prioritize the Gateways. Common reasons to prioritize include:

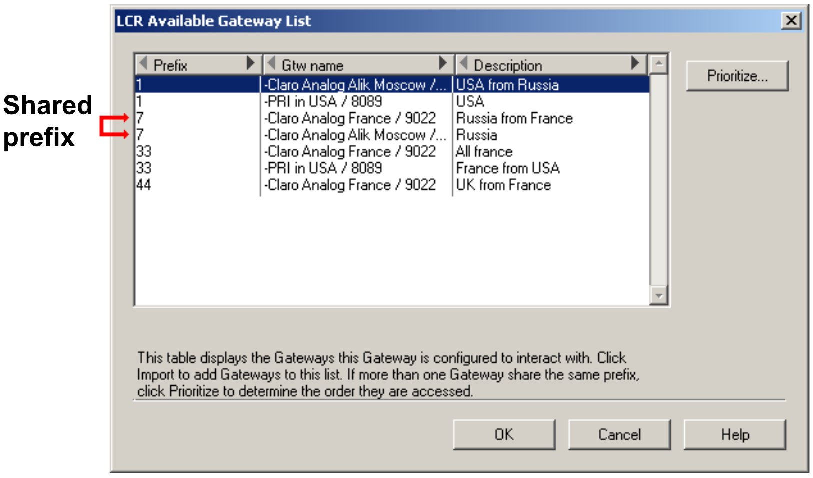
- Least Cost Routing (LCR)
- Recurring bandwidth issues and bottlenecks

This procedure affects all Gateways on the IP Telephony network. Subsequently, Private Gateway LCR definitions can be further configured. See “Least Cost Routing (LCR)” on page 166.

Assigning Hop-off Prefix Priorities

To prioritize Gateways sharing the same Hop-off Prefix:

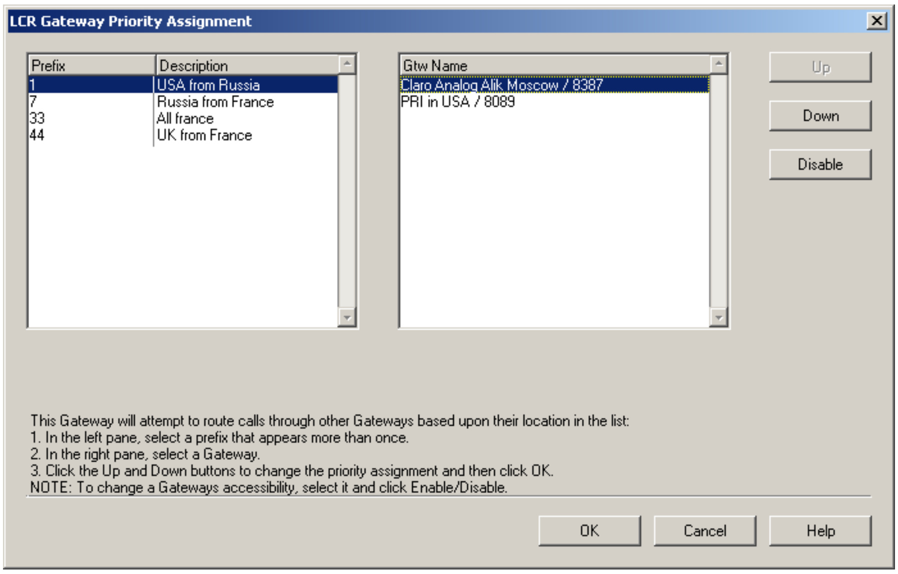
1. Connect and login to the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan**. The Officer’s Numbering Plan Configurator is displayed.
3. Expand the Common Tables branch.
4. Expand the Public Plan (E.164) branch.
5. In the left pane, select **Hop-off Prefixes**. The Hop-off Prefixes Table is displayed in the right pane.
6. Click **Change**. The LCR Available Gateway List is displayed.
7. Note which Gateways share the same prefix. Prioritization of Gateways is necessary only for Gateways that share the same prefix.



Prefix	Gtw name	Description
1	-Claro Analog Alik Moscow /...	USA from Russia
1	-PRI in USA / 8089	USA
7	-Claro Analog France / 9022	Russia from France
7	-Claro Analog Alik Moscow /...	Russia
33	-Claro Analog France / 9022	All france
33	-PRI in USA / 8089	France from USA
44	-Claro Analog France / 9022	UK from France

This table displays the Gateways this Gateway is configured to interact with. Click Import to add Gateways to this list. If more than one Gateway share the same prefix, click Prioritize to determine the order they are accessed.

8. From the LCR Available Gateway List screen, click **Prioritize**. The LCR Gateway Priority Assignment screen is displayed.



Prefix	Description
1	USA from Russia
7	Russia from France
33	All france
44	UK from France

Gtw Name
Claro Analog Alik Moscow / 8387
PRI in USA / 8089

This Gateway will attempt to route calls through other Gateways based upon their location in the list:
1. In the left pane, select a prefix that appears more than once.
2. In the right pane, select a Gateway.
3. Click the Up and Down buttons to change the priority assignment and then click OK.
NOTE: To change a Gateways accessibility, select it and click Enable/Disable.

9. From the left pane, select a hop-off prefix that appears more than once.

10. In the right pane, select a Gateway.

If the Up and Down buttons are grayed out, the Gateway is not enabled. Click Enable first and then continue with prioritization.

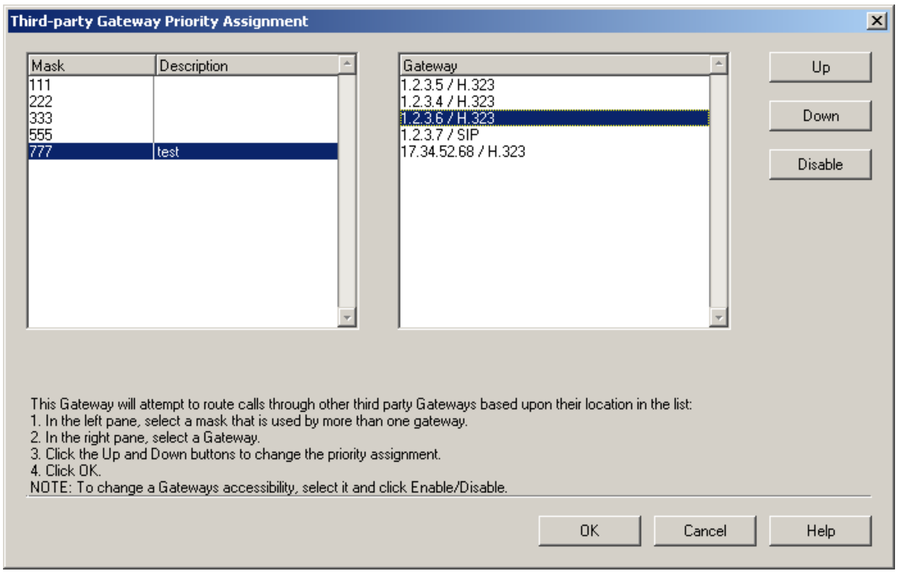
11. Use the Up and Down buttons to assign a position to the selected Gateway.

12. Click **OK**. The LCR Available Gateway List screen is displayed.

Assigning Mask Priorities

To prioritize third-party gateways sharing the same mask:

1. Connect and login to the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan**. The Officer's Numbering Plan Configurator is displayed.
3. Expand the Common Tables branch.
4. Expand the Gateways branch.
5. In the left pane, select **Third-party Gateways**. The Third Party Gateways Table is displayed in the right pane.
6. Click **Change**.
7. Click **Prioritize**. The Third-party Gateway Priority Assignment screen is displayed.
8. From the left pane, select a mask. The third-party gateways sharing that mask are listed according to their current prioritization in the right pane.



Mask	Description
111	
222	
333	
555	
777	test

Gateway
1.2.3.5 / H.323
1.2.3.4 / H.323
1.2.3.6 / H.323
1.2.3.7 / SIP
17.34.52.68 / H.323

This Gateway will attempt to route calls through other third party Gateways based upon their location in the list:
1. In the left pane, select a mask that is used by more than one gateway.
2. In the right pane, select a Gateway.
3. Click the Up and Down buttons to change the priority assignment.
4. Click OK.
NOTE: To change a Gateways accessibility, select it and click Enable/Disable.

9. In the right pane, select a gateway.
10. Use the Up and Down buttons to assign a position to the selected gateway.
11. Click OK. The Third-party Gateways Table screen is displayed.

Enabling and Disabling Gateways for LCR

To achieve IP Telephony network-wide Least Cost Routing, a Gateway may need to be temporarily disabled and, subsequently, enabled.

To disable a Gateway:

1. Connect and login to the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan**. The Officer's Numbering Plan Configurator is displayed.
3. Expand the Common Tables branch. Continue with one of the following:

Disabling Third-party Gateways Sharing a Mask

a. Expand the Gateways branch.

b. In the left pane, select **Third-party Gateways**. The Third-party Gateways Table is displayed in the right pane.

c. Click **Change**.

d. Click **Prioritize**. The Third-party Gateway Priority Assignment screen is displayed.

e. In the left pane, select a Mask.

f. In the right pane, select a Gateway.

g. Click **Disable**.

h. Click **OK**.

Disabling BOSâNOVA Gateways Sharing a Hop-off Prefix

a. Expand the Public Plan (E.164) branch.

b. In the left pane, select **Hop-off Prefixes**. The Hop-off Prefixes Table is displayed in the right pane.

c. Click **Change**. The LCR Available Gateway List is displayed.

d. Click **Prioritize**. The LCR Gateway Priority Assignment screen is displayed.

e. From the left pane, select a hop-off prefix that appears more than once.

f. In the right pane, select a Gateway.

g. Click **Disable**.

h. Click **OK**.

CONFIGURING PRIVATE NUMBER LENGTH

1. Connect and login to the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan**. The Officer's Numbering Plan Configurator is displayed.
3. Expand the Common Tables branch and click **Private Plan > Number Length**.
4. Enter a quantity from 1 to 23. This defines the length of all private numbers on the IP Telephony network. We recommend no greater than six since most public numbers are seven digits in length.
5. Click **Close**. The Private Number Length is saved and the Configurator main menu is displayed.

AUTHENTICATION

Use Authentication to control access to the IP Telephony network. Authentication is managed by the Officer Gateway. The Officer distributes these rules to all Private Gateways on the IP Telephony network via the Common dialing tables.

There are two types of Authentication:

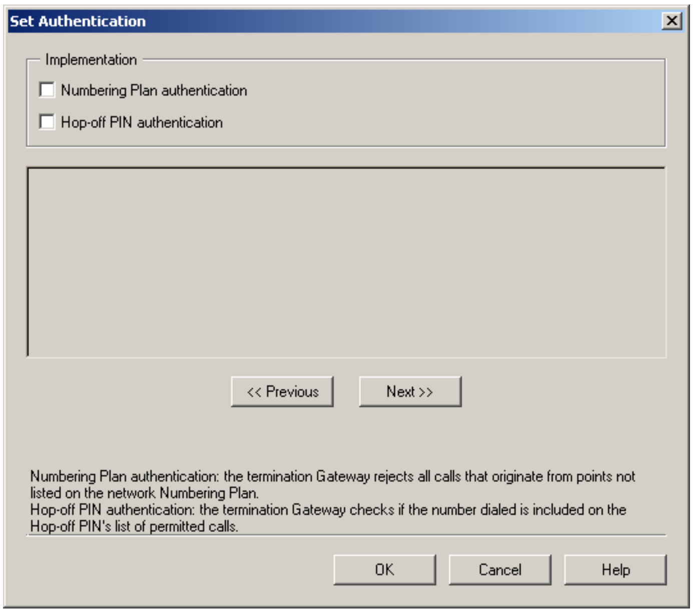
- **Numbering Plan authentication**
  When enabled, the termination Gateway rejects all calls that originate from points not listed on the BOSâNOVA IP Telephony network Numbering Plan. For example, calls from unregistered IP telephones or third-party gateways are rejected.
- **Hop-off ID authentication**
  When enabled, the termination Gateway checks if the number dialed is included on the Hop-off PIN's list of permitted calls. Before enabling Hop-off ID authentication, the BOSâNOVA IP Telephony network administrator must configure hop-off schemes and assign a scheme to each user.

The scenario of authorization messages is active whenever Authentication is implemented. To review the Authorization scenario, see p. 32.

Implementing Authentication

Authentication is implemented per Gateway. To implement Authentication on a Gateway:

1. Connect and login to the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan**. The Officer's Numbering Plan Configurator is displayed.
3. From the left pane of the Numbering Plan Configurator, expand the **Authentication** branch.
4. Select **Implementation**. The Authentication Implementation table is displayed.
5. Click **Set Authentication**. The Set Authentication dialog box is displayed.



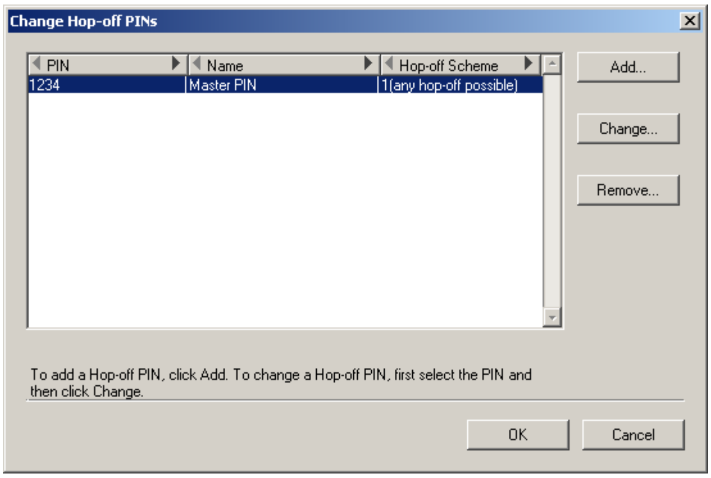
Numbering Plan authentication: the termination Gateway rejects all calls that originate from points not listed on the network Numbering Plan.
Hop-off PIN authentication: the termination Gateway checks if the number dialed is included on the Hop-off PIN's list of permitted calls.

6. Select or clear the checkboxes as required.
7. To perform authentication implementation on another Gateway, click either Previous or Next.
8. To finish, click **OK**.

Adding a PIN to the Hop-off PIN List

Create the Hop-off Scheme before adding a new Hop-off PIN.

1. Connect and login to the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan**. The Officer's Numbering Plan Configurator is displayed.
3. Expand the **Authentication** branch.
4. Select **Hop-off PIN**.
5. Click **Change**. The Change Hop-off PINS dialog box is displayed.



PIN	Name	Hop-off Scheme
1234	Master PIN	1(any hop-off possible)

To add a Hop-off PIN, click Add. To change a Hop-off PIN, first select the PIN and then click Change.

There are three possibilities:

- To add a Hop-off PIN, click **Add**. The Add a PIN dialog box opens. Follow the prompts on the screen.
- To change a Hop-off PIN, first select the PIN and then click **Change**.
- To delete a Hop-off PIN, first select the PIN and then click **Remove**.

Authentication for Caller ID Numbers

When configured, Caller IDs are checked to determine if the Caller ID is authorized to place the call via the BOSâNOVA IP Telephony network. The following three general comments may be helpful:

- Caller ID is a general term which includes all number patterns used to call a telephony end-point.
- Depending on the BOSâNOVA IP Telephony configuration, the Caller ID can be the full E.164 number, a Private number, a PBX extension number, etc.
- Caller IDs can be viewed from the Ports screen of a digital Gateway's Monitor (see "Gateway Ports Monitor" on page 266). The Partner Name column of the Ports screen of an analog Gateway's Monitor occasionally displays the Caller ID.

To configure Authentication for a specific Caller ID:

1. Connect and login to the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan**. The Officer's Numbering Plan Configurator is displayed.
3. Expand the **Authentication** branch.
4. Select **Caller ID**. The Caller ID table is displayed.
5. Click **Change**. The Caller ID dialog box is displayed.
6. Click **Add**. The Add Caller ID dialog box is displayed.
7. Enter the Caller ID. Do not use any hyphens in the number.
8. Enter a descriptive name to help identify the Caller ID number in the various tables it appears in.
9. From the Hop-off Scheme dropdown box, associate a hop-off scheme with the Caller ID. All hop-off calls permitted according to that scheme will be permitted when a call is placed from that Caller ID.
10. Click **OK**. The Caller ID dialog box is displayed.
11. Repeat steps 6–10 for each new Caller ID.
12. Click **OK**. The Caller ID table is displayed.

If configuring a Claro PRI, you may need to add rules to the Caller ID Rule Based Number management table. See p. 177.

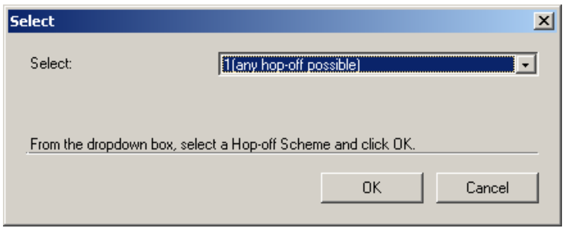
Authentication for BOSâNOVA Connects and Link & Talks

When configured, calls originating from a BOSâNOVA Connect or Link & Talk are checked to determine if the PC Phone is authorized to place the call via the BOSâNOVA IP Telephony network.

*Each PC Phone must be added to the IP Telephony network **before** rules of Authentication are applied to it. See "Configuring a BOSâNOVA Connect with an Officer" on page 246 and "Link & Talk and the Officer Gateway" on page 252.*

To configure Authentication for a PC Phone:

1. Connect and login to the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan**. The Officer's Numbering Plan Configurator is displayed.
3. Expand the **Authentication** branch.
4. Select **PC Phones**.
5. Click **Change**. The Associated Hop-off Schemes dialog box is displayed.
6. From the list of PC Phones already added to the IP Telephony network, select a PC Phone.
7. Click **Select**. The Select dialog box is displayed.



Select: 1(any hop-off possible)

From the dropdown box, select a Hop-off Scheme and click OK.

8. From the dropdown box, select a Hop-off Scheme.
9. Click **OK**.
10. Repeat steps 6–9 for each PC Phone.
11. On the Associated Hop-off Schemes dialog box, click **OK**. A log message is displayed advising that the "Softphone table has been updated successfully."
12. Click **Close**.

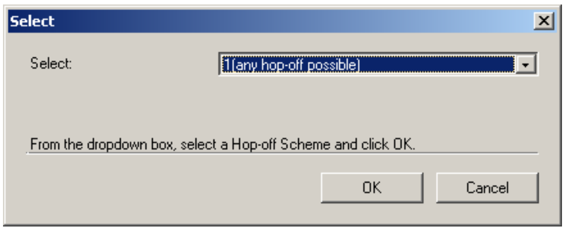
Authentication for Third-party Gateways

When configured, calls originating from third-party gateways are checked to determine if the third-party gateway is authorized to place the call via the BOSâNOVA IP Telephony network.

*Each third-party gateway must be added to the IP Telephony network **before** rules of Authentication are applied to it. See "Third Party Gateways" on page 189.*

To configure Authentication for a third-party gateway:

1. Connect and login to the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan**. The Officer's Numbering Plan Configurator is displayed.
3. Expand the **Authentication** branch.
4. Select **Third-party Gateways**.
5. Click **Change**. The Associated Hop-off Schemes dialog box is displayed.
6. From the list of third-party gateways already added to the IP Telephony network, select a third-party gateway.
7. Click **Select**. The Select dialog box is displayed.



Select: 1 (any hop-off possible)

From the dropdown box, select a Hop-off Scheme and click OK.

8. From the dropdown box, select a Hop-off Scheme.
9. Click **OK**.
10. Repeat steps 6–9 for each third-party gateway.
11. On the Associated Hop-off Schemes dialog box, click **OK**. A log message is displayed advising that the "The Third-party Gateway table has been updated successfully."
12. Click **Close**.

Creating Hop-off Schemes

A Hop-off Scheme is one or more, full or partial, E.164 numbers that are associated with a Hop-off Scheme identification number. The following rules apply:

- The Hop-off Scheme identification number can be any number between 1 and 9,999.
- Hop-off Scheme identification numbers are assigned automatically and incrementally.
- Up to twenty full or partial E.164 numbers can be associated with each Hop-off Scheme identification number.
- The same Hop-off Scheme identification number can be assigned to more than one Hop-off PIN.
- Create the Hop-off Scheme before assigning it to a PIN.

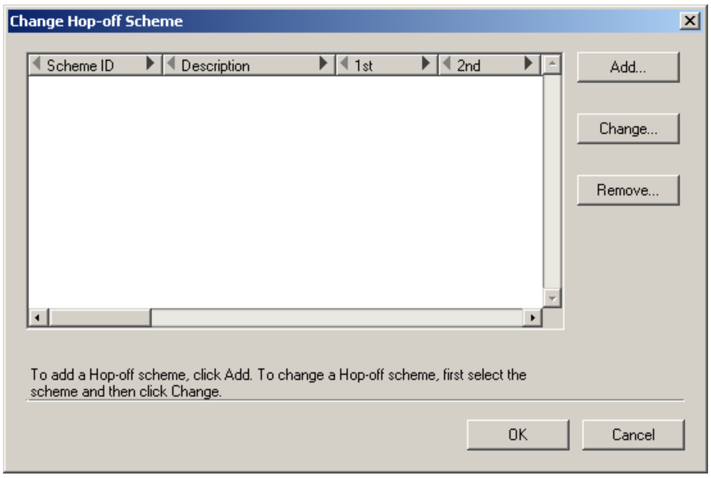
For example,

Hop-off Scheme ID	E.164 Number or Numbers	Who can be called?
1	1	Any location in the United States or Canada
2	1212	Any location in Manhattan
3	1-866-865-5250	Only this specific phone number
4	1212, 1-866-865-5250, 1-623-516-8697	Any location in Manhattan and either of these two numbers

To create a Hop-off Scheme.

1. Connect and login to the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan**. The Officer's Numbering Plan Configurator is displayed.
3. Expand the **Authentication** branch.
4. Select **Hop-off Schemes**. The Change Hop-off Schemes table is displayed.

5. Click **Change**. The Change Hop-off Schemes dialog box is displayed.



To add a Hop-off scheme, click Add. To change a Hop-off scheme, first select the scheme and then click Change.

There are three possibilities:

- To add a Hop-off Schemes, click **Add**. The Add/Edit a Hop-off Schemes dialog box opens. Follow the prompts on the screen.
- To change a Hop-off Schemes, first select the Hop-off Scheme and then click **Change**. The Add/Edit a Hop-off Schemes dialog box opens. Follow the prompts on the screen.
- To delete a Hop-off Schemes, first select the PIN and then click **Remove**.

DIALING SERVER

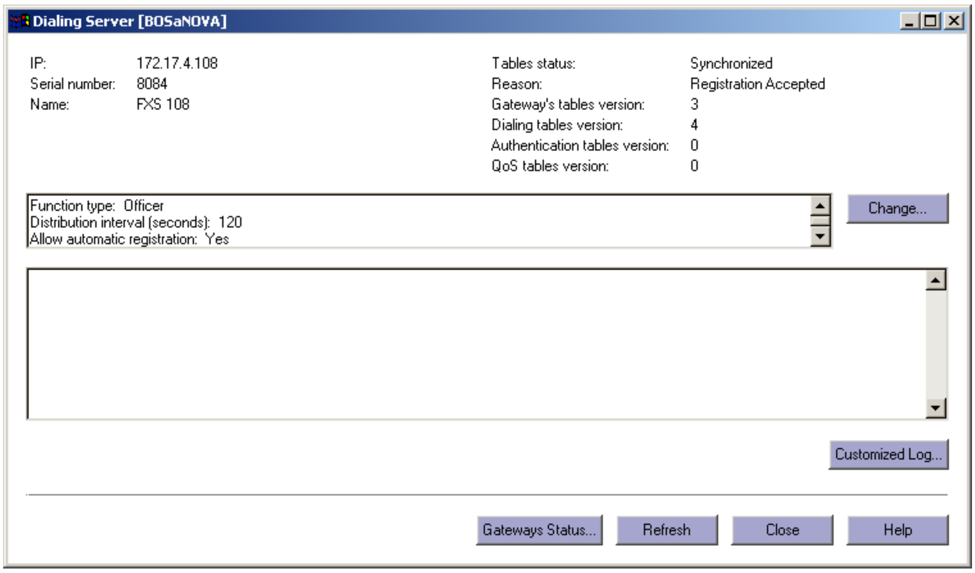
This section details the functions of the Dialing Server and procedures associated with those functions.

⚠ *Changing Officers must be performed in the sequence detailed in the next section. Any other sequence will result in conflicts.*

Assigning an Officer

Assigning an Officer is done in the Dialing Server. For an explanation of Officer functions, see page 102.

1. From the **Configurator main menu** of the Gateway that will be the Officer, select **Dialing Server**. The **Dialing Server** screen opens.



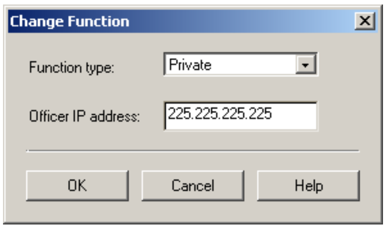
Dialing Server [BOSaNOVA]

IP:	172.17.4.108
Serial number:	8084
Name:	FXS 108

Tables status:	Synchronized
Reason:	Registration Accepted
Gateway's tables version:	3
Dialing tables version:	4
Authentication tables version:	0
QoS tables version:	0

Function type: Officer
Distribution interval (seconds): 120
Allow automatic registration: Yes

2. Click **Change**. The **Change Function** dialog box opens.

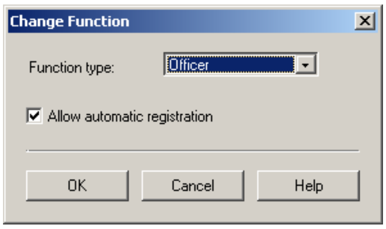


Change Function

Function type: Private

Officer IP address: 225.225.225.225

3. From the drop-down list, select **Officer** and click **OK**. The **Change Function** dialog box changes to:



4. Select or clear the **Allow automatic registration** checkbox.
   - When selected:
     A new or reconfigured Private Gateway registers automatically.
   - When cleared:
     The administrator must authorize registration of a new or reconfigured Gateway. When registration can be allowed, select Allow automatic registration.
5. Click **OK** and then click **Close**. The Configurator main menu is displayed.
6. Ensure that the other Gateways are registered as Privates and have the correct IP address of the Officer.

Changing Officers

⚠ *Changing Officers must be performed in this sequence. Any other sequence will result in conflicts.*

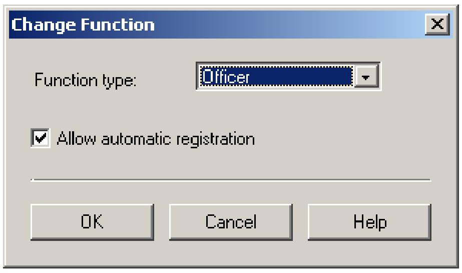
To designate a new Officer:

1. Assign the function of Officer to the ***new*** Officer Gateway. This involves completing all the steps in the Configuring an Officer section directly above.
2. Assign the function of Private to the Gateway that previously served as Officer.
3. Enter the IP address of the new Officer in the Gateway that previously served as Officer.
4. Enter the IP address of the new Officer in all the other Gateways on the VoIP network.

Adding a New Private

From the Officer Gateway, the administrator can control how and when new Private Gateways are accepted to the IP Telephony network.

1. Connect and login to the Gateway that is to be defined as Officer.
2. From the Configurator main menu, select **Dialing Server**. The Dialing Server screen is displayed.
3. Click **Change**. The Change Function dialog box opens.



Change Function

Function type: Officer

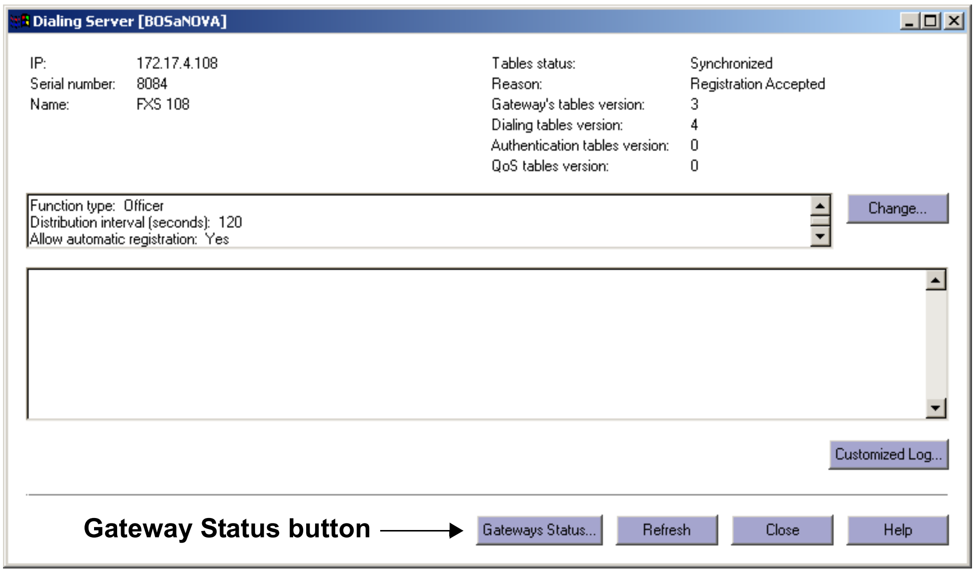
☑ Allow automatic registration

4. Select or clear the Allow automatic registration checkbox.
   - When selected:
     A new or reconfigured Gateway registers automatically.
   - When cleared:
     The administrator must authorize registration of a new or reconfigured Gateway. When registration can be allowed, select Allow automatic registration.

Reviewing Gateways' Synchronization Status

From a Gateway defined as the Officer, the administrator can review the table synchronization status of all Private Gateways on the IP Telephony network.

1. Connect and login to the Officer Gateway.
2. From the Configurator main menu, select **Dialing Server**. The Officer's Dialing Server screen is displayed.



Dialing Server [BOSaNOVA]

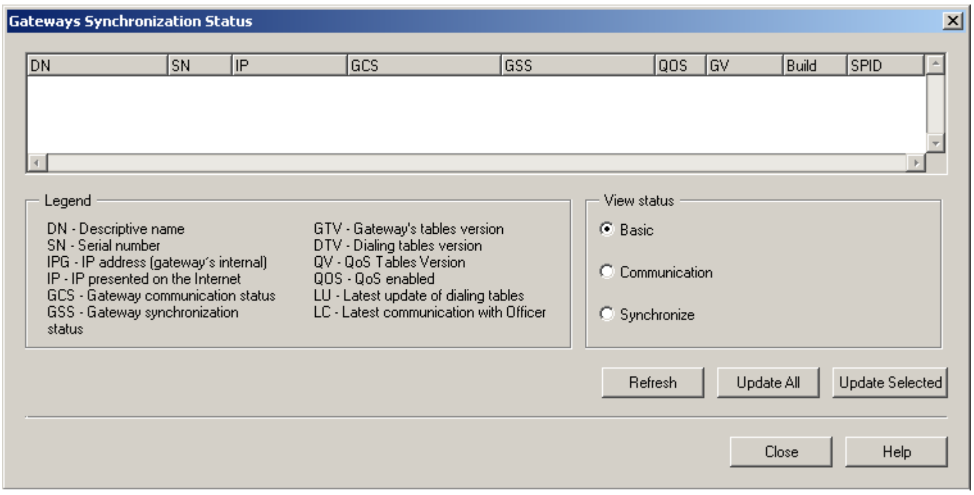
IP: 172.17.4.108
Serial number: 8084
Name: FXS 108

Tables status: Synchronized
Reason: Registration Accepted
Gateway's tables version: 3
Dialing tables version: 4
Authentication tables version: 0
QoS tables version: 0

Function type: Officer
Distribution interval (seconds): 120
Allow automatic registration: Yes

3. Click **Gateways Status**. The Gateways Synchronization Status screen opens.

*If the **Gateway Status** button does not appear, the Gateway is a Private, not the Officer.*



Gateways Synchronization Status

DN	SN	IP	GCS	GSS	QOS	GV	Build	SPID

Legend

DN - Descriptive name
SN - Serial number
IPG - IP address (gateway's internal)
IP - IP presented on the Internet
GCS - Gateway communication status
GSS - Gateway synchronization status

GTV - Gateway's tables version
DTV - Dialing tables version
QV - QoS Tables Version
QOS - QoS enabled
LU - Latest update of dialing tables
LC - Latest communication with Officer

View status
● Basic
○ Communication
○ Synchronize

4. Select one of the radio buttons in the view status box on the right side of the Gateways Synchronization Status screen.

    - Basic:
      This table informs you if each Gateway is active and synchronized, its build, and which modules are installed.
    - Communication:
      This table displays information regarding when each Gateway was lasted contacted by the Officer and when its tables were last updated.
    - Synchronization:
      This table displays information regarding the status of the three tables distributed by the Officer.

    A legend appears in the lower left corner. See Table 44 directly below for explanations.

*To open the configurator of any of Gateway listed in the Gateways Synchronization Screen, select the Gateway and click **Open**.*

Table 44: Legend for Gateway Synchronization Screen

Entries	Explanation
IP	IP address of a Private Gateway, that is, the IP address the Officer uses to connect to the Private.
IPG	Internal IP address of the Gateway
DN	**Descriptive name**: Descriptive name of a Private Gateway
SN	**Serial number**: Serial number of a Private Gateway
Build	The build version of this Gateway software
SPID	Software product ID number
GV	Gateway version

Table 44: Legend for Gateway Synchronization Screen

Entries	Explanation
GSS	**Gateway synchronization status**. Statuses of Private Gateways can be: • **Synchronized**: The Gateway has the latest version of the common dialing tables distributed by the Officer. • **Not synchronized**: The Gateway does not have the latest version of the common dialing tables distributed by the Officer. • **Rejected**: The Gateway rejected the common dialing tables sent by the Officer. This could be due to either a software conflict or because a different Gateway is defined on it as Officer. • **Not active**: The Officer could not establish a connection with the Gateway.
GCS	**Gateway communication status**: Is the Gateway active, inactive, or is there an IP conflict.
GT	**Gateway's** common dialing **tables version**: The Officer Gateway keeps a record of the common dialing table version on the Private Gateway. That record is displayed here.
QoS	Quality of Service: enabled or disabled
QT	Quality of Service table version
LU	**Latest update** of dialing tables: This is the date and time that the common dialing table of this Private Gateway was most recently updated.
LC	**Latest communication** with Officer: The most recent date and time that the Officer and this Gateway communicated.
CDT	Dialing table version

Updating Common Dialing Tables

From a Gateway defined as the Officer, the administrator can prompt an update of all common dialing tables on the Private Gateways.

There are two ways to update the common dialing tables:

1. Connect and login to the Officer Gateway.
2. From the Configurator main menu, select **Dialing Server**. The Officer's Dialing Server screen is displayed.
3. Click **Gateways Status**. The Gateways Synchronization Status screen opens.

*If the **Gateway Status** button does not appear on the Dialing Server screen, the Gateway is a Private, not the Officer.*

4. Use one of the two update options:
   - **Update Selected**
     To update the common dialing table on a particular Gateway, select the Gateway and click **Update Selected**.
   - **Update All**
     To update the common dialing tables on all Gateways, click Update All.
5. Click **Close** to return to the Dialing Server screen.

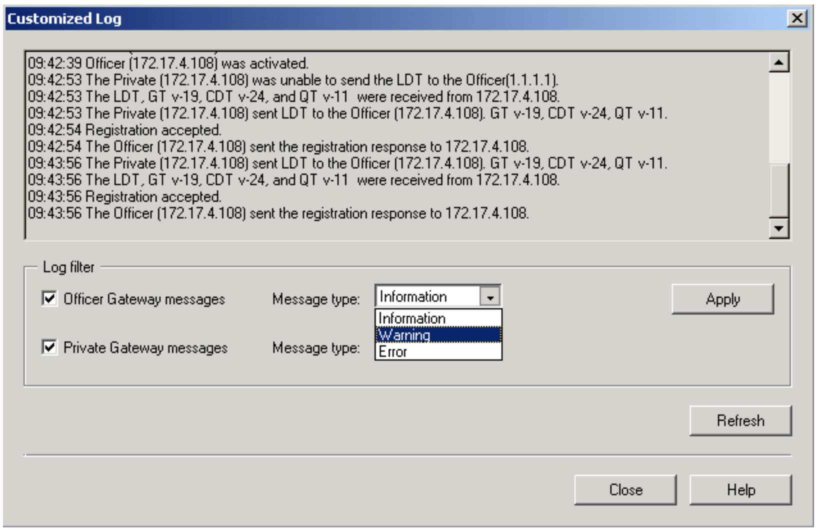
To Refresh the GSS table after you have updated click **Refresh**.

Customize Log

It is possible to view a customized log rather than the log that appears on the main screen of the Dialing Server.

To view a customized log:

1. Connect and login to the Gateway.
2. From the Configurator main menu, select **Dialing Server**. The Dialing Server screen is displayed.
3. Click **Customized Log**. The Customized Log screen appears.



```
09:42:39 Officer (172.17.4.108) was activated.
09:42:53 The Private (172.17.4.108) was unable to send the LDT to the Officer(1.1.1.1).
09:42:53 The LDT, GT v-19, CDT v-24, and QT v-11  were received from 172.17.4.108.
09:42:53 The Private (172.17.4.108) sent LDT to the Officer (172.17.4.108). GT v-19, CDT v-24, QT v-11.
09:42:54 Registration accepted.
09:42:54 The Officer (172.17.4.108) sent the registration response to 172.17.4.108.
09:43:56 The Private (172.17.4.108) sent LDT to the Officer (172.17.4.108). GT v-19, CDT v-24, QT v-11.
09:43:56 The LDT, GT v-19, CDT v-24, and QT v-11  were received from 172.17.4.108.
09:43:56 Registration accepted.
09:43:56 The Officer (172.17.4.108) sent the registration response to 172.17.4.108.
```

Log filter

☑ Officer Gateway messages — Message type: Information

☑ Private Gateway messages — Message type:

4. Select or clear the checkbox for Officer Gateway messages.
 If you choose to view the messages, then select a message type from the drop-down list.
5. Select or clear the checkbox for Private Gateway messages.
If you choose to view the messages, then select a message type from the drop-down list.

Customized Log is available for both Private Gateways and Officer Gateways.

IP Telephony...
Clear and Simple

SECTION 13: NETWORK ADDRESS TRANSLATION

This section explains prerequisites and configuration when Network Address Translation (NAT) is used on some or all of the BOSâNOVA IP telephony network.

This section includes:

- An overview of NAT and potential NAT related problems, see p. 227
- Configuring the BOSâNOVA solution to the NAT problem, see p. 228
- TCP/IP ports used by BOSâNOVA Gateways, see p. 232
- TCP/IP ports used by BOSâNOVA Connect, see p. 234

NAT OVERVIEW

Network Address Translation (NAT) refers to a process whereby an application exchanges a computer's Local Area Network (LAN) IP address for the LAN's global IP address. NAT creates problems for IP Telephony networks.

Problems Arising from the NAT Process

Each computer on a LAN is assigned a ***local*** IP address. These local IP addresses are restricted to the following ranges:

10.0.0.0	to	10.255.255.255
172.16.0.0	to	172.16.255.255
192.168.0.0	to	192.168.255.255

On the other hand, all traffic from the LAN to the Internet, and from the Internet to the LAN, is routed via the LAN's single ***global*** IP address which was assigned in accordance with standard IP addressing principles. The NAT server performs IP address translation at the exit/entrance point to the Internet.

The NAT server receives each packet from the LAN and modifies the IP header to match the global IP address before transmitting the packet to the Internet. The NAT server stores the local IP address, destination IP address, and port number in a routing table. When a request is returned on the same port, the NAT server can match the local IP address that originated the request and then modify the IP header to match that of the local address.

NAT servers create the following problem. Similar to the function of phone-numbers when placing a call over the PSTN, an IP Telephony connection occurs between two end-points with specific IP addresses. When a NAT server substitutes the global IP address for the local IP address, the computer's local IP address remains unknown to all other computers. Therefore, the computer on the LAN cannot receive any calls.

In other settings, the fact that a NAT server hides a computer's IP address from the Internet is considered positive because that represents another level of security.

CONFIGURING NAT SUPPORT

Configuring a BOSâNOVA Gateway to work with a NAT server involves four steps:

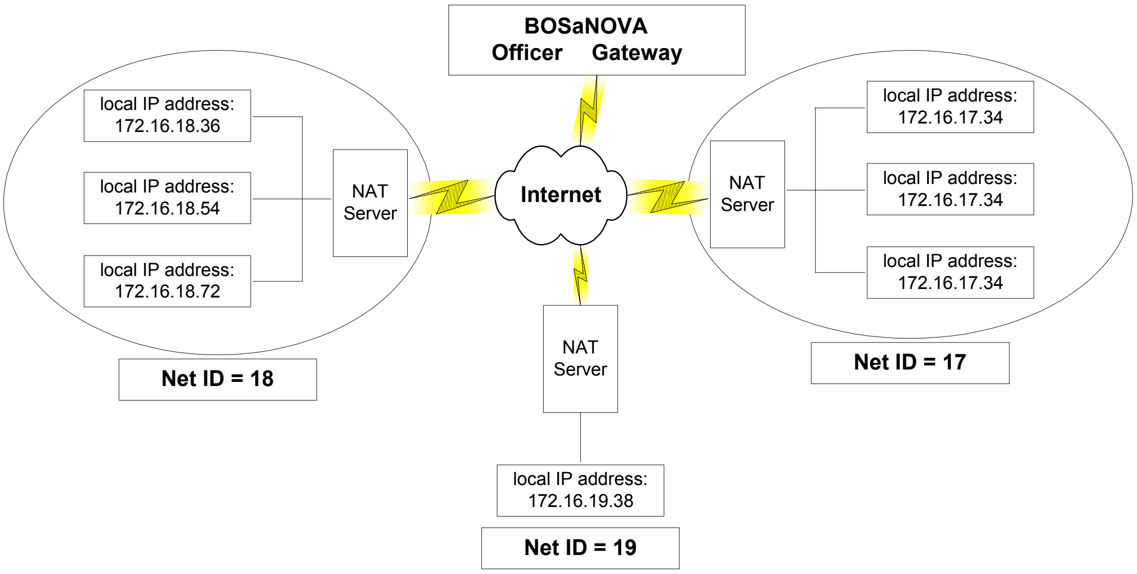
1. Employing the parameter NET ID
2. Ensuring the Officer is not behind a NAT Server
3. Selecting the NAT Support checkbox for each Gateway
4. Configuring the Net ID for each single and/or group of Gateways

Employing the Parameter: NET ID

Successful configuration is built upon advanced planning. The IP Telephony network administrator must determine which Net ID number will be assigned to each group of endpoints or single endpoint. An endpoint can be either a BOSâNOVA Gateway or a BOSâNOVA Connect.

The Net ID identifies the IP Telephony network subnet the Gateway or Connect is located in. More than one endpoint can be assigned the same Net ID. However, endpoints sharing the same Net ID must all be located behind the same NAT server. Conversely, all endpoints behind the same NAT server must be assigned the same Net ID.

Note in the following illustration that there are two groups of endpoints assigned Net IDs 17 and 18, and one single endpoint, assigned the Net ID 19.


BOSaNOVA
Officer Gateway
local IP address: 172.16.18.36
local IP address: 172.16.18.54
local IP address: 172.16.18.72
NAT Server
Net ID = 18
Internet
NAT Server
local IP address: 172.16.17.34
local IP address: 172.16.17.34
local IP address: 172.16.17.34
Net ID = 17
NAT Server
local IP address: 172.16.19.38
Net ID = 19

Location of the Officer Gateway

The Officer Gateway resolves all the IP Telephony network problems arising from NAT. Thus, the Officer Gateway must not be behind a NAT.

⚠ *Ensure that the Officer Gateway is not behind a NAT server. If it is, the IP Telephony network will not function.*

Configuring End-points Behind a NAT

⚠ *Regarding a **single** end-point behind a NAT:*
Ensure that the NAT server supports port-forwarding of the specific port numbers used by BOSâNOVA Gateways. Some NAT servers do not. The IP Telephony network will not function if port-forwarding cannot be applied to the specific ports.
See "TCP/IP Ports Used by BOSâNOVA Gateways" on page 232.

⚠ *Regarding **multiple** end-points behind a NAT:*
Ensure that the NAT server supports 1-to-1 NAT. Some NAT servers do not. If the NAT server does not support 1-to-1 NAT, you can place only one end-point behind it.

To configure end-points located behind a NAT:

1. Ensure that the NAT server matches the requirements listed in the two warnings above.
2. Configure the NAT server.
   - In the case of a single end-point behind a NAT, configure port-forwarding using the specific TCP/IP port numbers used by BOSâNOVA Gateways.
   - In the case of multiple end-points behind a NAT, configure 1-to-1 NAT.

   Refer to the manufacturers documentation for help.
3. Determine which Net ID number will be assigned to each group.

Assign the same Net ID to all end-points that are not behind a NAT server, including the Officer Gateway. This Net ID can be zero (0).

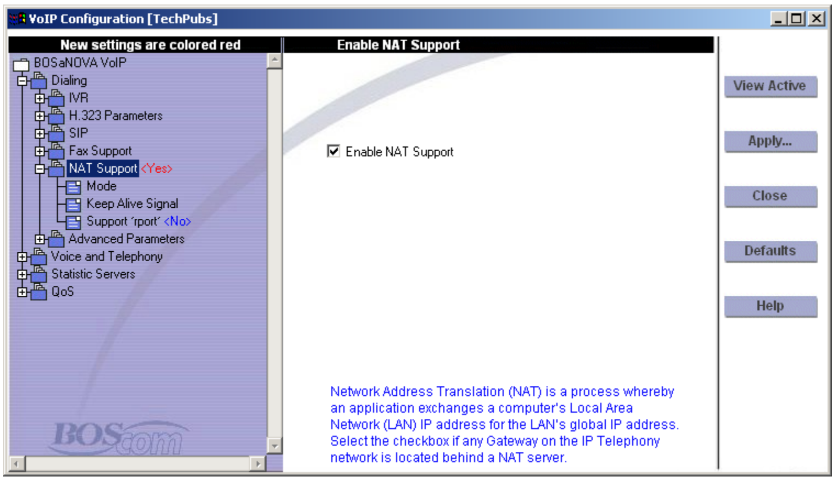
4. From the main menu of a Private Gateway’s Configurator, select **VoIP Configuration**.

5. In the left pane of the VoIP Configurator, expand the **Dialing** branch.

6. Expand the **Advanced Parameters** branch.

7. In the left pane of the VoIP Configurator, select **NAT Support**.

8. In the right pane of the VoIP Configurator, select **Enable NAT Support**.



☑ Enable NAT Support

Network Address Translation (NAT) is a process whereby an application exchanges a computer's Local Area Network (LAN) IP address for the LAN's global IP address. Select the checkbox if any Gateway on the IP Telephony network is located behind a NAT server.

9. Select the **Mode** sub-branch. Two options are available from the Mode dropdown menu in the right pane:

   - **BOS**
     When selected, the Gateway obtains its external IP address automatically. This address is included in H.323 messages where the local IP address is defined. Continue NAT configuration with step 12.

   - **Static NAT IP**
     When selected, enter the external IP address behind which this Gateway resides. This address will be included in H.323 messages where the local IP address is defined. This may resolve interoperability issues.

10. Select the **Keep Alive Signal** sub-branch. The Keep Alive signal prevents disconnect from a SIP proxy. As required, select the checkbox and enter the interval at which Keep Alive signals will be sent.

11. Select the **Support ‘rport’** sub-branch. As required, select the checkbox. ‘Rport’ is useful for basic NAT traversal. This parameter allows a client to request that the server send the response back to the source IP address and port where the request came from. ‘Rport’ is analogous to the “received” parameter, except “rport” contains a port number, not the IP address.

12. Click **Apply**.

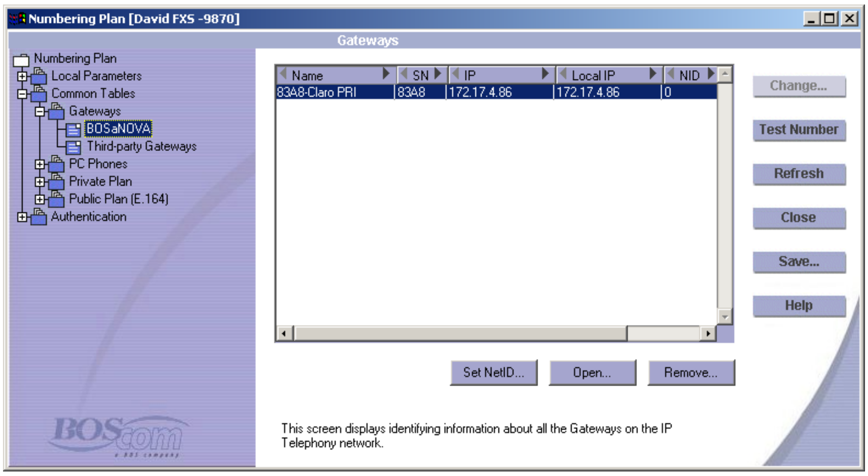
13. Repeat steps 4–12 for each Gateway. Then continue with step 14.

14. Log-on to the Configurator of the Officer Gateway.

15. From the main menu of the Officer’s Configurator, select **Numbering Plan**.

16. In the left pane of the Numbering Plan Configurator, expand the **Common Tables** branch.

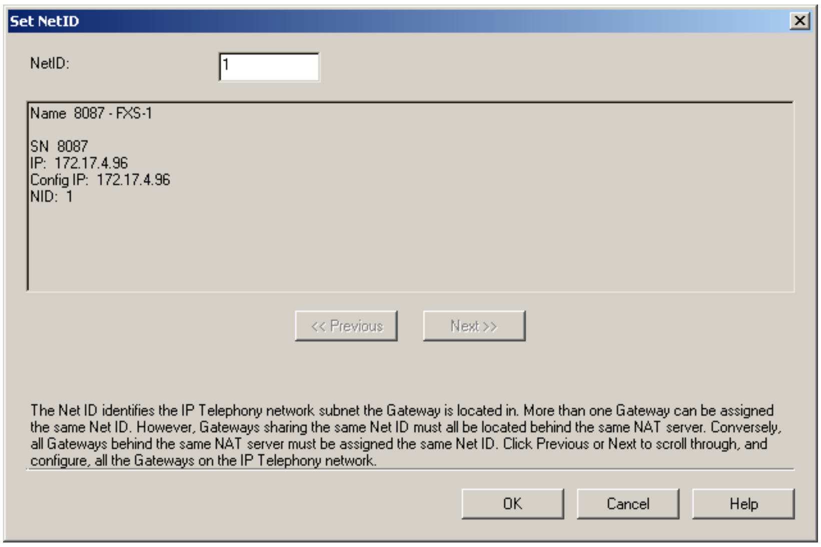
17. Select **Gateways > BOSaNOVA**. The Gateways table appears in the right pane and the Set NetID button appears under the table.



Name	SN	IP	Local IP	NID
83A8-Claro PRI	83A8	172.17.4.86	172.17.4.86	0

This screen displays identifying information about all the Gateways on the IP Telephony network.

18. Click **Set NetID**. The Set NetID dialog box opens.



NetID: 1

Name 8087 - FXS-1

SN 8087
IP: 172.17.4.96
Config IP: 172.17.4.96
NID: 1

The Net ID identifies the IP Telephony network subnet the Gateway is located in. More than one Gateway can be assigned the same Net ID. However, Gateways sharing the same Net ID must all be located behind the same NAT server. Conversely, all Gateways behind the same NAT server must be assigned the same Net ID. Click Previous or Next to scroll through, and configure, all the Gateways on the IP Telephony network.

19. Enter the ID number in the Net ID field for each Gateway in the group. Click **Previous** or **Next** to scroll through, and configure, all the Gateways.

20. Click **OK** to close the Set NetID dialog box.

21. Click **Close** to close the Numbering Plan Configurator.

TCP/IP PORTS USED BY BOSâNOVA GATEWAYS

The following ports are required for functioning of BOSâNOVA Gateways and therefore must be supported by NAT servers:

- For **H.323 VoIP**, the following ports are required:
  1720/tcp, 30000 +(4*n)/udp (n = number of lines)
- For **Configuration and Management**, the following ports are required:
  22/tcp, 80/tcp, 25051/tcp
- For **Numbering Plan Configuration Replication**, the following ports are required:
  25050/tcp, 25052/tcp/udp, 25053/udp

Use of the following ports is dependent upon the configuration of the Gateway:

- For the **Quality of Service** module, the following ports are required:
  25054/tcp, 25055/udp, 25060/udp, 25100+n/udp (n = number of gateways)
- For **Configuration and Management via SNMP**, the following port is required:
  161/udp
- Regarding **H.245 Tunneling**, the following ports may be required. See the table below for details:
  All ports >1024/tcp

Table 45: TCP/IP Ports Used by BOSâNOVA Gateways, versions 2.1xxx and up

Port/ Protocol	Inbound Traffic	Outbound Traffic	Notes
22/tcp	Yes	Yes	Standard SSH port. Used by the Maintenance Wizard for all maintenance operations. Used for communications with the BOSâNOVA CDR Server.
80/tcp	Yes	No (1)	This port is assigned to built-in HTTP server. Web-based BOSâNOVA Gateway Configurator connects to this port only for loading Java applet
161/udp	Yes	Yes	Optional. This is the standard port for SNMP communications. If you want to use an SNMP manager for Gateway monitoring, you should open this port on your Firewall.
1720/tcp	Yes	Yes	This port is used for H.323 communications (H225, RAS and Call Progress).
4568/udp	No	No	The Maintenance Wizard uses this port for searching Gateways located on the local network. No need to open this port on the Firewall.

Table 45: TCP/IP Ports Used by BOSâNOVA Gateways, versions 2.1xxx and up

Port/ Protocol	Inbound Traffic	Outbound Traffic	Notes
25050/tcp	Yes	Yes	BOSâNOVA Officer Gateway uses this port (server on Private Gateway) for communications with the Private Gateway.
25051/tcp	Yes	No (see note #1)	Web-based BOSâNOVA Configurator uses this port for communications with the Gateway modules.
25052/ tcp/udp	Yes	Yes	BOSâNOVA Gateway and BOSâNOVA Connect use this port (server on Officer Gateway) for communications with the Officer Gateway.
25053/ udp	Yes	No	BOSâNOVA Gateway and BOSâNOVA Connect use this port for communications for on-line resolving of the BOSâNOVA Connect number on the Officer Gateway.
25055/tcp	Yes	Yes	Optional (2). The port is used for QoS measurements.
25100+n/ udp	Yes	Yes	Optional (2). The port is used for QoS measurements. Where *n* is the number of BOSâNOVA Gateways on your VoIP network.
25060/ udp	No	No	QoS Relay server (NQS) receives test packets. Is not used in the current version.
30000-30500/ udp	Yes	Yes	RTP/RTCP/UDPTL packets. BOSâNOVA Gateway may use these ports for receiving the voice packets. One call requires 4 ports.
All ports >1024/tcp	Yes	Yes	Optional. These ports may be used for H.245 negotiation if H.245 Tunneling is disabled on either communication side. By default, H.245 Tunneling is enabled in both Gateway and BOSâNOVA Connect configuration.

NOTES:

1. You must open this port for outbound traffic if you want to be able to configure a Gateway that is located outside of the Firewall, via the Gateway Configurator, from a PC which is behind (inside of) the Firewall.
2. You must open this port only if your Gateway is configured for QoS measurements support.
3. In versions prior to 2.10, the port used for QoS was 25054.

TCP/IP PORTS USED BY BOSâNOVA CONNECT

Table 46: TCP/IP Ports Used by BOSâNOVA Connect

Port/ Protocol	Inbound Traffic	Outbound Traffic	Notes
1720/tcp	Yes	Yes	This port is used for H.323 communications (H225, RAS and Call Progress).
25052/ tcp/udp	Yes	Yes	BOSâNOVA Gateway and BOSâNOVA Connect use this port (server on Officer Gateway) for communications with the Officer Gateway.
25053/ udp	Yes	No	BOSâNOVA Gateway and BOSâNOVA Connect uses this port for communications for on-line resolving of the BOSâNOVA Connect number on the Officer Gateway.
30000-30002/ udp	Yes	Yes	RTP/RTCP/UDPTL packets. These ports are always used by BOSâNOVA Connect and may be used by BOSâNOVA Gateways for receiving the voice packets.
30000-30500/ udp	No	Yes	RTP/RTCP/UDPTL packets. BOSâNOVA Gateway may use these ports for receiving the voice packets.
All ports >1024/ tcp	Yes	Yes	Optional. These ports may be used for H.245 negotiation if H.245 Tunneling is disabled on either communication side. By default, H.245 Tunneling is enabled in both Gateway and BOSâNOVA Connect configuration.

SECTION 14:
BOSâNOVA CONNECT and CONNECT LITE

The BOSâNOVA Connect USB adapter is an external Plug and Play device that connects:

- On one side, into the USB port on a laptop or a desktop computer
- On the second side, into a regular, analog telephone

The BOSâNOVA Connect USB adapter allows you to place and receive telephone calls over a LAN, WAN, or the public Internet using a regular telephone.

Connect Lite, also called *the sound card option*, requires a full-duplex sound card, speakers, and microphone installed on your PC. Connect Lite lets you to talk and listen, via your computer, as if you were using a telephone.

If the IP Telephony network is configured using a BOSâNOVA Officer Gateway, a computer’s full duplex sound card and either a headset or microphone with speakers can be used instead of the USB device and phone.

The following content appears in this section:

- BOSâNOVA Connect system requirements, p. 236
- Installing the BOSâNOVA Connect, p. 237
- Upgrading the BOSâNOVA Connect, p. 242
- Manual installation of the driver, p. 243
- Reviewing current network Connect configuration, p. 245
- Configuring the BOSâNOVA Connect, p. 246

BOSâNOVA CONNECT SYSTEM REQUIREMENTS

PC Processor	Pentium II minimum
Memory	64 MB minimum
Operating System	Windows 98, Millennium Edition, 2000, and Windows XP
Hard Disk	10 MB
CD-ROM Drive	To install software
Network Connection	IP network connection or dial-up connection, 28.8 Kbps or faster
For USB Mode	Available USB port, to connect the USB cable from the PC to the BOSâNOVA Connect
For USB Mode, a touch-tone analog telephone	Chicago Electric Company 3C (This model is not touch-tone.)
For Sound Card Mode	Full-duplex sound card, microphone, and speakers

A BOSâNOVA Connect may not function properly if it is connected to a passive (unpowered) USB hub. Replace the passive USB hub with an active (powered) hub, that is, one that plugs into an electric outlet. If that is not possible, disconnect the BOSâNOVA Connect from the USB hub and plug it in directly to the USB port on the computer.

INSTALLING a BOSâNOVA CONNECT

Installation must progress in the following order:

1. *Install the Connect software.*
2. *Install the BOSâNOVA Connect USB adapter.*
3. *Configure the Connect software.*

1. Close all applications.
2. Ensure that the Connect's Installation Key is accessible; it is required to complete the installation. The Installation Key is the 14 character string found at the beginning of the BOSâNOVA Connect Installation Guide.
3. Install the BOSâNOVA Connect software.

The hardware must ***not*** *be connected during installation of the software. Installation complications will occur if the Connect box is attached to the PC during software installation.*

a. Insert the BOSâNOVA Connect CD-ROM. The BOSâNOVA Connect Welcome screen appears. If the Welcome screen does not appear automatically, run **setup.exe** from the root directory of the BOSâNOVA Connect CD-ROM.

b. From the Welcome screen, select **Install BOSâNOVA Connect**. The installation wizard appears.

c. Read the Welcome and click **Next**.

d. Enter the 14 character Installation Key that appears on the first page of the Installation booklet and click **Next**. The Destination Folder screen appears.

e. If you are an experienced user and prefer a different Destination Folder, click Browse and define your preferred Destination Folder. Otherwise, simply click **Next**. The Program Folders screen appears.

f. If you are an experienced user and prefer a different Program Folder, select it from the list. Otherwise, simply click **Next**. The Current Settings screen appears.

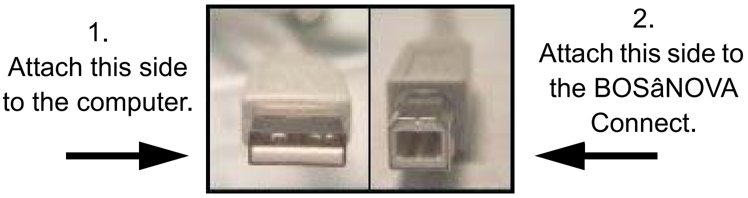
g. Review the information you've provided. If you want to make any changes, click Back. If you are satisfied, click **Next**. Installation begins.

When installing BOSâNOVA Connect on Windows XP, three additional screens appear (one now and two during the hardware installation segment). Simply click ***OK*** *➤* ***Next*** *on each screen. They are necessary to ensure proper installation of the driver.*

h. During installation, InstallShield displays a progress report. When installation is complete, one of two messages appear:

- **Driver installation succeeded.**
  Click **OK** and **Finish**. Continue with installation of the BOSâNOVA Connect harware.
- **Driver installation failed.**
  Click **OK** and **Finish**. You must manually install the BOSâNOVA Connect driver before installing the hardware. For instructions about installing the BOSâNOVA Connect driver manually, see “Manual Installation of the Driver” on page 243.

4. Install the hardware.


1.
Attach this side to the computer.
2.
Attach this side to the BOSâNOVA Connect.

a. Attach the rectangular connector of the supplied USB cable to a free USB port on the back of the computer.

b. Attach the square connector of the supplied USB cable to the BOSâNOVA Connect USB adapter.

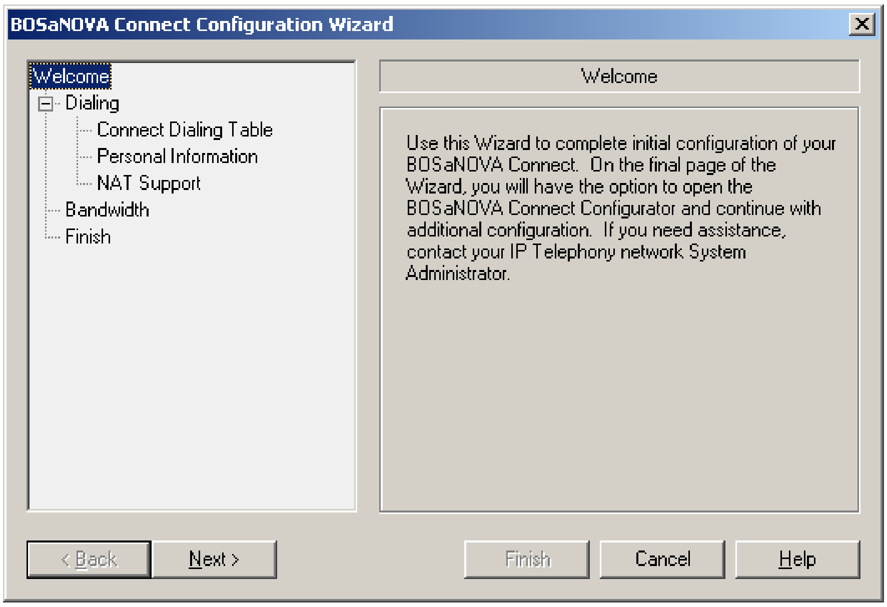
c. Attach the telephone’s cable to the adapter.

d. Wait patiently as the driver installation is automatically completed. Windows 2000 and XP provides indication of the progress. Windows 98 and Me do not.

5. Configure the BOSâNOVA Connect software. The following procedure will get you started and then refer you to the online Help.

   a. To start BOSâNOVA Connect, click the Windows **Start** button and select **Programs**.

   b. From the BOSâNOVA Connect program group (or other if you customized your installation), select BOSâNOVA Connect. The Configuration Wizard opens.

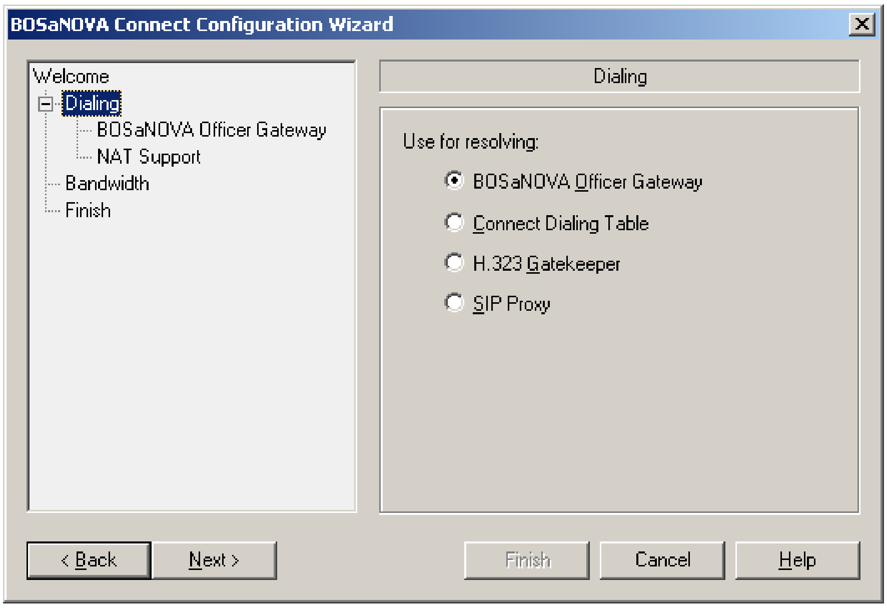


Use this Wizard to complete initial configuration of your BOSaNOVA Connect. On the final page of the Wizard, you will have the option to open the BOSaNOVA Connect Configurator and continue with additional configuration. If you need assistance, contact your IP Telephony network System Administrator.

If the Configuration Wizard does not open, an earlier version of Connect is already installed on your computer.

To navigate, use the ***Back*** *and* ***Next*** *buttons. Navigation is not possible from the left pane of the Wizard. It shows your location within the steps of the Wizard.*

c. Click **Next**. The Dialing page is displayed.



Use for resolving:

● BOSaNOVA Officer Gateway

○ Connect Dialing Table

○ H.323 Gatekeeper

○ SIP Proxy

d. Select an Address Resolution Method. Because different information is required for each method, the entries in the left pane change to match the selection in the right pane. For detailed assistance, click **Help**.

BOSâNOVA Officer Gateway
Select this option to use a BOSâNOVA Officer Gateway to place your calls.

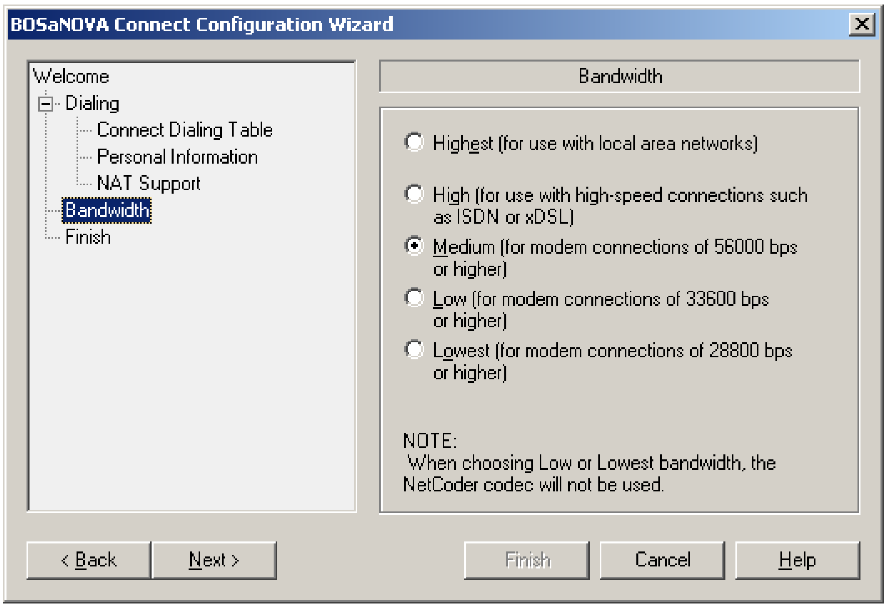
Connect Dialing Table (USB Adapter mode only)
Select this option to use a Connect dialing table to place your calls. At least one phone number must be entered.

H.323 Gatekeeper (USB Adapter mode only)
Select this option to configure a gatekeeper computer to place your calls.

SIP Proxy
Select this option to use a computer running a SIP proxy server to manage the calls. A SIP Proxy is a computer running the Session Initiation Protocol (SIP). SIP is one of two protocols for carrying voice over IP.

e. To configure the Address Resolution Method, click **Next** and define the required parameters. Repeat this for all the pages of the Dialing branch.

f. Click **Next**. The Bandwidth page is displayed.



○ Highest (for use with local area networks)

○ High (for use with high-speed connections such as ISDN or xDSL)

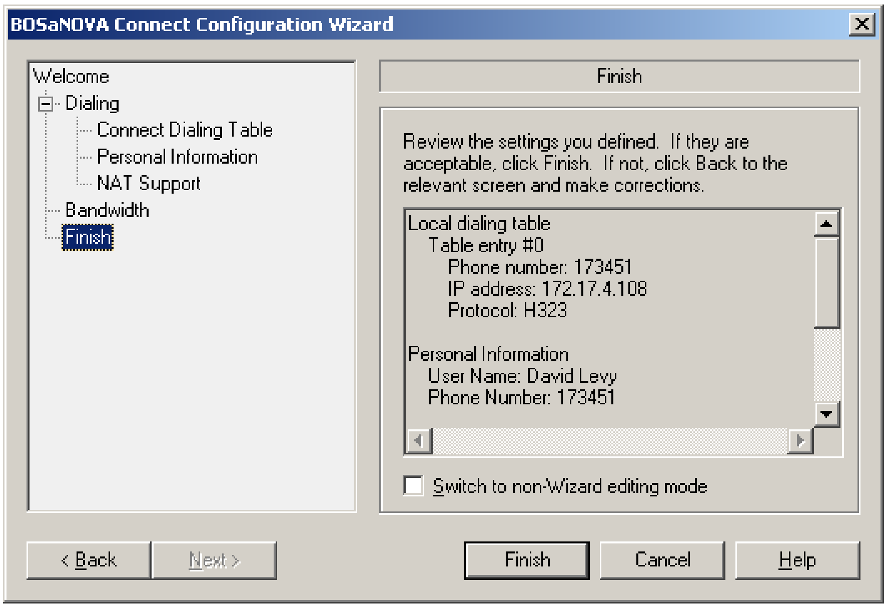
● Medium (for modem connections of 56000 bps or higher)

○ Low (for modem connections of 33600 bps or higher)

○ Lowest (for modem connections of 28800 bps or higher)

NOTE:
When choosing Low or Lowest bandwidth, the NetCoder codec will not be used.

g. Select a bandwidth and click **Next**. The Finish page is displayed.



Review the settings you defined. If they are acceptable, click Finish. If not, click Back to the relevant screen and make corrections.

```
Local dialing table
   Table entry #0
      Phone number: 173451
      IP address: 172.17.4.108
      Protocol: H323

Personal Information
   User Name: David Levy
   Phone Number: 173451
```

□ Switch to non-Wizard editing mode

h. Review the information and click **Finish**. Following initial installation only, the Connect Self-test will run.

*To configure additional and advanced parameters, select the **Switch to non-Wizard configuration mode** checkbox. After clicking Finish, the Connect Configurator opens.*

UPGRADING a BOSâNOVA CONNECT

1. ***The hardware must be disconnected before upgrading.*** We also recommend closing all applications.
2. Insert the BOSâNOVA Connect CD-ROM. The BOSâNOVA Connect Welcome screen appears. If the Welcome screen does not appear automatically, run **setup.exe** from the root directory of the BOSâNOVA Connect CD-ROM.
3. From the Welcome screen, select **Install BOSâNOVA Connect**. The Wizard's Welcome screen appears.
4. Select **Update or Repair** and click **Next**. Depending upon the BOSâNOVA Connect version number, the Installation Key might be required. The Installation Key is the 14 character string found at the beginning of the BOSâNOVA Connect Installation Guide.
5. One of two messages appears:
   - **Driver installation succeeded.**
     Click **OK** and **Finish**. Reattach the USB cable and (as with a new installation) wait for installation to finish. You can now use BOSâNOVA Connect.
   - **Driver installation failed.**
     Click **OK** and **Finish**. You must manually update the BOSâNOVA Connect driver.

To manually update the driver, run the Update Device Driver Wizard. Steps 6–16 illustrate illustrate how that is done in Windows 2000. Other versions of Windows are similar but not identical. If you encounter difficulties, contact Technical Support.

6. Attach the USB cable to the BOSâNOVA Connect.
7. Select **Start > Settings > Control Panel**. The Control Panel opens.
8. Double-click **System**.
9. Select the **Hardware** tab.
10. Click **Device Manager**.
11. Expand the **Universal Serial Bus controllers** branch.
12. Right-click **BOSâNOVA Connect USB** driver.
13. From the popup menu, select **Properties**.
14. Select the **Driver** tab.
15. Select **Update Driver**.
16. Complete the **Update Device Driver** wizard. The latest USB driver is located on the BOSâNOVA Connect CD-ROM in the **USBDriver** folder.

MANUAL INSTALLATION OF THE DRIVER

Follow the instructions for the version of Windows that is running on the computer. To check which version of Windows is running on the computer, click the Windows Start button. The Windows version is listed on the left side of the Start menu.

Windows 98

1. There are five screens in the Add New Hardware Wizard. The first screen explains that Windows will begin the search for new drivers for a device. Click **Next**.
2. Screen 2: Windows searches for a suitable driver for the BOSâNOVA Connect USB adapter. Select **Search for the best driver for your device** and click **Next**.
3. Screen 3: Select **Specify a location** and browse to locate the file path of the BOSâNOVA Connect USB driver. The driver is located on the BOSâNOVA Connect CD-ROM in the **USBDriver** folder. Click **Next**.
4. Screen 4: The Wizard has finished searching for the driver files for the BOSâNOVA Connect CTI Box Loader. The file path for the location of the driver is displayed. Click **Next**.
5. Screen 5: Installation is complete. Click **Finish**.

Windows 2000:

1. The first screen in the Found New Hardware Wizard is a Welcome screen. Click **Next**.
2. Verify that the **Search for a suitable driver for my device** option is selected and click **Next**.
3. Verify that ***only*** the **Specify a location** checkbox is selected. Click **Next**.
4. Browse to locate the file path of the BOSâNOVA Connect USB driver. The driver is located on the BOSâNOVA Connect CD-ROM in the **USBDriver** folder. Click **Open** ➢ **OK**.
5. Click **Next**. The Insert Disk message box appears.
6. Click **OK** ➢ **Browse** ➢ **Open** ➢ **OK**.
7. Installation of the BOSâNOVA Connect CTI Box Loader is complete. Click **Finish**.
8. The Insert Disk message box appears again. Click **OK**.
9. Browse to locate the file path of the BOSâNOVA Connect USB driver. The driver is located on the BOSâNOVA Connect CD-ROM in the **USBDriver** folder. Click **Open** ➢ **OK**. Installation of the CTI USB Box is complete. The Wizard closes automatically.

Windows ME:

1. There are four screens in the Add New Hardware Wizard. The first screen identifies the new hardware that Windows located. Select the **Specify the location** (Advanced) option. Click **Next**.
2. Screen 2: Windows searches for a suitable driver for the USB device.
   a. Select **Search for the best driver for your device**.
   b. Select **Specify a location**.
   c. Browse to locate the file path of the BOSâNOVA Connect USB driver. The driver is located on the BOSâNOVA Connect CD-ROM in the **USBDriver** folder. Click **Next**.
3. Screen 3: The Wizard has finished searching for the driver files for the BOSâNOVA Connect CTI Box Loader. The file path for the location of the driver is displayed. Click **Next**.
4. Screen 4: Installation is complete. Click **Finish**.

Windows XP

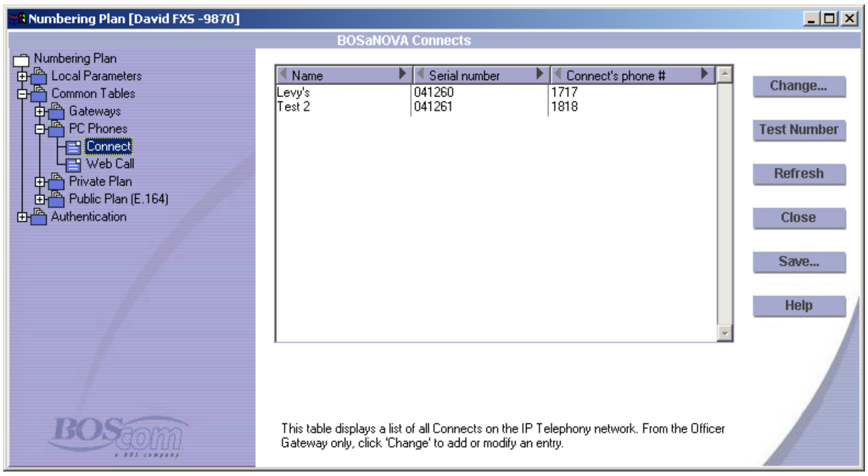
1. The first screen in the Found New Hardware Wizard is a Welcome screen. Select **Install from a list or specific location** and click **Next**.
2. Windows searches for a suitable driver.
   a. Select the **Search for the best driver in these locations** radio button.
   b. Select the **Include this location in the search** checkbox and clear the other checkbox.
   c. Click **Browse** to locate the file path of the BOSâNOVA Connect USB driver. The driver is located on the BOSâNOVA Connect CD-ROM in the **USBDriver** folder. Click **OK** ➢ **Next**.
3. On the Hardware Installation message box, click **Continue Anyway**.
4. The Insert Disk message box appears. Click **OK**.
5. Click **Browse** and select the USB Driver folder.
6. Click **Open** ➢ **OK**.
7. Click **Finish**. The Wizard starts over again, this time installing BOSâNOVA Connect CTI USB Box.
8. Repeat steps a and b.
9. On the “Please select best match ...” page of the Wizard, click **Next**.
10. Click **Continue Anyway** ➢ **OK**.
11. Click **Browse** and select the USB Driver folder.
12. Click **Open** ➢ **OK** ➢ **Finish**.

REVIEWING CURRENT CONNECT CONFIGURATION

Connect configuration can be reviewed from any Gateway. However, new Connects can only be integrated via the Numbering Plan Configurator of the Officer. See "Adding a Connect to the Officer Gateway" on page 246.

To review the current Connect configuration on an IP Telephony network:

1. Open the Configurator of the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan Configurator**.
3. From the Parameters Field, select **Common Tables > PC Phones > Connects**. The table is displayed in the Configuration field.



Name	Serial number	Connect's phone #
Levy's	041260	1717
Test 2	041261	1818

This table displays a list of all Connects on the IP Telephony network. From the Officer Gateway only, click 'Change' to add or modify an entry.

Three columns appear in the Connect Configuration table.

- **Name**
  This is the descriptive name that has been assigned to a Connect. The descriptive name is a unique name which readily identifies each Connect. The descriptive name can be up to 32 digits long.
- **Serial Number**
  The serial number is the 14 digit number found on the packaging accompanying the BOSâNOVA Connect CD-ROM.
- **Connect's Phone #**
  This is the phone number assigned to this Connect. The Officer reviews the list of Connects and sends a message approving or rejecting the list.

CONFIGURING a BOSâNOVA CONNECT with an OFFICER

When call resolution will occur through the Officer, there are two steps to integrating BOSâNOVA Connects into an IP Telephony network:

1. Configuring the Officer to recognize the Connect. ***This step must be completed before step #2***.
2. Configuring the Connect to locate the Officer.

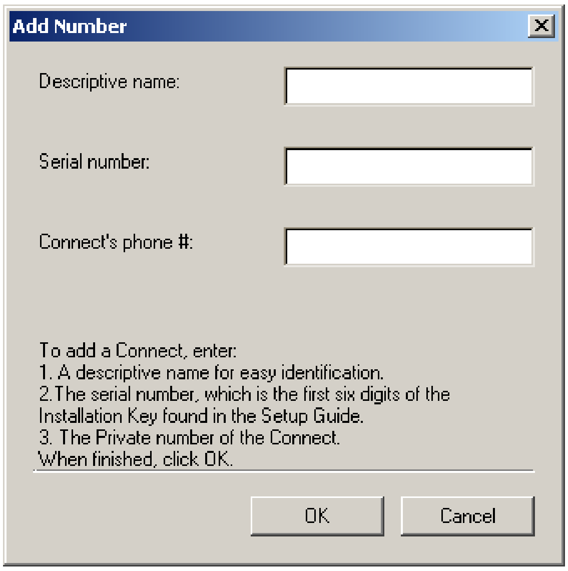
An explanation of BOSâNOVA Connect configuration also appears in the Connect online Help.

Connects can only be integrated via the Numbering Plan Configurator of the Officer. See also "Using the Officer Gateway" on page 203.

Adding a Connect to the Officer Gateway

To add a Connect to an IP Telephony network:

1. Open the Configurator of the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan Configurator**.
3. From the Parameters Field, select **Common Tables > PC Phones > Connects**. The table is displayed in the Configuration field.
4. Click **Change**. The Connect Numbers dialog box opens.
5. Click **Add**. The Add Number dialog box opens.



To add a Connect, enter:
1. A descriptive name for easy identification.
2.The serial number, which is the first six digits of the Installation Key found in the Setup Guide.
3. The Private number of the Connect.
When finished, click OK.

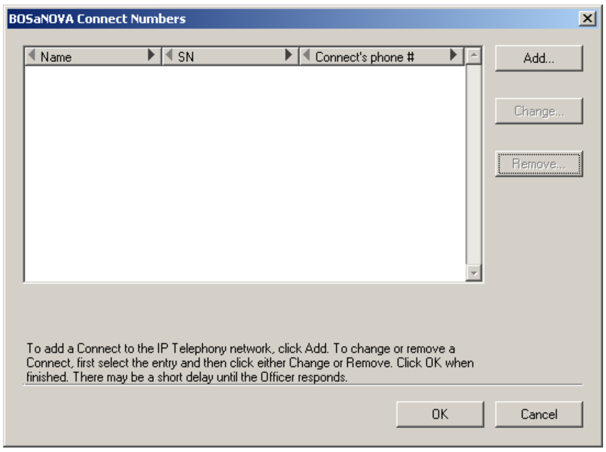
6. Enter a descriptive name. The descriptive name is a unique name which readily identifies each Connect and each Gateway. The descriptive name can be up to 32 digits long.
7. Enter ***only*** the first 6 digits of the serial number that is found on the packaging accompanying the BOSâNOVA Connect CD-ROM.
8. Enter the Private Number assigned to this Connect and click **OK**.

The Officer reviews the list of Connects and sends a message approving or rejecting the list. If the list of Connects is long, the process of reviewing the list may take several minutes.

Modifying a Connect Configuration from the Officer Gateway

To modify a Connect configuration:

1. Open the Configurator of the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan Configurator**.
3. From the Parameters Field, select **Common Tables > PC Phones > Connects**. The table is displayed in the Configuration field.
4. Click **Change**. The Connect Numbers dialog box opens.



To add a Connect to the IP Telephony network, click Add. To change or remove a Connect, first select the entry and then click either Change or Remove. Click OK when finished. There may be a short delay until the Officer responds.

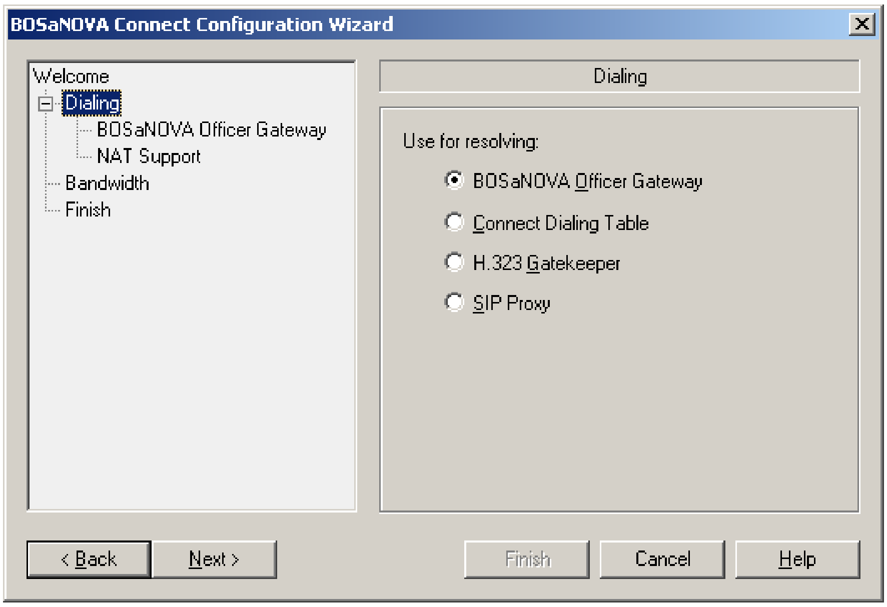
5. Select a Connect entry.
6. Click **Change**. The Change Number dialog box opens.
7. Enter new information in any of the three fields and click OK.

Configuring the Connect to Locate the Officer

Complete this step only after configuring the Officer to recognize the Connects. See "Adding a Connect to the Officer Gateway" on page 246.

To configure the Connect to locate the Officer:

1. Complete installation of the BOSâNOVA Connect. For installation instructions, see page 237.
2. From the BOSâNOVA Connect menu bar, click **File** > **Configuration Wizard**. The Configuration Wizard Welcome screen is displayed.
3. Click **Next**. The Address Resolution Method screen is displayed.



Use for resolving:

● BOSaNOVA Officer Gateway

○ Connect Dialing Table

○ H.323 Gatekeeper

○ SIP Proxy

4. Choose **BOSâNOVA Officer Gateway** and click **Next**.
5. Enter the IP address of the BOSâNOVA Officer Gateway to be used for address resolution. This address is available from the IP Telephony network System Administrator. Click **Next**.
6. Only if NAT is required:
   a. From the left pane, select **NAT Support**.
   b. From the right pane, select **Enable NAT support**.
   c. Enter the **Network ID**. The Network ID is available from the IP Telephony System Administrator.
7. Click **Next**, review the configuration, and click **Finish**.

IP Telephony...
Clear and Simple

SECTION 15:
BOSâNOVA LINK & TALK

This section includes:

- An overview of BOSâNOVA Link & Talk, p. 250

Procedures for the BOSâNOVA IP Telephony network Administrator:

- Link & Talk system requirements, p. 251
- TCP/IP Ports used by Link & Talk, p. 251
- Adding Link & Talk to the Officer Gateway, p. 252
- Establishing a Link & Talk web site, p. 254
- Creating the Link & Talk tag, p. 255
- Reviewing current Link & Talk configuration, p. 259

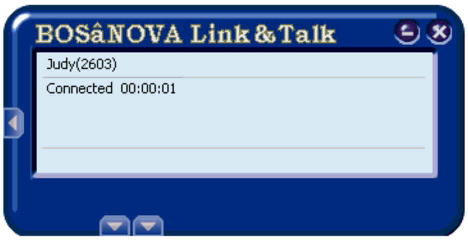
Procedures for BOSâNOVA IP Telephony network Users:

- Installing and uninstalling the Link & Talk PC plug-in, p. 260
- Using Link & Talk, p. 261
- Troubleshooting, p. 262

OVERVIEW

BOSâNOVA Link & Talk is a web phone application that utilizes any BOScom BOSâNOVA IP Telephony Gateway. The application is an ActiveX implementation of Session Interface Protocol (SIP) that can be activated using any kind of HTML tag including a text link, a button, or another image file. The tag can be added to any Web page.

The first time a user clicks the Link & Talk tag, BOSâNOVA Link & Talk is downloaded onto the user's computer. It is added to Microsoft Internet Explorer. Subsequently, each time a user clicks the Link & Talk tag, their version of BOSâNOVA Link & Talk is inspected and, if necessary, updated.



Judy(2603)

Connected 00:00:01

The call process develops as follows:

1. A user browsing with Internet Explorer surfs to a URL with a Link & Talk button, which is hosted on a company's Web server.
2. The URL contains Link & Talk software that points to the BOSâNOVA Gateway Officer IP address and pre-configured phone numbers. When a destination is clicked, the thin client software is downloaded or inspected.
3. Link & Talk software makes a SIP call (to a pre-configured phone number) routed over the Internet to the appropriate BOSâNOVA Gateway.
4. The BOSâNOVA Gateway "terminates" the call to the PSTN or PBX, where the phone or extension rings.

LINK & TALK SYSTEM REQUIREMENTS

PC Processor	Pentium II – 233 MHz compatible or higher / K6-2 processor or higher
Memory	64 Mb minimum
Operating System	Windows 98–Second Edition, Millennium Edition, 2000, and Windows XP
Hard Disk	1 Mb
Software	Microsoft Internet Explorer, version 5.00 or higher
Hardware	Full duplex sound card, microphone, and speakers (or headset)
Network Connection	IP network connection or dial-up connection, 28.8 Kbp or faster

⚠ *BOSâNOVA Link & Talk requires a full duplex sound card. It will not operate with a half-duplex sound card.*

TCP/IP PORTS USED BY LINK & TALK

Table 47: TCP/IP Ports Used by Link & Talk

Port	Protocol	Direction	Description
5060	UDP	In/Out	SIP signaling
25052	UDP	Out	Link & Talk uses this port for sending requests to the Officer
25053	UDP	In	Link & Talk uses this port for receiving Officer responses
30000	UDP	In/Out	RTP

LINK & TALK AND THE OFFICER GATEWAY

There are two steps to integrating BOSâNOVA Link & Talk into an IP Telephony network:

1. Configuring the Officer to recognize the Link & Talk. This step must be completed before step #2.
2. Entering the Officer Gateway's IP address into the Link & Talk Web site's HTML. See "Establishing the Link & Talk Web Site" on page 254.

Link & Talk can only be integrated via the Numbering Plan Configurator of the Officer. See also "Using the Officer Gateway" on page 203.

Adding a Link & Talk to the Officer Gateway

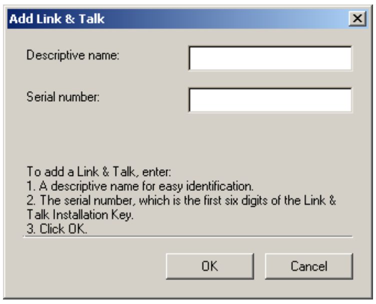
To add a Link & Talk to an IP Telephony network:

1. Obtain a BOSâNOVA Link and Talk Installation Key for each Gateway.
    a. Prepare a list of BOSâNOVA Gateway serial numbers. One Installation Key will be provided for each serial number.
    b. In any Web browser, open the Link & Talk Registration page. At the time of this writing, the full web address is:

       http://www.boscom.com/linkandtalk-registration.htm

    c. Complete and submit the registration form. The Installation Keys will be emailed to the address entered in the registration form.
    d. We recommend also downloading the Link & Talk software now. The software will be needed to create the Link & Talk Web presence. (See "Creating the Link & Talk Web Presence" on page 255.) It can be downloaded from: http://www.boscom.com/linkandtalk-get.htm
2. After receiving the Installation Keys, open the Configurator of the BOSâNOVA IP Telephony network Officer Gateway.
3. From the Configurator main menu, select **Numbering Plan**.
4. From the Parameters Field, select **Common Tables > PC Phones > Link & Talk**. The table is displayed in the Configuration field.
5. Click **Change**. The Link & Talk dialog box opens.

6. Click **Add**. The Add Number dialog box opens.



To add a Link & Talk, enter:
1. A descriptive name for easy identification.
2. The serial number, which is the first six digits of the Link & Talk Installation Key.
3. Click OK.

7. Enter a descriptive name. The descriptive name is a unique name which readily identifies each Link & Talk and each Gateway. The descriptive name can be up to 32 digits long.
8. Enter the serial number. The serial number is the first 6 digits of the BOSâNOVA Link & Talk Installation Key.
9. Click **OK**.

The Officer reviews the list of Link & Talks and sends a message approving or rejecting the list. If the list of Link & Talks is long, the process of reviewing the list may take several minutes.

To define Authentication and Hop-off call permissions for Link and Talks, see Authentication for BOSâNOVA Connects and Link & Talks on page 214.

Modifying a Link & Talk Configuration from the Officer Gateway

To modify a Link & Talk configuration:

1. Open the Configurator of the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan**.
3. From the Parameters Field, select **Common Tables > PC Phones > Link & Talk**. The table is displayed in the Configuration field.
4. Click **Change**. The Link & Talk Numbers dialog box opens.
5. Select a Link & Talk entry.
6. Click **Change**. The Change Number dialog box opens.
7. Enter new information in any of the two fields and click **OK**.

ESTABLISHING THE LINK & TALK WEB SITE

These instructions are intended for Web designers.

Complete this step only after configuring the Officer to recognize the Link & Talk. See “Adding a Link & Talk to the Officer Gateway” on page 252.

There are two steps to establishing Link & Talk Web functionality:

- Create the Link & Talk HTML page
- Add the Link & Talk files and the HTML page to the Web server

Background: The Building Block Files

To establish and maintain a Link & Talk site, the site must include the following files.

These files can be downloaded from the BOScom Link & Talk web site. They are contained within a single zip file named LinkTalk.zip. *At the time of this writing, the download site is: http://www.boscom.com/linkandtalk-get.htm*

- **BsLT*nnnn*.cab**
  This file contains the actual BOSâNOVA Link & Talk, along with two other files. The version number is displayed in place of the *nnnn*.
- **call.html**
  This file contains a message informing the user that BOSâNOVA Link & Talk is loading, for example, “BOSâNOVA Link & Talk is loading. Please wait …” This file can be customized.
- **plugin.js**
  This file contains the **InvokeLinkAndTalk( )** function. In addition, the script contains other functions necessary for loading the Link & Talk ActiveX object.
- **ip.js**
  The ip.js script contains only one Java variable (szLinkAndTalkURL) wherein you define the URL that points to the location of the **BsLT*nnnn*.cab** and **call.html**. By default the variable is empty. Define the URL only if those two files are located in a different place than the plugin.js and the ip.js. See the next section for more explanation.

Creating the Link & Talk Web Presence

1. Ensure that you have downloaded the Link & Talk software. It is contained within a single zip file named LinkTalk.zip. If you have not, it is available from: http://www.boscom.com/linkandtalk-get.htm
2. Extract the Link & Talk software from the LinkTalk.zip file.
3. Ensure that you have the four files listed in "Background: The Building Block Files" on page 254.
4. Create your HTML page. Information and procedures concerning the Link & Talk Web page are documented from pages 255 (immediately below) to page 258.
5. Create a folder on your Web server and place in it the following building block files:
   - **BsLT*nnnn*.cab**
   - **call.html**
6. Save the Link & Talk HTML page and the files **ip.js** and **plugin.js** on the Web server. There are two possibilities:
   - Save them in the same folder created in step 1.
   - Save them in a different location on the server. In this case, define the szLinkAndTalkURL variable in the **ip.js** Java script such that it points to the folder created in step 1. This variable is used in the Plugin.js.

Creating the Link & Talk Tag

1. Include these two links in your Web page before the <BODY> tag:
   - <script language="JavaScript" SRC="./ip.js"></script>
   - <script language="JavaScript" SRC="./plugin.js"></script>

The following two optional scripts are included in the example on page 257. Use these to avoid multiple replacement of the Officer Gateway IP address and Installation Key if they change.
<script language="JavaScript">OfficerIP='1.2.3.4'</script>
<script language="JavaScript">InstKey='80002156V45375'</script>

2. Add a tag for the Link & Talk button or link. You can use text, an image, or an HTML object. Examples of Link & Talk buttons appear on pages 257–258.

3. Customize the tag by editing the following properties:

   For an <a href> HTML tag, add:
   href="javascript:InvokeLinkAndTalk(‘Descriptive text’,‘Officer IP’,‘Target phone number’,‘Installation key’,‘Auto-dial’,‘Auto-close’)"

   For an <input type=button> tag, add:
   onclick="InvokeLinkAndTalk(‘Descriptive text’,‘Officer IP’,‘Target phone number’,‘Installation key’,‘Auto-dial’,‘Auto-close’)"

   In both cases, the definitions are as follows:

   - Descriptive text:
     Text that is displayed in the Link & Talk window.
   - Officer IP:
     The BOSâNOVA IP Telephony network’s Officer Gateway’s IP address.
   - Target phone number:
     The phone number the Link & Talk button calls.

To use Link & Talk to dial a public number, this parameter must be defined according to the ITU E.164 format, that is, country code, area code etc. For an explanation of E.164, see “ITU E.164 Standard” on page 83.

   - Installation key:
     The string of numbers and letters which identifies this BOSâNOVA Link & Talk to the BOSâNOVA IP Telephony network’s Officer Gateway. The first six digits of this string is the serial number that must be entered into the Officer Gateway. See step 8 on page 253.
   - Auto-dial:
     A setting which determines if the call is placed as soon as the Web site’s button is clicked. If this parameter is defined as 1, the call is dialed immediately. If this parameter is defined as 0, the call is dialed when the Call button is pushed.
   - Auto-close:
     A setting which determines if Link & Talk closes as soon as the call is disconnected. If this parameter is defined as 1, Link & Talk closes automatically. If this parameter is defined as 0, Link & Talk remains open.

Examples of Link & Talk HTML

The following illustrates a list of targets called by text links in an HTML table made up of two rows with two cells per row. The Link & Talk components are indicated in bold.

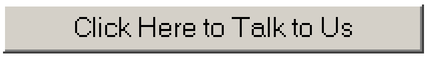
```
<html>
<head>
<title>BOSaNOVA Link & Talk Example Page</title>
<META HTTP-EQUIV="Pragma" CONTENT="no-cache"> <META HTTP-EQUIV="Expires" CONTENT="-1">
</head>

<script language="JavaScript" SRC="./plugin.js"></script>
<script language="JavaScript" SRC="./ip.js"></script>

<script language="JavaScript">OfficerIP='1.2.3.4'</script>
<script language="JavaScript">InstKey='80002156V45375'</script>

<body >
<p dir="ltr" align="center">
<font size="5" color="maroon" face="Verdana">Company Phone Directory</font></p>

<div align="center">
<table border="1" cellpadding="0" cellspacing="0" style="border-collapse: collapse" bordercolor="#111111"
width="50%" id="AutoNumber1">
  <tr>
   <td width="50%">&nbsp;
    <a href="javascript:InvokeLinkAndTalk ('John Ray', OfficerIP,'1111', InstKey, '1', '1')">
    John Ray</a>
   </td>
   <td width="50%">&nbsp;
    <a href="javascript:InvokeLinkAndTalk ('David Davidson', OfficerIP,'1112', InstKey, '1', '1')">
    David Davidson</a>
   </td>
  </tr>
  <tr>
   <td width="50%">&nbsp;
    <a href="javascript:InvokeLinkAndTalk ('Nik Nicolson', OfficerIP,'1113', InstKey, '1', '1')">
    Nik Nicolson</a>
   </td>
   <td width="50%">&nbsp;
    <a href="javascript:InvokeLinkAndTalk ('Peter Peterson', OfficerIP,'1114', InstKey, '1', '1')">
    Peter Peterson</a>
   </td>
  </tr>
</table>
</div>
</body>

</html>
```

Following are other examples of links that could be used to initiate a Link & Talk call. The HTML for each of these is a variation of that which appears on the preceding page. Ensure that the Link & Talk components are included as per instructions.

A single text link:

Click **Here** to Talk to Us

A plain HTML button:



Click Here to Talk to Us

A graphic button:

A graphic button with accompanying text:

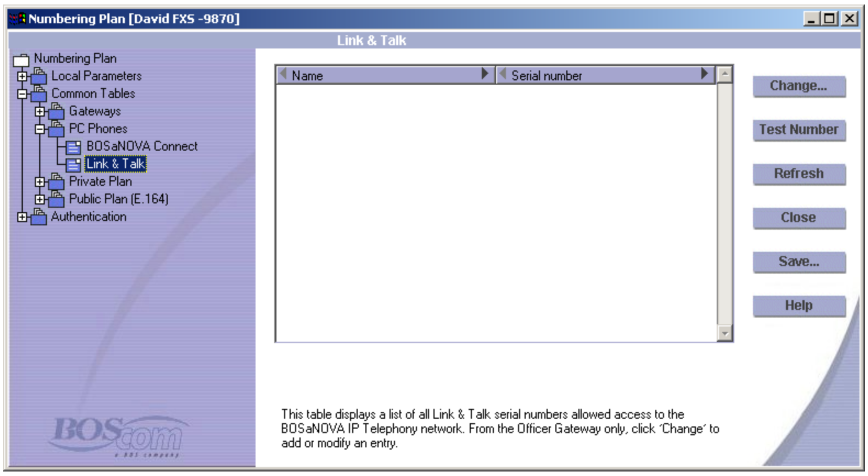
Talk to Us

REVIEWING CURRENT LINK & TALK CONFIGURATION

Link & Talk configuration can be reviewed from any Gateway. However, new Link & Talks can only be integrated via the Numbering Plan Configurator of the Officer. See "Adding a Link & Talk to the Officer Gateway" on page 252.

To review the current Link & Talk configuration on an IP Telephony network:

1. Open the Configurator of the Officer Gateway.
2. From the Configurator main menu, select **Numbering Plan**.
3. From the Parameters Field, select **Common Tables > PC Phones > Link & Talk**. The table is displayed in the Configuration field.



This table displays a list of all Link & Talk serial numbers allowed access to the BOSaNOVA IP Telephony network. From the Officer Gateway only, click 'Change' to add or modify an entry.

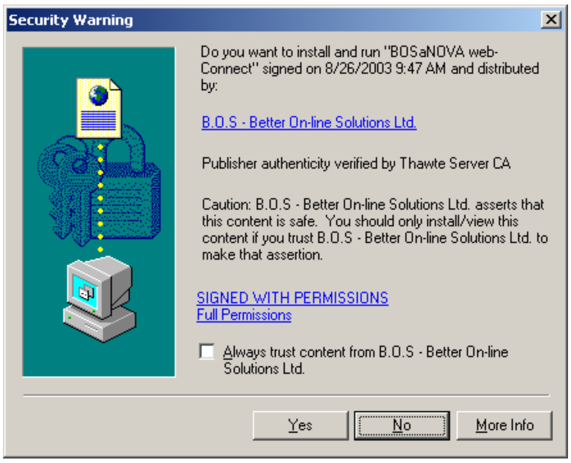
Two columns appear in the Link & Talk Configuration table.

- **Name**
  This is the descriptive name that has been assigned to a Link & Talk. The descriptive name is a unique name which readily identifies each Link & Talk. The descriptive name can be up to 32 digits long.
- **Serial Number**
  The serial number is the first 6 digits of the BOSâNOVA Link & Talk Installation Key.

INSTALLING a LINK & TALK PC PLUG-IN

To install the BOSâNOVA Link & Talk plug-in:

1. Open Microsoft Internet Explorer.
2. Enter the IP address of the Web site hosting the Link & Talk tag.
3. Click the Link & Talk button. A security message appears:



Security Warning

Do you want to install and run "BOSaNOVA web-Connect" signed on 8/26/2003 9:47 AM and distributed by:

B.O.S - Better On-line Solutions Ltd.

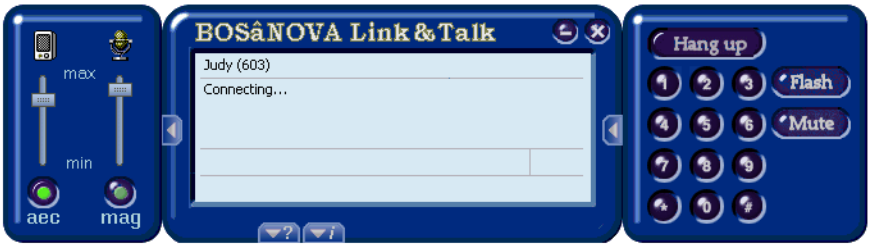
Publisher authenticity verified by Thawte Server CA

Caution: B.O.S - Better On-line Solutions Ltd. asserts that this content is safe. You should only install/view this content if you trust B.O.S - Better On-line Solutions Ltd. to make that assertion.

SIGNED WITH PERMISSIONS
Full Permissions

□ Always trust content from B.O.S - Better On-line Solutions Ltd.

4. Click **Yes**. The plug-in is downloaded, the BOSâNOVA Link & Talk opens, and the call is dialed.



Judy (603)

Connecting...

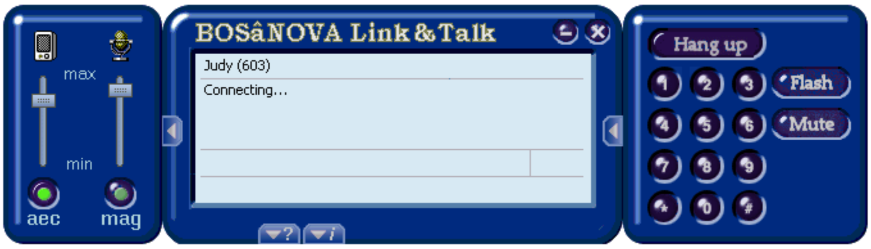
UNINSTALLING LINK & TALK

The following instructions are for Explorer version 5.5. The procedure for other versions may differ slightly.

1. Open Microsoft Internet Explorer.
2. Click **Tools** > **Internet Options**. The Internet Options dialog box is displayed.
3. From the General tab, click **Settings** > **View Objects**.
4. Select **BsWebActX Control**.
5. Click **Delete**. The Remove Program File confirmation message appears.
6. Click **Yes**.
7. Click **OK** until the Internet Options dialog box is closed.

USING LINK & TALK

Clicking the Link & Talk tag opens BOSâNOVA Link & Talk with the right and left panes displayed. BOSâNOVA Link & Talk automatically dials the call. The bottom pane is hidden.



Judy (603)

Connecting...

The following options are available from the right pane:

- Before the call is answered, only the Hang up button is operative.
- After the call is answered:
  - Use the number-pad exactly as if it were a telephone’s number-pad.
  - Click **Flash**, and dial the extension, to forward a call to another end-point.
  - Click **Mute** to disable the microphone. Click Mute a second time to enable the microphone.

The following options are available from the left pane:

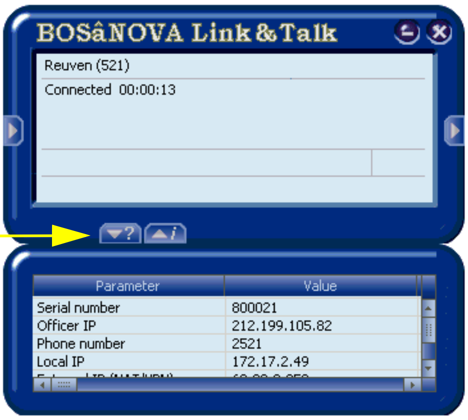
- Enable or disable Acoustic Echo Cancellation (aec)
  Your partner might hear an echo. This occurs when your microphone picks up the sound from your speakers and transfers it back to your partner. With aec enabled, that effect is significantly reduced. By default, aec is enabled. Click the button to disable it.

To eliminate the acoustic echo effect totally, we recommend using a headset instead of external speakers.

- Manually set the level of your speaker (headset) volume
  Use the slide control above the aec button to set the volume level of your speakers or headset.
- Enable or disable Microphone Automatic Gain (mag)
  Mag regulates the volume heard by the person you are speaking with. By default, mag is enabled. Click the button to disable it.
- Manually set the level of microphone gain
  When disabled, manually tune the microphone gain using the slide control.

Two displays are available from the bottom pane:

- “About” information pertaining to the current version of BOSâNOVA Link & Talk
- Parameters pertaining to the current configuration of BOSâNOVA Link & Talk



Reuven (521)

Connected 00:00:13

Parameter	Value
Serial number	800021
Officer IP	212.199.105.82
Phone number	2521
Local IP	172.17.2.49

Click this arrow to display and hide the left pane.

Click these arrows to display and hide the bottom panes.

Click this arrow to display and hide the right pane.

TROUBLESHOOTING

If you cannot download Link & Talk, verify that your browser is set to download clients.

1. Close all Internet Explorer windows except for one.
2. Select **Tools** > **Internet Options** (IE5).
3. Click the **Security** tab.
4. Select the **Internet** icon and click **Custom Level**.
5. Scroll to locate the **Run ActiveX controls and plug-ins** setting.
6. Select **Enable**.
7. Scroll to locate the **Download signed ActiveX controls** setting.
8. Select **Enable**.
9. Click **OK** to accept the changes and to exit the dialog boxes.

If you can’t hear the person you called or can't be heard:

1. Verify that your microphone and speakers are installed and configured correctly and are turned on.
2. Verify that your PC has a full-duplex sound card. BOSâNOVA Link & Talk is not compatible with half-duplex sound cards.

IP Telephony...
Clear and Simple

SECTION 16: GATEWAY MONITOR

This section includes:

- Overview of the Gateway Monitor, see p. 264
- Gateway Log Monitor, see p. 264
- Gateway Ports Monitor, see p. 266
- Call Detail Records (CDR) Monitor, see p. 267
- Quality Service Records (QSR) Monitor, see p. 269

The information displayed on a Gateway Monitor depends upon the type of Gateway. For example, the information displayed on an analog Gateway's monitor is different than the information displayed on a digital Gateway's monitor. This section provides an overview of the Gateway Monitor but does not detail every monitor configuration.

OVERVIEW

Use the Gateway Monitor to examine current Gateway usage.

The Gateway monitor can display four tables:

- Gateway Log
  a record of all Warning, Error and Alert messages
- Ports
  a table showing all the Gateway ports and their status
- Call Detail Records
  a table showing specific parameters from the CDR trace buffer
- Quality of Service Records
  a table showing specific parameters from the QSR trace buffer

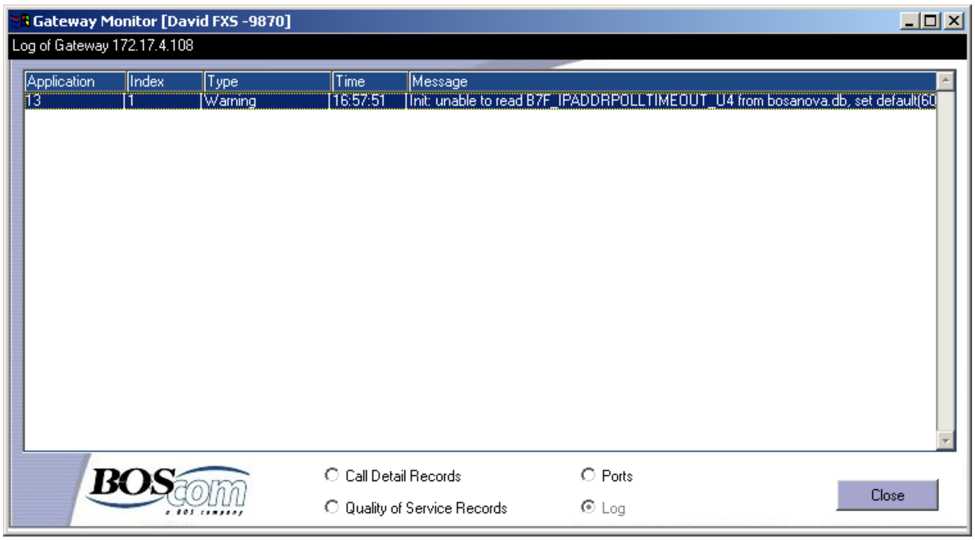
In addition to the categories explained below, the Gateway Monitor uses colors to report the Gateway status.

- The color yellow (YELLOW) indicates that the line is connected.
- The color turquoise (TURQUOISE) indicates that a connection is in progress.
- The color green (GREEN) indicates that the line is enabled but not in use.
- The color gray (GRAY) indicates that the line is disabled.

Gateway Log Monitor

To open the Gateway Log monitor:

1. In a browser, enter the IP address of the Gateway and press Enter. The Configurator Welcome screen appears.
2. Enter the password and click Login. The Configurator main menu appears.
3. Select **Gateway Monitor**.
4. Select **View Log**. The Log screen is displayed.



Log of Gateway 172.17.4.108

Application	Index	Type	Time	Message
13	1	Warning	16:57:51	Init: unable to read B7F_IPADDRPOLLTIMEOUT_U4 from bosanova.db, set default(60

○ Call Detail Records ○ Ports

○ Quality of Service Records ● Log

The Gateway Log is primarily a tool for BOScom Technical Support. There are a number of circumstances when BOScom Technical Support might ask you to refer to the log.

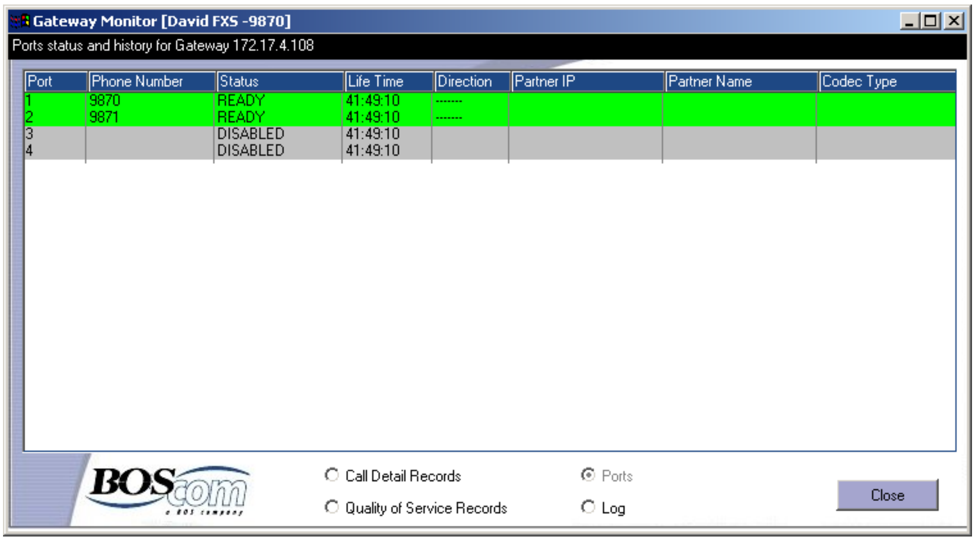
The following information is displayed in the log:

- **Application**
  This is internal information regarding the model of the Gateway.
- **Index**
  This is internal information regarding the model of the Gateway.
- **Type**
  There are Warning, Error, and Alert messages.
- **Time**
  This column contains the time when the message was issued.
- **Message**
  This column contains the content of the message.

Gateway Ports Monitor

To open the Gateway Ports monitor:

1. In a browser, enter the IP address of the Gateway and press Enter. The Configurator Welcome screen appears.
2. Enter the password and click Login. The Configurator main menu appears.
3. Select **Gateway Monitor**. The Ports status screen is displayed.



Gateway Monitor [David FXS -9870]

Ports status and history for Gateway 172.17.4.108

Port	Phone Number	Status	Life Time	Direction	Partner IP	Partner Name	Codec Type
1	9870	READY	41:49:10	-------			
2	9871	READY	41:49:10	-------			
3		DISABLED	41:49:10				
4		DISABLED	41:49:10				

The following information is displayed in the lines table:

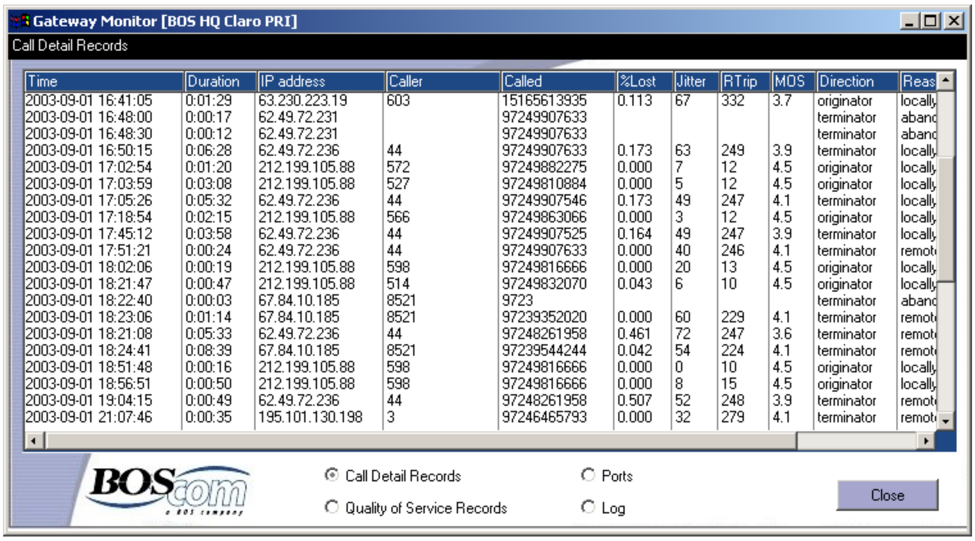
- **Port**
  This number corresponds to the port number on the back of the Gateway.
- **Phone Number**
  This displays the phone number that was called via the monitored Gateway.
- **Status**
  The Gateway's status can be either Ready, Disabled, or Connected. Call progress status can be any of the following:
  - Ring
  - Dialing
  - Off hook
  - Connecting
  - Busy due to time-out
  - Busy due to disconnect
  - Busy due to invalid number
  - Busy

- **Life Time**
  This displays the duration of the latest status. Each time the status changes, the count begins anew.
- **Direction**
  - If the monitored Gateway received the call, the direction is **In**.
  - If the call was outgoing via the monitored Gateway, the direction is **Out**.
- **Partner IP Address**
  The IP address of the second Gateway, that is, the Gateway the monitored Gateway is connected to.
- **Partner Name**
  The name of the second Gateway, that is, the Gateway the monitored Gateway is connected to. A name can be either words or numbers.
- **Codec Type**
  The codec being used by the two Gateways.

Call Detail Records (CDR)

To open the Gateway CDR monitor:

1. In a browser, enter the IP address of the Gateway and press Enter. The Configurator Welcome screen appears.
2. Enter the password and click Login. The Configurator main menu appears.
3. Select **Gateway Monitor**.
4. Select **Call Detail Records**.



Time	Duration	IP address	Caller	Called	%Lost	Jitter	RTrip	MOS	Direction	Reas
2003-09-01 16:41:05	0:01:29	63.230.223.19	603	15165613935	0.113	67	332	3.7	originator	locally
2003-09-01 16:48:00	0:00:17	62.49.72.231		97249907633					terminator	aband
2003-09-01 16:48:30	0:00:12	62.49.72.231		97249907633					terminator	aband
2003-09-01 16:50:15	0:06:28	62.49.72.236	44	97249907633	0.173	63	249	3.9	terminator	locally
2003-09-01 17:02:54	0:01:20	212.199.105.88	572	97249882275	0.000	7	12	4.5	originator	locally
2003-09-01 17:03:59	0:03:08	212.199.105.88	527	97249810884	0.000	5	12	4.5	originator	locally
2003-09-01 17:05:26	0:05:32	62.49.72.236	44	97249907546	0.173	49	247	4.1	terminator	locally
2003-09-01 17:18:54	0:02:15	212.199.105.88	566	97249863066	0.000	3	12	4.5	originator	locally
2003-09-01 17:45:12	0:03:58	62.49.72.236	44	97249907525	0.164	49	247	3.9	terminator	locally
2003-09-01 17:51:21	0:00:24	62.49.72.236	44	97249907633	0.000	40	246	4.1	terminator	remot
2003-09-01 18:02:06	0:00:19	212.199.105.88	598	97249816666	0.000	20	13	4.5	originator	locally
2003-09-01 18:21:47	0:00:47	212.199.105.88	514	97249832070	0.043	6	10	4.5	originator	locally
2003-09-01 18:22:40	0:00:03	67.84.10.185	8521	9723					terminator	aband
2003-09-01 18:23:06	0:01:14	67.84.10.185	8521	97239352020	0.000	60	229	4.1	terminator	remot
2003-09-01 18:21:08	0:05:33	62.49.72.236	44	97248261958	0.461	72	247	3.6	terminator	remot
2003-09-01 18:24:41	0:08:39	67.84.10.185	8521	97239544244	0.042	54	224	4.1	terminator	remot
2003-09-01 18:51:48	0:00:16	212.199.105.88	598	97249816666	0.000	0	10	4.5	originator	locally
2003-09-01 18:56:51	0:00:50	212.199.105.88	598	97249816666	0.000	8	15	4.5	originator	locally
2003-09-01 19:04:15	0:00:49	62.49.72.236	44	97248261958	0.507	52	248	3.9	terminator	remot
2003-09-01 21:07:46	0:00:35	195.101.130.198	3	97246465793	0.000	32	279	4.1	terminator	remot

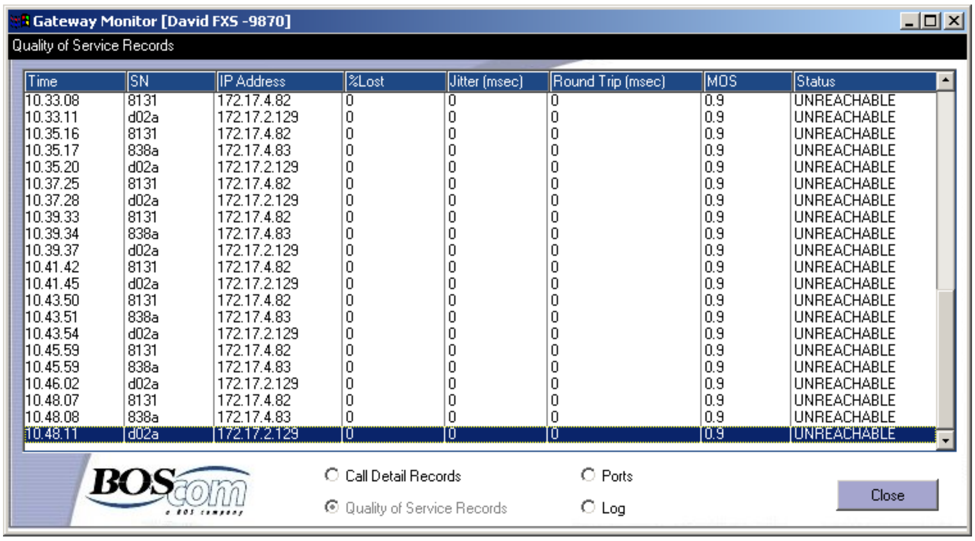
The CDR log displays:

- **Time**
  This displays the time of the call as recorded on the Gateway.
- **Duration**
  This displays the duration of the call in hours, minutes, and seconds.
- **IP Address**
  This displays the IP address of the partner Gateway.
- **Caller**
  This display identifies the ID number of the originator of the call.
- **Called Number**
  This display identifies the ID number of the recipient of the call.
- **% Lost**
  This displays the percent of packages lost en route.
- **Jitter**
  This displays the time delay of individual packets relative to the other packets in a transmission in milliseconds.
- **Round Trip**
  This displays the time in milliseconds for the transmission of packets from the initiating Gateway to the Receiving Gateway and back again.
- **MOS**
  Mean Opinion Score-a subjective evaluation of the voice quality of a transmission; 1 being poor, 5 being excellent.
- **Call Direction**
  This displays the direction of the call; which Gateway, initiator or terminator made the call.
- **Reason**
  This displays the reason for termination of the call.
  - Normal
  - Busy
  - Abandoned
  - Not resolved
  - Other
- **Codec**
  Displays the codec used by the two Gateways

Quality of Service Records (QSR)

To open the Gateway QSR monitor:

1. In a browser, enter the IP address of the Gateway and press Enter. The Configurator Welcome screen appears.
2. Enter the password and click Login. The Configurator main menu appears.
3. Select **Gateway Monitor**.
4. Select **QSR**.



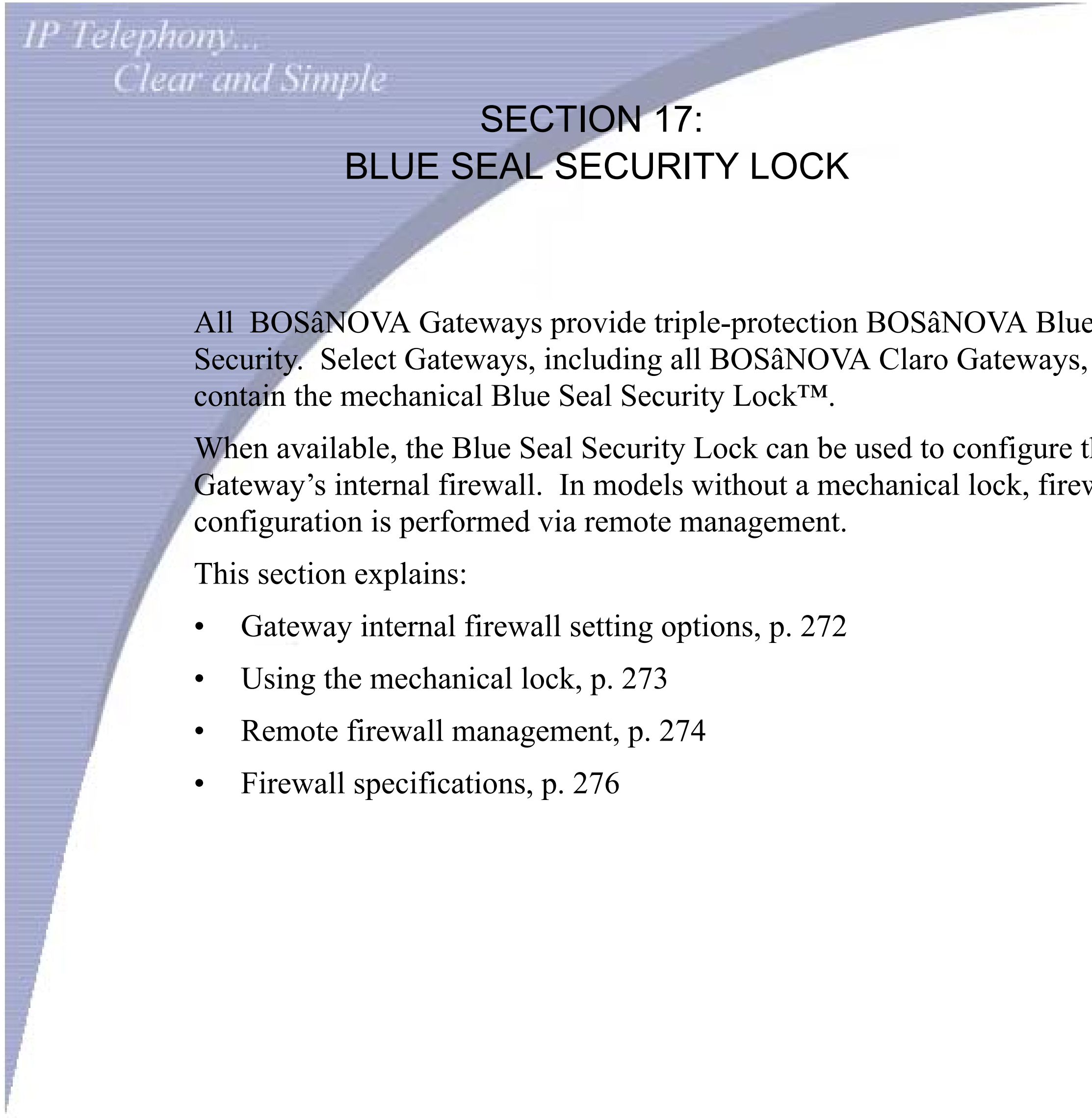
Time	SN	IP Address	%Lost	Jitter (msec)	Round Trip (msec)	MOS	Status
10.33.08	8131	172.17.4.82	0	0	0	0.9	UNREACHABLE
10.33.11	d02a	172.17.2.129	0	0	0	0.9	UNREACHABLE
10.35.16	8131	172.17.4.82	0	0	0	0.9	UNREACHABLE
10.35.17	838a	172.17.4.83	0	0	0	0.9	UNREACHABLE
10.35.20	d02a	172.17.2.129	0	0	0	0.9	UNREACHABLE
10.37.25	8131	172.17.4.82	0	0	0	0.9	UNREACHABLE
10.37.28	d02a	172.17.2.129	0	0	0	0.9	UNREACHABLE
10.39.33	8131	172.17.4.82	0	0	0	0.9	UNREACHABLE
10.39.34	838a	172.17.4.83	0	0	0	0.9	UNREACHABLE
10.39.37	d02a	172.17.2.129	0	0	0	0.9	UNREACHABLE
10.41.42	8131	172.17.4.82	0	0	0	0.9	UNREACHABLE
10.41.45	d02a	172.17.2.129	0	0	0	0.9	UNREACHABLE
10.43.50	8131	172.17.4.82	0	0	0	0.9	UNREACHABLE
10.43.51	838a	172.17.4.83	0	0	0	0.9	UNREACHABLE
10.43.54	d02a	172.17.2.129	0	0	0	0.9	UNREACHABLE
10.45.59	8131	172.17.4.82	0	0	0	0.9	UNREACHABLE
10.45.59	838a	172.17.4.83	0	0	0	0.9	UNREACHABLE
10.46.02	d02a	172.17.2.129	0	0	0	0.9	UNREACHABLE
10.48.07	8131	172.17.4.82	0	0	0	0.9	UNREACHABLE
10.48.08	838a	172.17.4.83	0	0	0	0.9	UNREACHABLE
10.48.11	d02a	172.17.2.129	0	0	0	0.9	UNREACHABLE

*The records displayed on this monitor indicate the Quality of Service (QoS) between Gateways, **not** the QoS achieved during a specific phone call. This information is helpful, therefore, for decisions regarding routing.*

The QSR log displays:

- **Time**
  This displays the time of the call as recorded on the Gateway.
- **SN**
  This displays the serial number of the partner Gateway.
- **IP Address**
  This displays the IP address of the partner Gateway.
- **% Lost**
  This displays the percent of packages lost en route.

- **Jitter**
  This displays the time delay of individual packets relative to the other packets in a transmission (in milliseconds).
- **Round Trip**
  This displays the time in milliseconds for the transmission of packets from the initiating Gateway to the terminating Gateway and back again.
- **MOS**
  Mean Opinion Score-a subjective evaluation of the voice quality of a transmission; 1 being poor, 5 being excellent.
- **Status**
  This displays the status of the line.



SECTION 17:
BLUE SEAL SECURITY LOCK

All BOSâNOVA Gateways provide triple-protection BOSâNOVA Blue Seal Security. Select Gateways, including all BOSâNOVA Claro Gateways, contain the mechanical Blue Seal Security Lock™.

When available, the Blue Seal Security Lock can be used to configure the Gateway's internal firewall. In models without a mechanical lock, firewall configuration is performed via remote management.

This section explains:

- Gateway internal firewall setting options, p. 272
- Using the mechanical lock, p. 273
- Remote firewall management, p. 274
- Firewall specifications, p. 276

INTERNAL FIREWALL SETTINGS

Detailed firewall specifications are listed beginning on page 276.

The Blue Seal Security Lock can be set to any of three settings:

Disabled:

When the firewall is disabled, all Gateway ports send and receive all packet types.

Medium:

When the firewall is set to medium, the following packets are rejected:

- All packets similar to port-scanner packets
- All junk packets
- User defined rules as configured in the Terminal Server. (See “Remote Management” on page 274 for details about user defined rules.)
- Packets not matching one of 23 acceptable packet types

High:

When the firewall is set to high, the following packets are rejected:

- All packets similar to port-scanner packets
- All junk packets
- All ping requests
- Packets not matching one of ***only*** 12 acceptable packet types

NAT, firewall, DNS, and DHCP may not work with the high setting.

CONFIGURING THE BLUE SEAL SECURITY LOCK

If the key is lost, using Remote Management (see see p. 274) the setting can be lowered to medium. However, the key is needed to turn the firewall to OFF. Contact your BOScom dealer for replacement keys.

The Blue Seal Security Lock can be disabled or set to either medium or high.

Turning Off the Blue Seal Security Lock

Turning the key to OFF disables the Blue Seal Security Lock. The factory default setting is OFF.

When disabled, the blue LED is turned off.

Selecting a Protection Level

Select a level of security using the key as a toggle switch.

Each OFF > ON cycle toggles the level of security from medium to high to medium to high, etc.

Medium Security

From the factory set default OFF setting, turn the key to ON.

From the high security level, turn the key to OFF and then turn it to ON.

When set to medium, the blue LED flashes.

High Security

From the medium security level, turn the key to OFF and then turn it to ON.

When set to high, the blue LED remains illuminated.

REMOTE MANAGEMENT

Two options exist for remote management of the Blue Seal Security Lock. These options are also used to set the firewall on models without a mechanical lock.

Using the Maintenance Wizard

General documentation concerning the Maintenance Wizard begins with the chapter "Maintenance Wizard's Primary Applications" on page 293.

To configure the Blue Seal Security Lock over a LAN/WAN using the Maintenance Wizard:

1. From the Welcome Screen of the BOSâNOVA IP Telephony CD-ROM, select Run Maintenance Wizard. The Maintenance Wizard Welcome screen appears.
2. Select **Connect to any Gateway with a known IP address** and click **Next**. The "Select a specific Gateway" screen appears.
3. Enter the IP address and password of the Gateway and click **Next**. The "Product Information and Task Selection" screen appears.
4. Select **Open Terminal Server** (task number 10) and click **Next**. The "Open Terminal Server" screen appears.
5. Click **Start**. The Terminal Server main menu appears.
6. Using the keyboard's UP and DOWN arrow keys, select **Change the network configuration**.
7. Using the keyboard's UP and DOWN arrow keys, select **OK** and press **Enter**. The Network Configuration menu appears.
8. Select **Change Gateway firewall configuration** and click **OK**. The Gateway Firewall dialog box appears.
9. Select Yes or No and press **Enter**. If you selected Yes, the Configure Filtering screen appears.
10. Configure the firewall and close the Terminal Server. For assistance with configuration parameters, contact Technical Support.

Using a PC and a Serial Connection (RS-232)

To configure the Blue Seal Security Lock using a PC through a serial connection (RS-232):

1. Turn on the Gateway and wait 1–2 minutes for the system to boot.
2. Attach a Windows-based PC to the Gateway via the COM port on the rear panel of the Gateway.
3. Click **Start** > **Programs** > **Accessories** > **Communications** > **HyperTerminal**. HyperTerminal opens.
4. Follow the HyperTerminal prompts:

   a. Assign a name to the connection and click **OK**.

   b. In the **Connect using** field of the Connect to dialog box, select the correct COM port and click **OK**.

   c. In the **Port Settings** dialog box, enter the following parameters:

   - **Bits per second**: 115200
   - **Data bits**: 8
   - **Parity**: None
   - **Stop bits**: 1
   - **Flow control**: Hardware

   Click **OK**.
5. Press **Enter**. This connects the PC to the Gateway.
6. At the BOSâNOVA login prompt, *using lowercase letters only*, enter **voip** and press **Enter**.
7. Enter the password and press **Enter**. The default password is **1234**. The Terminal Server Main Menu is displayed.
8. Using the keyboard's UP and DOWN arrow keys, select **Change the network configuration**.
9. Using the keyboard's UP and DOWN arrow keys, select **OK** and press **Enter**. The Network Configuration menu appears.
10. Select **Change Gateway firewall configuration** and click **OK**. The Gateway Firewall dialog box appears.
11. Select Yes or No and press **Enter**. If you selected Yes, the Configure Filtering screen appears.
12. Configure the firewall and close the Terminal Server. For assistance with configuration parameters, contact Technical Support.

FIREWALL SPECIFICATIONS

Table 48: Medium, blue LED flashes

All packets similar to port-scanner packets	reject
All invalid packets (junk)	reject
All packets that appear to belong to an already established connection	accept
RTP/RTCP/UDPTL, 30000–30256/udp	accept
H.323 host call progress, 1720/tcp	accept
Officer ↔ Private Numbering Plan, 25050/tcp	accept
BOSâNOVA Connect ↔ Gateway, 25052/udp	accept
BOSâNOVA Connect ↔ Gateway, 25053/udp	accept
BOSâNOVA Connect ↔ Gateway, 25052/tcp	accept
All TCP ports greater than 1024 including: PPTP 1723/tcp jCentral ↔ BOSmaster 25051/tcp QoS 25054/tcp H.245 negotiations All TCP ports greater then 1024	accept
QoS dynamic, 25100–25000/udp	accept
QoS modem backup, 25055/udp	accept
QoS NQS, 25060/udp	accept
All ports, destination IP is any of default Gateways	accept
DHCP, 67/udp and 68/udp	accept
GRE (needed for pptp), IP protocol 47, accept only to/from defined PPtP server.	accept
All packets originated and destined to/from local IP (127.0.0.1)	accept
SSH, 22/tcp	accept
Maintenance Wizard → Gateway, 4567/udp	accept
Gateway → Maintenance Wizard, 4568/udp	accept.
SNMP, 161/udp	accept
WEB, 80/tcp, accept only for incoming connections	accept
DNS, 53/udp, accept only to/from defined DNS server	accept

Table 48: Medium, blue LED flashes

NTP, 123/udp (time synchronization), accept only to/from defined servers.	accept
Ping requests, accept but limit response rate to 1 response in 1 second	accept
User defined rules (port, IP, port + IP)	reject or accept
Packets not matching one of the 23 acceptable packet types listed above	reject or accept as defined by user’s policy

Table 49: High, blue LED is on

All packets similar to port-scanner packets	reject
All invalid packets (junk)	reject
All packets that appear to belong to an already established connection	accept
RTP/RTCP/UDPTL, 30000–30256/udp	accept
H.323 call progress, 1720/tcp	accept
Officer ↔ Private numbering plan, 25050/tcp	accept
BOSâNOVA Connect ↔ Gateway, 25052/udp	accept
BOSâNOVA Connect ↔ Gateway, 25053/udp	accept
BOSâNOVA Connect ↔ Gateway, 25052/tcp	accept
Ping requests	reject
All ports, destination is any of default routers	accept
PPTP,1723/tcp, accept only to/from defined PPtP server	accept
DHCP, 67/udp and 68/udp	accept
GRE (needed for pptp), IP protocol 47, accept only to/from defined PPtP server	accept
All packets originated and destined to/from local IP (127.0.0.1)	accept
Packets not matching one of ***only*** 12 acceptable packet types listed above	reject

IP Telephony...
Clear and Simple

SECTION 18:
COMMAND LINE CONFIGURATOR and HIDDEN PARAMETERS

BOSâNOVA Gateways with software version 2.13.00 and higher are equipped with a BOScom utility called the Command Line Configurator (CLC). The BOSâNOVA Command Line Configurator provides access to all database files and parameters, including parameters that do not appear in the browser based Configurators.

In addition, because it is possible to run scripts on the BOSâNOVA Command Line Configurator, it can be used by IP Telephony terminators to facilitate efficient configuration of a large number of Gateways.

This section explains:

- How to access the BOSâNOVA CLC, see p. 279
- CLC commands, see p. 280
- Running scripts using the CLC, see p. 285
- Hidden parameters that can be accessed using the CLC, see p. 286

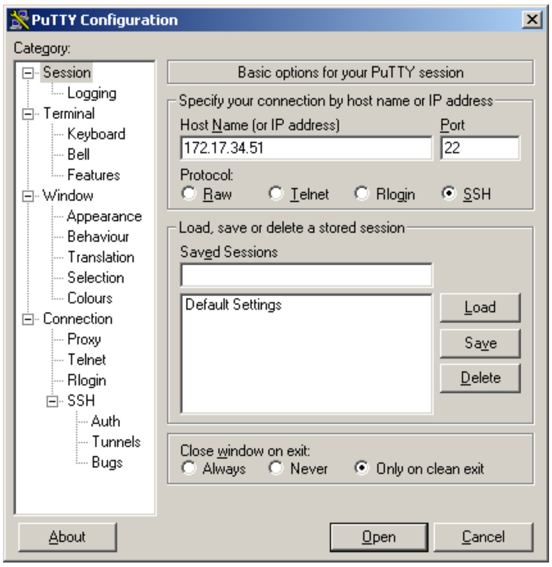
ACCESSING THE COMMAND LINE CONFIGURATOR

The Command Line Configurator (CLC) can be accessed:

- If a keyboard and monitor are attached to the Gateway, by pressing F2. The console session will be displayed.
- Via an RS-232 terminal connected to the Gateway's RS-232 port.
- Using an SSH program which implements the client end of a remote session. There are several free SSH clients available from the internet. The example used in this procedure is named PuTTY. It can be downloaded from:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

1. Run your SSH client.



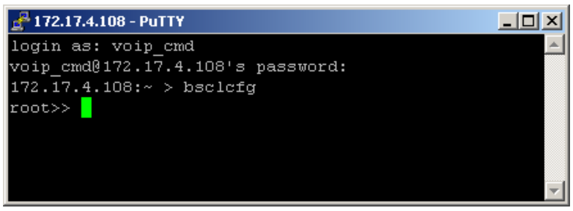
Host Name (or IP address): 172.17.34.51

Port: 22

Protocol: ○ Raw ○ Telnet ○ Rlogin ● SSH

Close window on exit: ○ Always ○ Never ● Only on clean exit

2. Enter the IP address of the Gateway.
3. Ensure that **SSH** is selected.
4. Click **Open**. The login screen is displayed.



```
login as: voip_cmd
voip_cmd@172.17.4.108's password:
172.17.4.108:~ > bsclcfg
root>>
```

5. At the login prompt, type **`voip_cmd`** and press **Enter**.
6. Enter the password. The default password is 1234. Press **Enter**.
7. At the IP address prompt, type **`/opt/BOSutils/bsclcfg`** and press **Enter**.

8. At the **`root >>`** prompt, and at all subsequent prompts, type a command and press **Enter**.

   Alternately, to display a list of commands available for the specific prompt, type **`help`** or enter a question mark—**?**— and press **Enter**.

A sample procedure, How to change the Maximum Call Duration, is provided on page 282.

Command Line Configurator (CLC) Commands

Table 50: Commands Available from the Root Level

Command	Result
apply	Applies all changes (<[force] [silent]>)
enter	Enters the configuration mode of the specified database or table. Type the name of the database, including the extension, after the word **`enter`**. For example: **`enter bosanova.db`**
?, help	Displays all commands available for this branch
list	Displays a list of available databases
print	Displays all database tables and table data
prn_mod	Changes the display mode (<1> - aligned by columns, <2> - not aligned)
quit	Quits the program
refresh	Resets all tables with content from the databases

Table 51: Commands Available from the Database Level

Command	Result
apply	Applies all changes (<[force] [silent]>)
enter	Enters the configuration mode of the specified database or table. Type the name of the database, including the extension, after the word **`enter`**. For example: **`enter bosanova.db`**
exit	Exits to a previous branch

Table 51: Commands Available from the Database Level

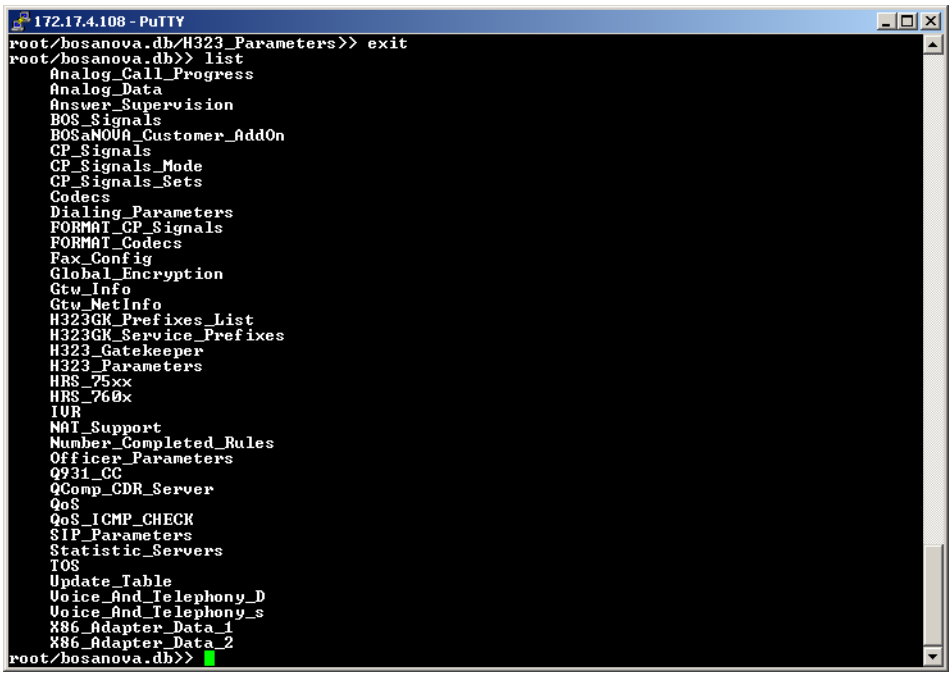
Command	Result
exit!	Exits to the 'root' branch
?, help	Displays all commands available for this branch
list	Displays a list of tables available for this databases
print	Displays the content of all tables
prn_mod	Changes the display mode (<1> - aligned by columns, <2> - not aligned)
quit	Quits the program
refresh	Resets all tables with content from the databases

Table 52: Commands Available from the Table Level

Command	Result
add	Adds a row to the table (<param_name param_value>)
apply	Applies all changes (<[force] [silent]>)
clr	Deletes all rows from the table
del	Deletes a row from the table (<param_name>)
exit	Exits to a previous branch
exit!	Exits to the 'root' branch
?, help	Displays all commands available for this branch
print	Displays the content of the table
prn_col	Prints the specified column (<column_number>)
prn_mod	Changes the display mode (<1> - aligned by columns, <2> - not aligned)
prn_row	Prints the specified row (<row_number>)
quit	Quits the program
refresh	Resets all tables with content from the databases
set	Changes a row in the table (<param_name param_value>)

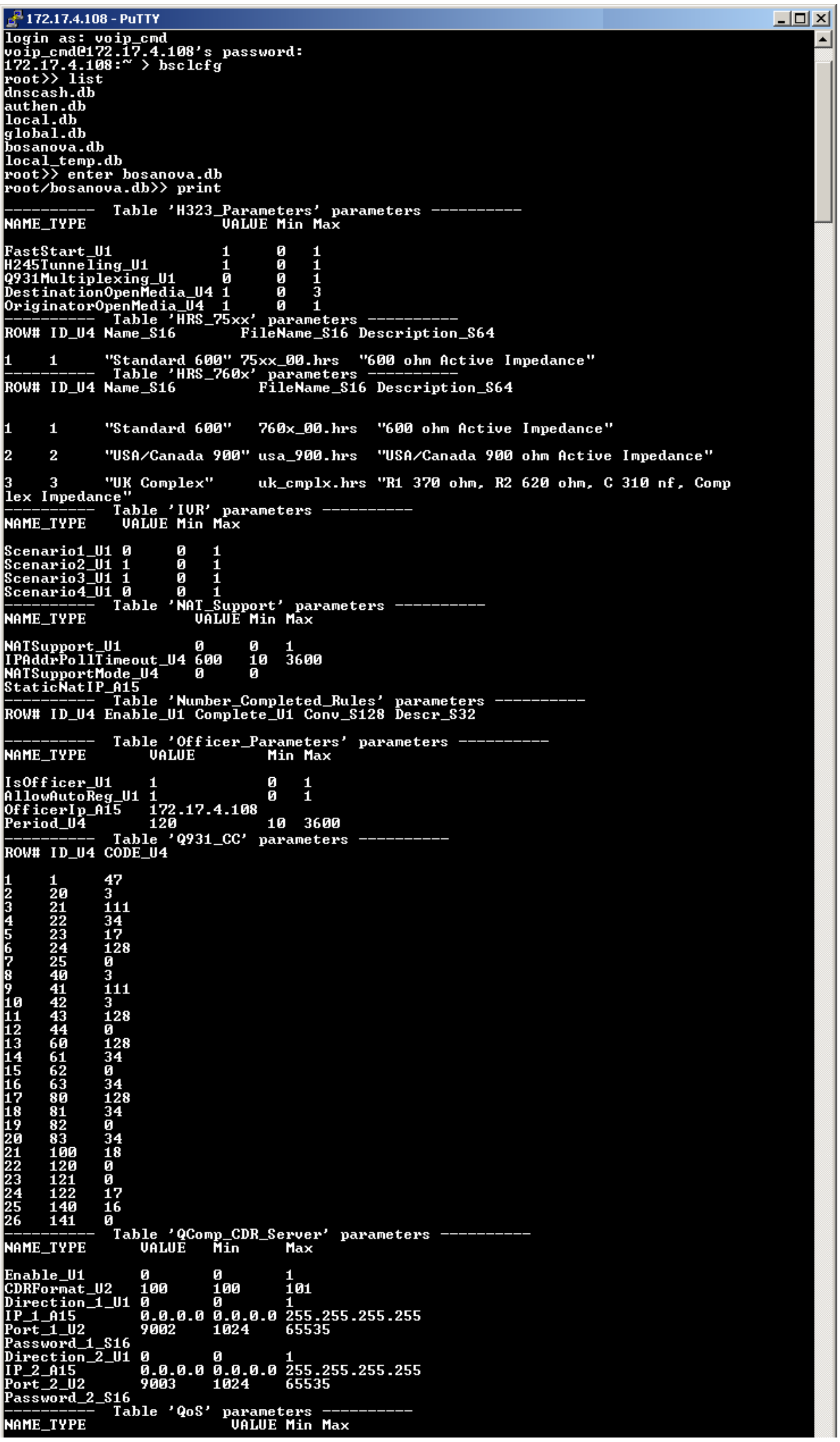
Sample CLC Procedure—How to change the Maximum Call Duration

1. At the login prompt, type **`voip_cmd`** and press **Enter**.
2. Enter the password. The default password is 1234. Press **Enter**.
3. At the IP address prompt, type **`/opt/BOSutils/bsclcfg`** and press **Enter**.
4. At the **`root>>`** prompt, type **`list`** and press **Enter**. A list of databases is displayed.
5. Type **`enter bosanova.db`** and press **Enter**. The root/bosanova.db>> branch is displayed.
6. Type **`print`** and press **Enter**. Tables, similar to the tables in the following illustration, are displayed.
7. Type **`exit`** and press **Enter**. The previous branch—that is, the root/bosanova.db>> branch—is displayed again.
8. Type **`list`** and press **Enter**. This time, a list of all the tables in the database are displayed.



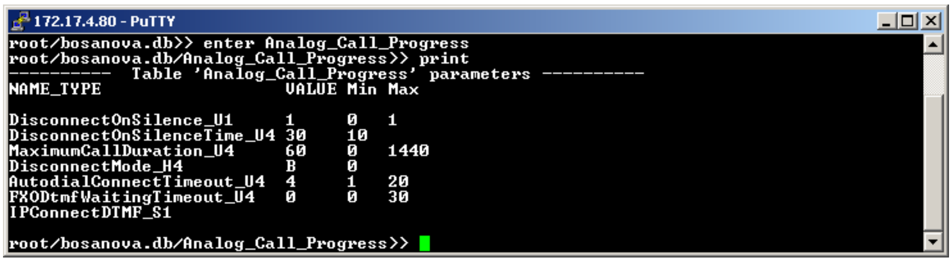
```
root/bosanova.db/H323_Parameters>> exit
root/bosanova.db>> list
    Analog_Call_Progress
    Analog_Data
    Answer_Supervision
    BOS_Signals
    BOSaNOVA_Customer_AddOn
    CP_Signals
    CP_Signals_Mode
    CP_Signals_Sets
    Codecs
    Dialing_Parameters
    FORMAT_CP_Signals
    FORMAT_Codecs
    Fax_Config
    Global_Encryption
    Gtw_Info
    Gtw_NetInfo
    H323GK_Prefixes_List
    H323GK_Service_Prefixes
    H323_Gatekeeper
    H323_Parameters
    HRS_75xx
    HRS_760x
    IVR
    NAT_Support
    Number_Completed_Rules
    Officer_Parameters
    Q931_CC
    QComp_CDR_Server
    QoS
    QoS_ICMP_CHECK
    SIP_Parameters
    Statistic_Servers
    TOS
    Update_Table
    Voice_And_Telephony_D
    Voice_And_Telephony_s
    X86_Adapter_Data_1
    X86_Adapter_Data_2
root/bosanova.db>>
```

9. Type **`enter Analog_Call_Progress`** and press **Enter**. The CLC enters the Analog_Call_Progress table of the database.



```
login as: voip_cmd
voip_cmd@172.17.4.108's password:
172.17.4.108:~ > bsclcfg
root>> list
dnscash.db
authen.db
local.db
global.db
bosanova.db
local_temp.db
root>> enter bosanova.db
root/bosanova.db>> print
----------  Table 'H323_Parameters' parameters ----------
NAME_TYPE               VALUE Min Max

FastStart_U1            1     0   1
H245Tunneling_U1        1     0   1
Q931Multiplexing_U1     0     0   1
DestinationOpenMedia_U4 1     0   3
OriginatorOpenMedia_U4  1     0   1
----------  Table 'HRS_75xx' parameters ----------
ROW# ID_U4 Name_S16       FileName_S16 Description_S64

1    1     "Standard 600" 75xx_00.hrs  "600 ohm Active Impedance"
----------  Table 'HRS_760x' parameters ----------
ROW# ID_U4 Name_S16         FileName_S16 Description_S64


1    1     "Standard 600"   760x_00.hrs  "600 ohm Active Impedance"

2    2     "USA/Canada 900" usa_900.hrs  "USA/Canada 900 ohm Active Impedance"

3    3     "UK Complex"     uk_cmplx.hrs "R1 370 ohm, R2 620 ohm, C 310 nf, Comp
lex Impedance"
----------  Table 'IVR' parameters ----------
NAME_TYPE    VALUE Min Max

Scenario1_U1 0     0   1
Scenario2_U1 1     0   1
Scenario3_U1 1     0   1
Scenario4_U1 0     0   1
----------  Table 'NAT_Support' parameters ----------
NAME_TYPE            VALUE Min Max

NATSupport_U1        0     0   1
IPAddrPollTimeout_U4 600   10  3600
NATSupportMode_U4    0     0
StaticNatIP_A15
----------  Table 'Number_Completed_Rules' parameters ----------
ROW# ID_U4 Enable_U1 Complete_U1 Conv_S128 Descr_S32

----------  Table 'Officer_Parameters' parameters ----------
NAME_TYPE       VALUE        Min Max

IsOfficer_U1    1            0   1
AllowAutoReg_U1 1            0   1
OfficerIp_A15   172.17.4.108
Period_U4       120          10  3600
----------  Table 'Q931_CC' parameters ----------
ROW# ID_U4 CODE_U4

1    1     47
2    20    3
3    21    111
4    22    34
5    23    17
6    24    128
7    25    0
8    40    3
9    41    111
10   42    3
11   43    128
12   44    0
13   60    128
14   61    34
15   62    0
16   63    34
17   80    128
18   81    34
19   82    0
20   83    34
21   100   18
22   120   0
23   121   0
24   122   17
25   140   16
26   141   0
----------  Table 'QComp_CDR_Server' parameters ----------
NAME_TYPE      VALUE   Min     Max

Enable_U1      0       0       1
CDRFormat_U2   100     100     101
Direction_1_U1 0       0       1
IP_1_A15       0.0.0.0 0.0.0.0 255.255.255.255
Port_1_U2      9002    1024    65535
Password_1_S16
Direction_2_U1 0       0       1
IP_2_A15       0.0.0.0 0.0.0.0 255.255.255.255
Port_2_U2      9003    1024    65535
Password_2_S16
----------  Table 'QoS' parameters ----------
NAME_TYPE                VALUE Min Max
```

10. Type **`print`** and press **Enter**. The Analog_Call_Progress table is displayed.

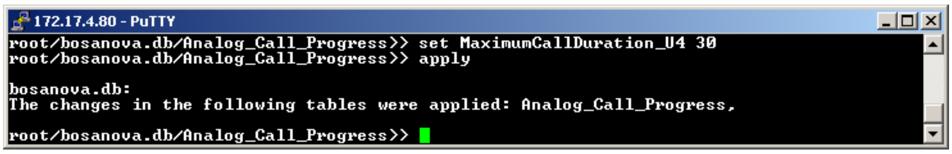


```
root/bosanova.db>> enter Analog_Call_Progress
root/bosanova.db/Analog_Call_Progress>> print
----------  Table 'Analog_Call_Progress' parameters ----------
NAME_TYPE                  VALUE Min Max

DisconnectOnSilence_U1     1     0   1
DisconnectOnSilenceTime_U4 30    10
MaximumCallDuration_U4     60    0   1440
DisconnectMode_H4          B     0
AutodialConnectTimeout_U4  4     1   20
FXODtmfWaitingTimeout_U4   0     0   30
IPConnectDTMF_S1

root/bosanova.db/Analog_Call_Progress>>
```

11. Type **`set MaximumCallDuration_U4 30`** and press **Enter**. The parameter is changed.

12. Type **`apply`** and press **Enter**.

13. Confirm or delay the restart.

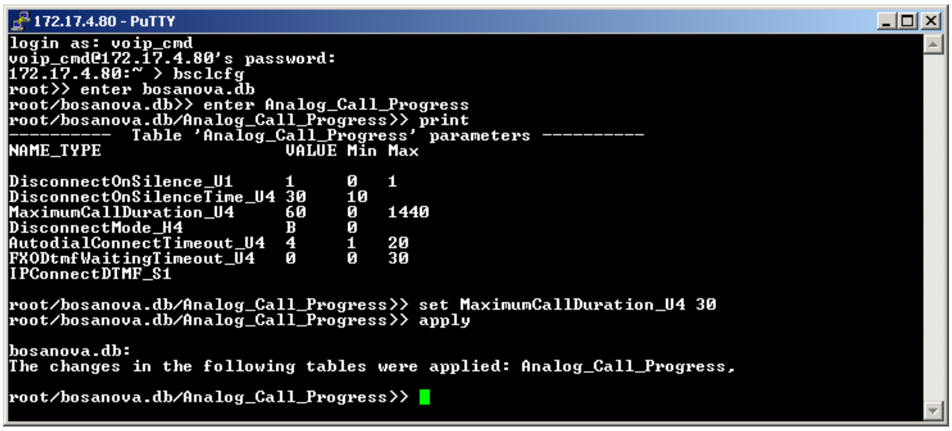


```
root/bosanova.db/Analog_Call_Progress>> set MaximumCallDuration_U4 30
root/bosanova.db/Analog_Call_Progress>> apply

bosanova.db:
The changes in the following tables were applied: Analog_Call_Progress,

root/bosanova.db/Analog_Call_Progress>>
```

If you delay the restart, you must enter Apply again.

Summary of Command Line Configurator Tutorial

Once familiar with the Command Line Configurator, the entire 11-step procedure described on the previous three pages will look like this:



172.17.4.80 - PuTTY

```
login as: voip_cmd
voip_cmd@172.17.4.80's password:
172.17.4.80:~ > bsclcfg
root>> enter bosanova.db
root/bosanova.db>> enter Analog_Call_Progress
root/bosanova.db/Analog_Call_Progress>> print
----------  Table 'Analog_Call_Progress' parameters ----------
NAME_TYPE                  VALUE Min Max

DisconnectOnSilence_U1     1     0   1
DisconnectOnSilenceTime_U4 30    10
MaximumCallDuration_U4     60    0   1440
DisconnectMode_H4          B     0
AutodialConnectTimeout_U4  4     1   20
FXODtmfWaitingTimeout_U4   0     0   30
IPConnectDTMF_S1

root/bosanova.db/Analog_Call_Progress>> set MaximumCallDuration_U4 30
root/bosanova.db/Analog_Call_Progress>> apply

bosanova.db:
The changes in the following tables were applied: Analog_Call_Progress,

root/bosanova.db/Analog_Call_Progress>>
```

Running Scripts Using the Command Line Configurator

Use the Command Line Configurator to run a script, that is, to automatically execute a series of keystrokes that would otherwise have to be entered one at a time.

Ensure that the script is written in a text editor that supports Unix format. The Unix format uses a different "new line" command. If the script is written in a text editor such as Windows Notepad, it will not run.

1. Write the script.
2. Open the SSH client.
3. Login to the Gateway upon which the script is to be run.
4. Depending upon which SSH client is used:
   - Copy the script from the text editor and paste it into the SSH terminal.
   - Use the SSH terminal's Open > File function to run the script.

HIDDEN PARAMETERS

The following parameters can only be accessed from either the Command Line Configurator or the Maintenance Wizard.

Table 53: Hidden Parameters in the PRI_Call_Progress Table Applicable for E1, T1, and PRI Claro Gateways

Name_Type	Default Value	Min	Max
DisconnectOnSilence_U1	= 0	= 0	= 1
DisconnectOnSilenceTime_U4	= 60	= 10	=
MaximumCallDuration_U4	= 1440	= 0	=1440
Maximum length (in minutes) of the call , when exceeded Gateway disconnects it. 0 - no limit. (1440 minutes = 24 hours)			
PseudoInBlock_U1	= 0	= 0	= 1
TeleLynk compatible mode			
AudioMode_U4	= 0	= 0	= 2
0- default proceed as usual, 1-Replace Audio with Speech in both Interfaces, 2 - Add PI for all Audio calls, use data (as string) from parameter AudioProgressIndicator_S8			
AudioPI_S8	1E028183		
value for progress indicator , when used with Audio calls			

Table 54: Hidden Parameters in the Analog_Call_Progress Table Applicable for FXS, FXO, and Analog Claro Gateways, and ROBO

Name_Type	Default Value	Min	Max
MaximumCallDuration_U4	= 60	= 0	= 1440
Maximum length (in minutes) of the call. If exceeded, the Gateway disconnects the call. 0 = no limit			
DisconnectMode_H4	= B	= 0	
Bit mask corresponds to LKe_ADAPTER_TYPE Unknown =1, E1=2 , FXS=4, FXO=8, FXO uses this as a bit mask of the gateway type conversion with which should be disconnected on tone detection			
AutodialConnectTimeout_U4	= 4	= 1	=20
Use for an FXO, to define the timeout that a Gateways awaits the next ring before deciding that there will be no more rings and, therefore, disconnecting (used inAutodial only).			
FXODtmfWaitingTimeout_U4	= 0	= 0	=30
Use for FXO termination Gateway, to disconnect if no DTMFs from origination Gateway via the IP were received after Off-hook. Defined in seconds. 0 = means there is no disconnect.			
IPConnectDTMF_S1	=		
Use for FXS/FXO origination. Sends a DTMF to a line, when Connect is received from the IP. May be 0-9,*,#,A,B,C,D. When it is empty or does not exist - does nothing.			

Table 55: Hidden Parameters in the Analog_Data Table Applicable for FXS, FXO, and Analog Claro Gateways, and ROBO

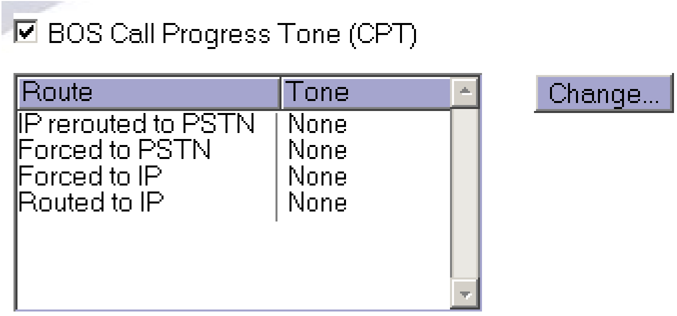
Name_Type	Value	Min	Max
RingerFrequency_U4	= 50	= 17	= 50
Use for ring generation on FXS Vintage Gateway			
RingerAmplitude_U4	= 25000	= 0	= 32635
Used for ring detection parameters on FXO Vintage Gateway.			
RingSampleRate_U4	= 1	= 1	= 5
Used for ring detection parameters on FXO Vintage Gateway.			
RingDecidePercent_U4	= 16	= 10	= 90
Used for ring detection parameters on FXO Vintage Gateway.			
SwitcherCurrentLimit_U1	= 0	= 0	= 1
Used for ring detection parameters on FXO Vintage Gateway.			
FlashTime_U4	= 150	= 150	= 900
Define Flash generation time on FXS ports of Vintage and Claro/ROBO Gateways, Rounded up to 50.			

Table 56: Hidden Parameters in the BOSaNOVA_Customer_AddOn table

Name_Type	Value	Min	Max
LoginCounter_U4	= 0	= 0	= 10
Use to define the maximum number of consequtive failed login attempts during the LoginTimeout_U4 before BOSmaster blocks the call.			
LoginTimeout_U4	= 0	= 0	= 1000
Use to define the maximum number of minutes a user can attempt to login before he runs out of time. Used together with LoginCounter_U4.			
HideClaroPorts_U1	= 0	= 0	= 1
Used for Analog Claro and ROBO. When set to 1, the Configurator will not show the matrix with all Claro ports, but will automatically define all of them as independent FXS and FXO.			

BOS Call Progress Signals Hidden Parameters

These optional tones indicate the routing of the call and are enabled from VoIP Configurator. See “BOS Tones” on page 59.



☑ BOS Call Progress Tone (CPT)

Route	Tone
IP rerouted to PSTN	None
Forced to PSTN	None
Forced to IP	None
Routed to IP	None

The following signals are available from TableID = 78 in the bosanova.db:

Table 57:

ID_U4	Name_S32	Code_S64
1 =	"Rising tone"	= "1:6,2:6,3:6,17:30,"
2 =	"Sinking tone"	= "3:6,2:6,1:6,17:30,"
3 =	"Trill tone"	= "1:10,2:10,3:10,2:10,1:10,17:30,"
4 =	"Short tone"	= "11:6,10:6,11:6,17:30,"
5 =	"Long trill tone"	= "11:10,5:10,10:10,11:10,5:10,10:10,17:30,"
ToneNumber_1:Duration_1,ToneNumber_2:Duration_2,...,ToneNumber_n :Duration_n\0		

Clearing Cause Hidden Parameters

The following clearing cause parameters are available from TableID = 75 in the bosanova.db:

ID_U4
This ID is equal to the enumerator of the Clearing Causes which are used in LKc_CONFIG::LoadQ931Cause()

CODE_U4
CODE_U4=128 means that the actual CC value must be taken either from

H323 releaseComplete message (internal events) or from PRI CC (telephony events).

Table 58: Clearing Cause Parameters

ID_U4	CODE _U4		
Common for origination and termination gateways.			
1	=47	CC_OT _ NOCAPABILITY.	There are no common H.245 or SDP capabilities.
Common for termination gateways			
20	=3	CC_T _NOTRESOLVED.	NP resolving failed on termination gateway.
21	=111	CC_T _NOTAUTHORIZED.	Authorization failed on termination gateway.
22	=34	CC_T _NOCHANNELS.	No channels available on termination gateway.
23	=17	CC_T_BUSY.	Termination FXS-to-phone line is busy.
24	=128	CC_T_IP _NOCONNECT.	IP (H.323 or SIP) disconnect was received before CONNECT was received from the telephony interface.
25	=0	CC_T_IP _AFTER_CONNECT.	IP (H.323 or SIP) disconnect was received after CONNECT was received from the telephony interface.
Common for origination gateways			
40	=3	CC_O _NOTRESOLVED.	Called number was not resolved.
41	=111	CC_O _NOTAUTHORIZED.	The call is not authorised on the origination gateway.
42	=3	CC_O _UNREACHABLE.	The IP call was not established due to IP conditions.
43	=128	CC_O _IP_NOCONNECT	The IP call was disconnected before it was connected.

Table 58: Clearing Cause Parameters

ID_U4	CODE _U4		
44	=0	CC_O_IP _AFTER_CONNECT.	The IP call was disconnected after it was connected.
Termination PRI, internal events			
60	=128	CC_2TPRI _L128_NOCONNECT	Local PRI disconnect with CC <128 before it was connected.
61	=34	CC_2TPRI_G128 _NOCONNECT.	Local PRI disconnect with CC >=128 before it was connected.
62	=0	CC_2TPRI_L128 _AFTER_CONNECT.	Local PRI disconnect with CC <128 after it was connected.
63	=34	CC_2TPRI_G128 _AFTER_CONNECT.	Local PRI disconnect with CC >=128 after it was connected.
Termination PRI, telephony events			
80	=128	CC_2OPRI_L128 _NOCONNECT.	Local PRI disconnect with CC <128 before it was connected.
81	=34	CC_2OPRI_G128 _NOCONNECT.	Local PRI disconnect with CC >= 128 before it was connected.
82	=0	CC_2OPRI_L128 _AFTER_CONNECT.	Local PRI disconnect with CC <128 after it was connected.
83	=34	CC_2OPRI_G128 _AFTER_CONNECT.	Local PRI disconnect with CC >= 128 after it was connected.
Termination analog, internal events			
100	=18	CC_1TAN _NO_ANSWER.	a)FXS: the call was disconnected due to timeout. b)FXO didn't detect that the call was established (not implemented yet)
Termination analog, telephony events			
120	=0	CC_2TAN _AFTER_FXS_CONN.	On-hook detected after FXS was connected.

Table 58: Clearing Cause Parameters

ID_U4	CODE _U4		
121	=0	CC_2TAN _AFTER_FXO_CONN .	FXO disconnect signal was detected more than 20 seconds after off-hook. (In current version the timeout is not considered.)
122	=17	CC_2TAN _EARLY_FXO_DISC.	FXO line was off-hooked but disconnection signal was detected in 20 seconds (not implemented yet)
Origination analog, telephony events			
140	=16	CC_2OAN_IP _NOCONNECT.	Analog interface caused disconnect before IP was connected.
141	=0	CC_2OAN_IP _AFTER_CONNECT.	Analog interface caused disconnect after IP was connected.

IP Telephony...
Clear and Simple

SECTION 19:
MAINTENANCE WIZARD'S PRIMARY APPLICATIONS

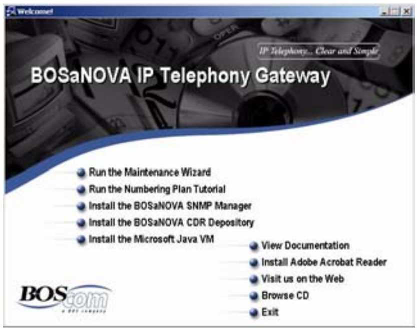
This section contains the most common procedures performed with the BOSâNOVA IP Telephony Gateway Maintenance Wizard, including:

- Running the Maintenance Wizard, see p. 294
- Reviewing product information, see p. 295
- Finding Gateways and reviewing their status, see p. 296
- Updating the Gateway software, see p. 301
- Checking an IP connection, see p. 310
- Online monitoring, see p. 302
- Getting and saving trace buffer files, see p. 303
- Setting diagnostic levels, see p. 307
- Opening the Terminal Server, see p. 308
- Connecting to a Gateway with a known IP address, see p. 299
- Configuring Network Time Protocol, see p. 312

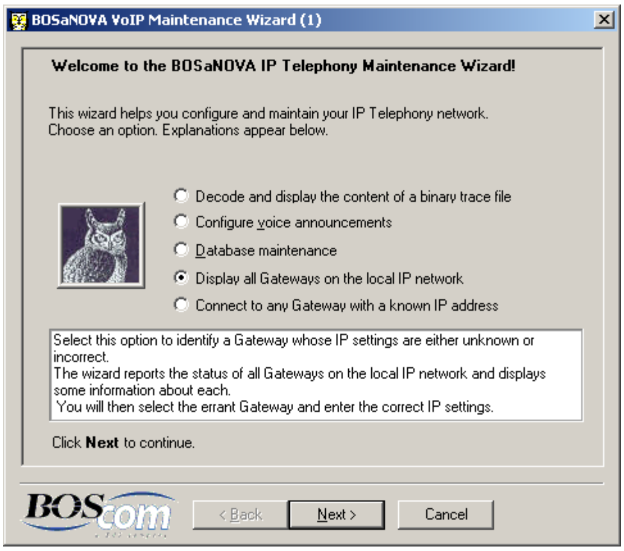
RUNNING THE MAINTENANCE WIZARD

To access the Maintenance Wizard:

1. Insert the BOSâNOVA IP Telephony CD-ROM into the CD-ROM drive. The CD-ROM Welcome screen is displayed.


Welcome!
IP Telephony... Clear and Simple
BOSaNOVA IP Telephony Gateway
Run the Maintenance Wizard
Run the Numbering Plan Tutorial
Install the BOSaNOVA SNMP Manager
Install the BOSaNOVA CDR Depository
Install the Microsoft Java VM
View Documentation
Install Adobe Acrobat Reader
Visit us on the Web
Browse CD
Exit
BOScom

2. Select **Run the Maintenance Wizard**. The Maintenance Wizard Welcome screen appears.



BOSaNOVA VoIP Maintenance Wizard (1)

Welcome to the BOSaNOVA IP Telephony Maintenance Wizard!

This wizard helps you configure and maintain your IP Telephony network.
Choose an option. Explanations appear below.

○ Decode and display the content of a binary trace file
○ Configure voice announcements
○ Database maintenance
● Display all Gateways on the local IP network
○ Connect to any Gateway with a known IP address

Select this option to identify a Gateway whose IP settings are either unknown or incorrect.
The wizard reports the status of all Gateways on the local IP network and displays some information about each.
You will then select the errant Gateway and enter the correct IP settings.

Click **Next** to continue.

REVIEWING PRODUCT INFORMATION

The BOScom Technical Support department or sales department might need a Gateway's product information.

To review the product information for a Gateway:

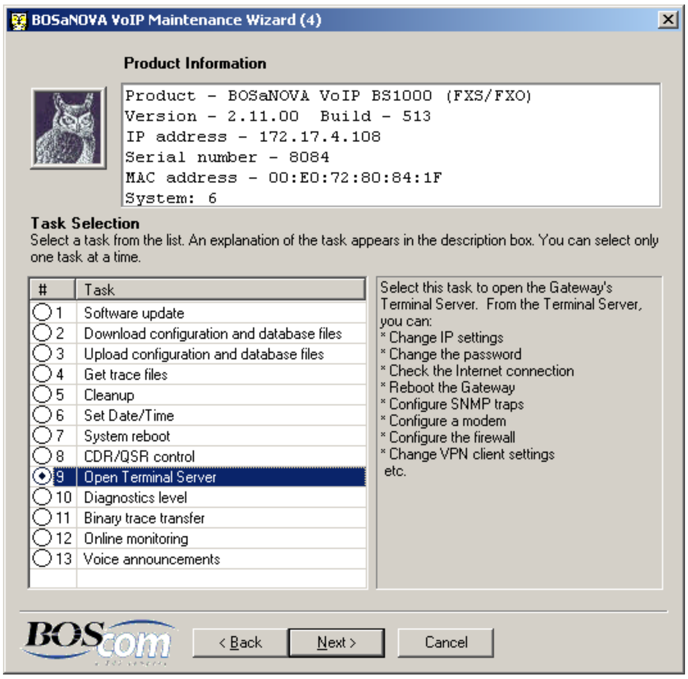
1. Run the Maintenance Wizard. (If you need help, see "Running the Maintenance Wizard" on page 294.)

2. Connect to the required Gateway.

   - If you need help and know the Gateway's IP address, see "Connecting to a Gateway With a Known Address" on page 299.

   - If you need help and do not know the Gateway's IP address, see "Finding Gateways and Reviewing Their Status" on page 296.

The product information is located at the top of Maintenance Wizard screen number (4).



Product Information

```
Product - BOSaNOVA VoIP BS1000 (FXS/FXO)
Version - 2.11.00  Build - 513
IP address - 172.17.4.108
Serial number - 8084
MAC address - 00:E0:72:80:84:1F
System: 6
```

Task Selection

Select a task from the list. An explanation of the task appears in the description box. You can select only one task at a time.

#	Task
○ 1	Software update
○ 2	Download configuration and database files
○ 3	Upload configuration and database files
○ 4	Get trace files
○ 5	Cleanup
○ 6	Set Date/Time
○ 7	System reboot
○ 8	CDR/QSR control
● 9	Open Terminal Server
○ 10	Diagnostics level
○ 11	Binary trace transfer
○ 12	Online monitoring
○ 13	Voice announcements

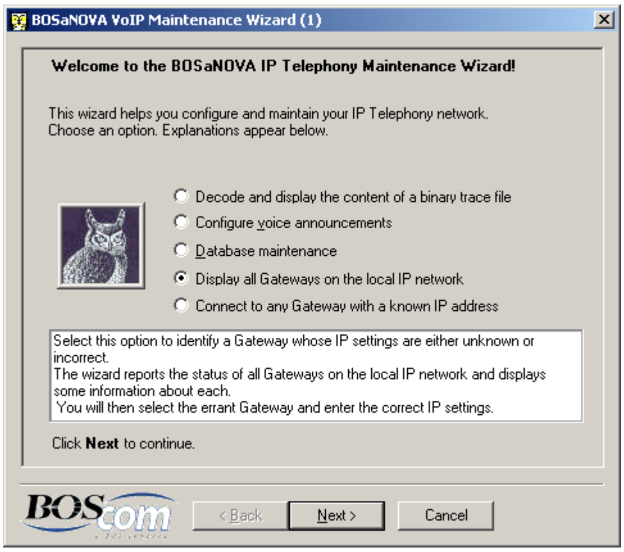
Select this task to open the Gateway's Terminal Server. From the Terminal Server, you can:
* Change IP settings
* Change the password
* Check the Internet connection
* Reboot the Gateway
* Configure SNMP traps
* Configure a modem
* Configure the firewall
* Change VPN client settings
etc.

To copy the product information to the clipboard, right-click within the information field. From the popup menu, select ***Copy all****.*

FINDING GATEWAYS AND REVIEWING THEIR STATUS

1. Run the Maintenance Wizard. (If you need help, see “Running the Maintenance Wizard” on page 294.)

2. Select **Display the status of all Gateways on this IP Telephony network**.



Welcome to the BOSaNOVA IP Telephony Maintenance Wizard!

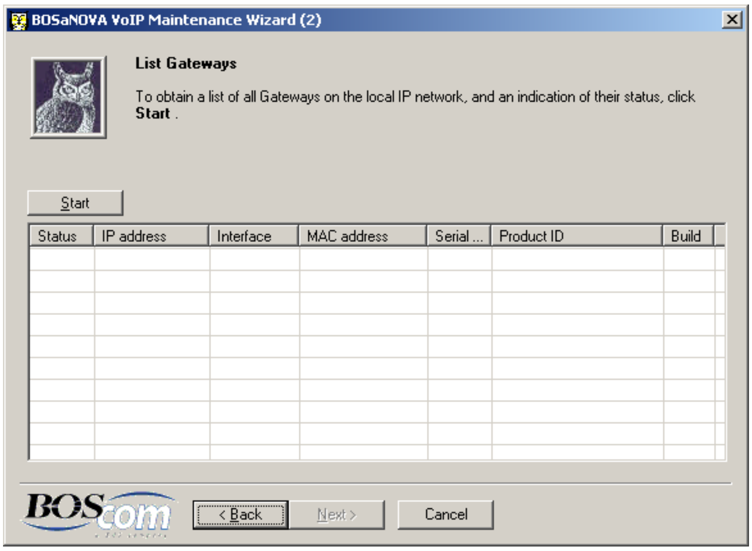
This wizard helps you configure and maintain your IP Telephony network.
Choose an option. Explanations appear below.

○ Decode and display the content of a binary trace file
○ Configure voice announcements
○ Database maintenance
● Display all Gateways on the local IP network
○ Connect to any Gateway with a known IP address

Select this option to identify a Gateway whose IP settings are either unknown or incorrect.
The wizard reports the status of all Gateways on the local IP network and displays some information about each.
You will then select the errant Gateway and enter the correct IP settings.

Click **Next** to continue.

3. Click **Next**. The List Gateways screen is displayed.

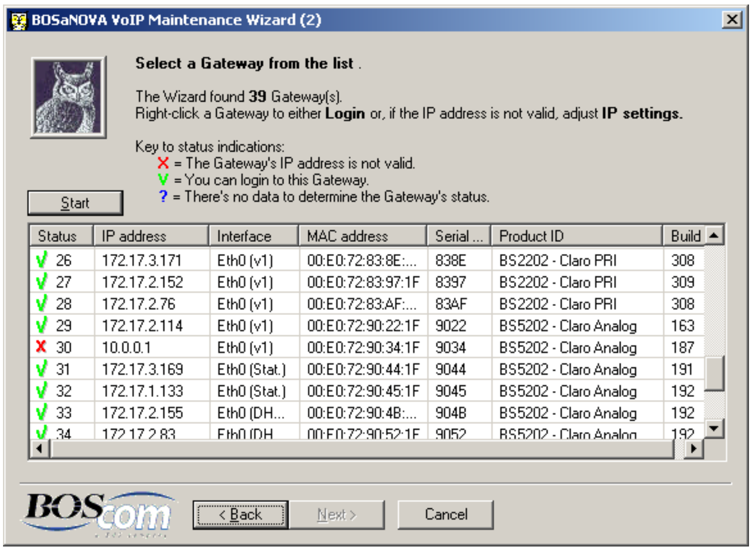


List Gateways

To obtain a list of all Gateways on the local IP network, and an indication of their status, click **Start** .

Status	IP address	Interface	MAC address	Serial ...	Product ID	Build

4. Click **Start**. The Maintenance Wizard begins listing all Gateways on the local IP network. When all Gateways are listed, the Maintenance Wizards ends the listing process automatically. Alternately, click **Stop** to discontinue the listing.



Select a Gateway from the list .

The Wizard found **39** Gateway(s).
Right-click a Gateway to either **Login** or, if the IP address is not valid, adjust **IP settings**.

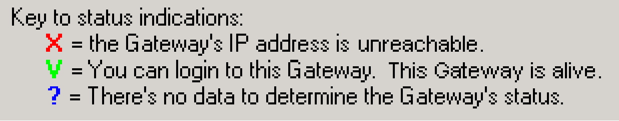
Key to status indications:
✗ = The Gateway's IP address is not valid.
✓ = You can login to this Gateway.
? = There's no data to determine the Gateway's status.

Status	IP address	Interface	MAC address	Serial ...	Product ID	Build
✓ 26	172.17.3.171	Eth0 (v1)	00:E0:72:83:8E:...	838E	BS2202 - Claro PRI	308
✓ 27	172.17.2.152	Eth0 (v1)	00:E0:72:83:97:1F	8397	BS2202 - Claro PRI	309
✓ 28	172.17.2.76	Eth0 (v1)	00:E0:72:83:AF:...	83AF	BS2202 - Claro PRI	308
✓ 29	172.17.2.114	Eth0 (v1)	00:E0:72:90:22:1F	9022	BS5202 - Claro Analog	163
✗ 30	10.0.0.1	Eth0 (v1)	00:E0:72:90:34:1F	9034	BS5202 - Claro Analog	187
✓ 31	172.17.3.169	Eth0 (Stat.)	00:E0:72:90:44:1F	9044	BS5202 - Claro Analog	191
✓ 32	172.17.1.133	Eth0 (Stat.)	00:E0:72:90:45:1F	9045	BS5202 - Claro Analog	192
✓ 33	172.17.2.155	Eth0 (DH...	00:E0:72:90:4B:...	904B	BS5202 - Claro Analog	192
✓ 34	172.17.2.83	Eth0 (DH	00:E0:72:90:52:1F	9052	BS5202 - Claro Analog	192

Stopping and then starting restarts the listing process.

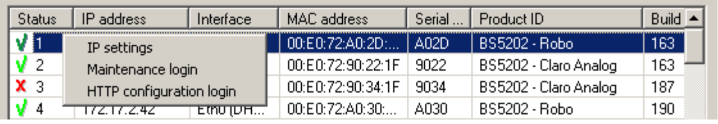
5. Sort the Gateways by clicking a heading in the title bar of the table.

6. Review a Gateway's status and limited product information. Status icons are listed in the first column.



Key to status indications:
✗ = the Gateway's IP address is unreachable.
✓ = You can login to this Gateway. This Gateway is alive.
? = There's no data to determine the Gateway's status.

7. Right-click a Gateway. The following popup menu is displayed:



Status	IP address	Interface	MAC address	Serial ...	Product ID	Build
✓ 1			00:E0:72:A0:2D:...	A02D	BS5202 - Robo	163
✓ 2			00:E0:72:90:22:1F	9022	BS5202 - Claro Analog	163
✗ 3			00:E0:72:90:34:1F	9034	BS5202 - Claro Analog	187
✓ 4	172.17.2.42	Eth0 (DH...	00:E0:72:A0:30:...	A030	BS5202 - Robo	190

8. Select one of the three options:

   - **IP settings**:
     A dialog box displaying the IP settings opens.

To change the IP settings of a functioning Gateway, use the Terminal Server.

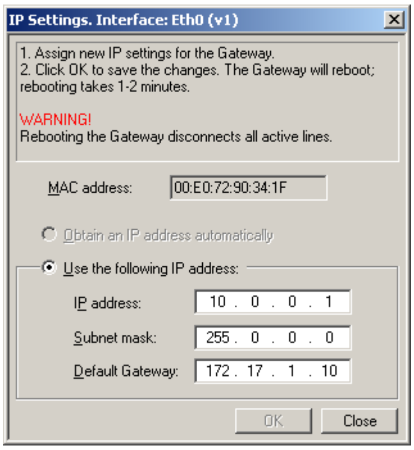
   - **Maintenance login**:
     The login screen of the Maintenance Wizard opens.
   - **HTTP configuration login**:
     A browser window opens and the login screen of the Gateway Configurator is displayed.

Gateway with an Undefined IP Address

The status symbol ✗ indicates that the Gateway's IP address has not been assigned.

To assign the IP address from the Maintenance Wizard:

1. Right-click the Gateway with the ✗ status symbol.
2. Select **IP settings**. The IP Settings dialog box appears.



IP Settings. Interface: Eth0 (v1)

1. Assign new IP settings for the Gateway.
2. Click OK to save the changes. The Gateway will reboot; rebooting takes 1-2 minutes.

WARNING!
Rebooting the Gateway disconnects all active lines.

MAC address: 00:E0:72:90:34:1F

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 0 . 0 . 1

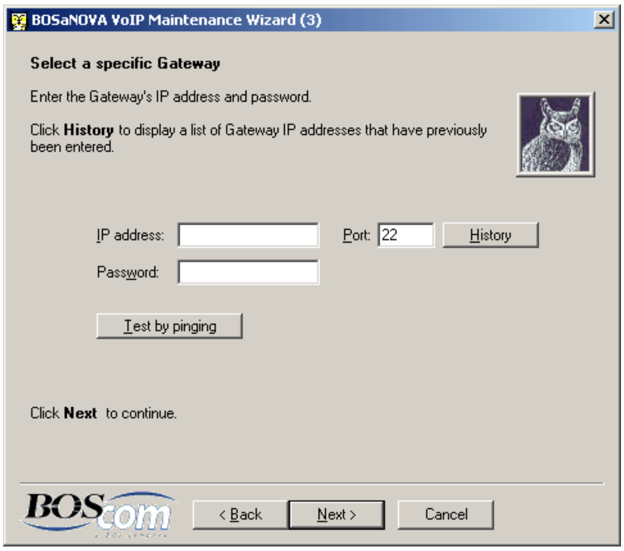
Subnet mask: 255 . 0 . 0 . 0

Default Gateway: 172 . 17 . 1 . 10

3. Enter the IP settings.
4. Click **Close**.

CONNECTING TO A GATEWAY WITH A KNOWN ADDRESS

1. Run the Maintenance Wizard. (If you need help, see "Running the Maintenance Wizard" on page 294.)
2. Select **Connect to any Gateway with a known IP address.**
3. Click **Next**. The Select a specific Gateway screen is displayed.



BOSaNOVA VoIP Maintenance Wizard (3)

Select a specific Gateway

Enter the Gateway's IP address and password.

Click **History** to display a list of Gateway IP addresses that have previously been entered.

IP address:

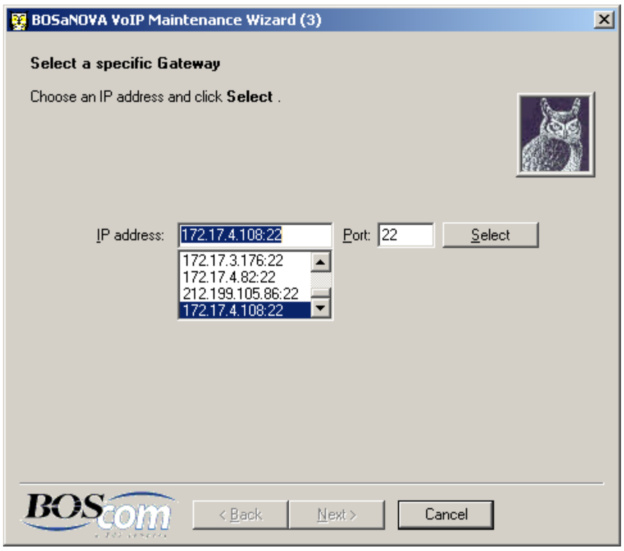
Port: 22

Password:

Click **Next** to continue.

4. To select a specific Gateway, either:
   - Enter the IP address and password of the Gateway.
   - If you have previously connected to the Gateway:

     a. Click **History**. The following screen appears:



BOSaNOVA VoIP Maintenance Wizard (3)

Select a specific Gateway

Choose an IP address and click **Select** .

IP address: 172.17.4.108:22

Port: 22

172.17.3.176:22
172.17.4.82:22
212.199.105.86:22
172.17.4.108:22

     b. Select a Gateway from the list.

c. Click **Select**. The Select a specific Gateway screen reappears.

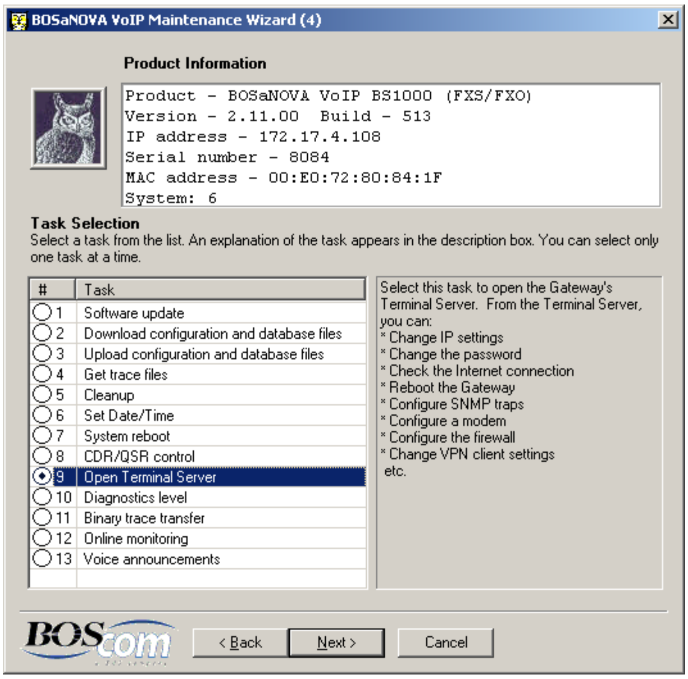
d. Enter the Gateway's password. The default password is **1234**.

5. To test if the Gateway is functioning, click **Test by pinging**. If the Gateway is functioning, the message =Alive= appears in the text box beside the button.

Testing continues until either ***Stop pinging*** *or* ***Next*** *is clicked.*

6. Enter the Port number for the Gateway.

7. Click **Next**. The **Product Information** and **Task Selection** screen, which is screen number (4), appears. The Gateway is now open and accessible. If there is a problem connecting to the Gateway check that you have the correct IP number, port number, and password.



Product Information

```
Product - BOSaNOVA VoIP BS1000 (FXS/FXO)
Version - 2.11.00  Build - 513
IP address - 172.17.4.108
Serial number - 8084
MAC address - 00:E0:72:80:84:1F
System: 6
```

Task Selection

Select a task from the list. An explanation of the task appears in the description box. You can select only one task at a time.

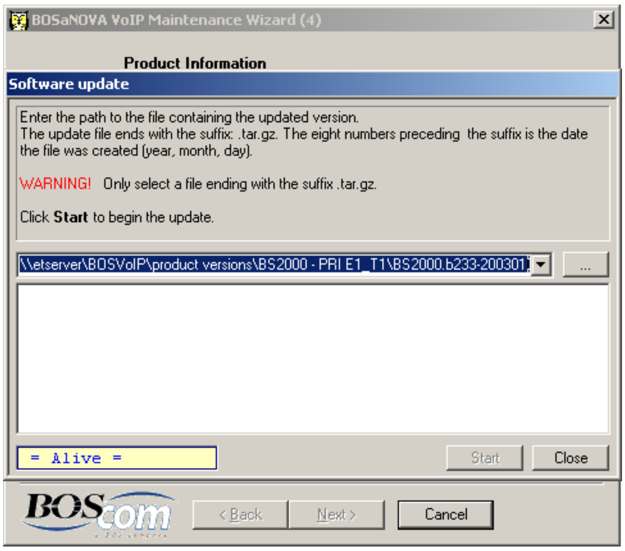
#	Task
○ 1	Software update
○ 2	Download configuration and database files
○ 3	Upload configuration and database files
○ 4	Get trace files
○ 5	Cleanup
○ 6	Set Date/Time
○ 7	System reboot
○ 8	CDR/QSR control
● 9	Open Terminal Server
○ 10	Diagnostics level
○ 11	Binary trace transfer
○ 12	Online monitoring
○ 13	Voice announcements

Select this task to open the Gateway's Terminal Server. From the Terminal Server, you can:
* Change IP settings
* Change the password
* Check the Internet connection
* Reboot the Gateway
* Configure SNMP traps
* Configure a modem
* Configure the firewall
* Change VPN client settings
etc.

8. Choose a task and click **Next**.

UPDATING SOFTWARE

1. Run the Maintenance Wizard. (If you need help, see “Running the Maintenance Wizard” on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway’s IP address, see “Connecting to a Gateway With a Known Address” on page 299.
   - If you need help and do not know the Gateway’s IP address, see “Finding Gateways and Reviewing Their Status” on page 296.
3. Select **Software update**.
4. Click **Next**. The **Software update** screen appears.



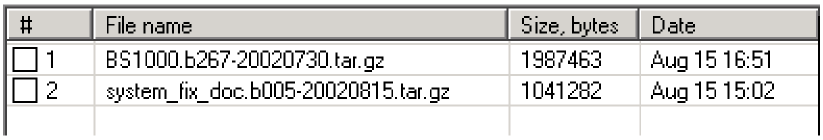
Enter the path to the file containing the updated version.
The update file ends with the suffix: .tar.gz. The eight numbers preceding the suffix is the date the file was created (year, month, day).

WARNING! Only select a file ending with the suffix .tar.gz.

Click **Start** to begin the update.

\\etserver\BOSVoIP\product versions\BS2000 - PRI E1_T1\BS2000.b233-200301

5. Enter the path to the file containing the updated version. The update files and system fixes end with the suffix.tar.gz.



#	File name	Size, bytes	Date
□ 1	BS1000.b267-20020730.tar.gz	1987463	Aug 15 16:51
□ 2	system_fix_doc.b005-20020815.tar.gz	1041282	Aug 15 15:02

Use the browse button the right of the drop down list to browse through the folders and add all of the .tar.gz files to the drop down list. Files added to the drop down list will be saved there.

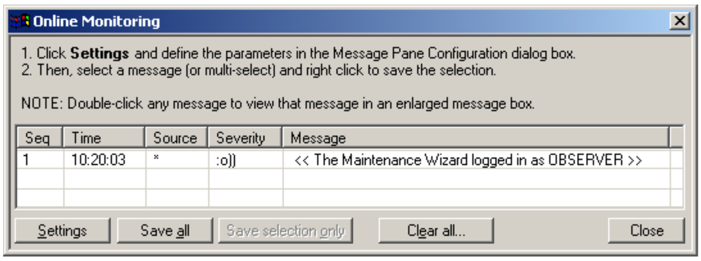
Only select a file ending with the suffix.tar.gz

6. Click **Start** to begin the update. After updating, the Gateway will reboot. The Configurator and all lines will be disconnected. Startup takes 1 to 2 minutes.

ONLINE MONITORING

To monitor a Gateway:

1. Run the Maintenance Wizard. (If you need help, see “Running the Maintenance Wizard” on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway’s IP address, see “Connecting to a Gateway With a Known Address” on page 299.
   - If you need help and do not know the Gateway’s IP address, see “Finding Gateways and Reviewing Their Status” on page 296.
3. Select **Online Monitoring** and click **Next**. The Online Monitoring screen is displayed.

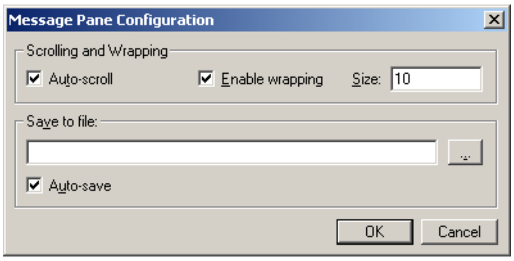


1. Click **Settings** and define the parameters in the Message Pane Configuration dialog box.
2. Then, select a message (or multi-select) and right click to save the selection.

NOTE: Double-click any message to view that message in an enlarged message box.

Seq	Time	Source	Severity	Message
1	10:20:03	*	:o))	<< The Maintenance Wizard logged in as OBSERVER >>

4. Click **Settings**. The Message Pane Configuration dialog box is displayed.



☑ Auto-scroll ☑ Enable wrapping Size: 10

☑ Auto-save

5. Define the parameters in the Message Pane Configuration dialog box and click **OK**.

*Double-click any message to view that message in an enlarged message box. Click the **Esc** key to close the enlarged message box.*

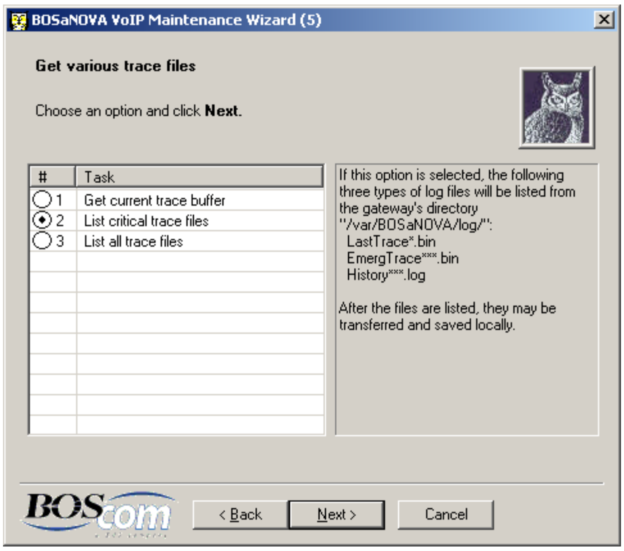
GETTING THE TRACE FILES AND SAVING THEM LOCALLY

This task saves the trace files to a PC file system not on the Gateway. At times, technical support will ask for either:

- the current trace buffer file, or
- the trace buffer file after a "traced event" occurred.

Either option may include decoding and showing of EventMarker messages.

1. Run the Maintenance Wizard. (If you need help, see "Running the Maintenance Wizard" on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway's IP address, see "Connecting to a Gateway With a Known Address" on page 299.
   - If you need help and do not know the Gateway's IP address, see "Finding Gateways and Reviewing Their Status" on page 296.
3. Select **Get trace files**. The Get various trace files screen is displayed.



BOSaNOVA VoIP Maintenance Wizard (5)

Get various trace files

Choose an option and click **Next**.

#	Task
○ 1	Get current trace buffer
● 2	List critical trace files
○ 3	List all trace files

If this option is selected, the following three types of log files will be listed from the gateway's directory "/var/BOSaNOVA/log/":
LastTrace*.bin
EmergTrace***.bin
History***.log

After the files are listed, they may be transferred and saved locally.

4. Choose one of the three options available on Maintenance Wizard Get various trace files screen(5).
   - **Get current trace buffer**
     The Gateways trace buffer is flushed to the Gateway's file "/var/BOSaNOVA/log/LastTrace.bin". This file is then transferred off of the Gateway and saved locally. It then may be decoded and displayed.

*After choosing option #1, click **Next**. Documentation continues with "Getting Current Trace Buffer" on page 305.*

- **List critical trace files**
  The following three files will be listed and can then be copied to a file off of the Gateway and saved locally. The files are:
  - /var/BOSaNOVA/log/LastTrace.bin
  - /var/BOSaNOVA/log/EmergTrace***.bin
  - /var/BOSaNOVA/log/History***.log.

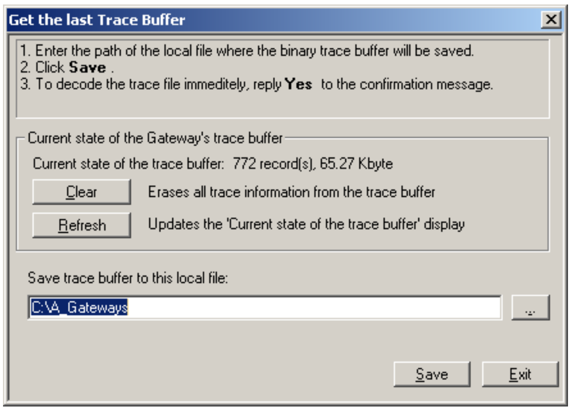
*After choosing option #2, click **Next**. Documentation continues with "Listing Critical Trace Files" on page 306.*

- **List all trace files**
  Select this option to obtain lists of different types of log files, update files, CDR and QSR files. After these files are listed they may be transferred and saved locally.

*After choosing option #3, click **Next**. Documentation continues in the next chapter.*

GETTING CURRENT TRACE BUFFER

1. Complete steps 1–4 in the section entitled "Getting the Trace Files and Saving them Locally" on page 303.
2. From the Maintenance Wizard Get various trace files screen(5), select **Get current trace buffer** and click **Next**. The Get the last Trace Buffer screen is displayed.



Get the last Trace Buffer

1. Enter the path of the local file where the binary trace buffer will be saved.
2. Click **Save** .
3. To decode the trace file immeditely, reply **Yes** to the confirmation message.

Current state of the Gateway's trace buffer

Current state of the trace buffer: 772 record(s), 65.27 Kbyte

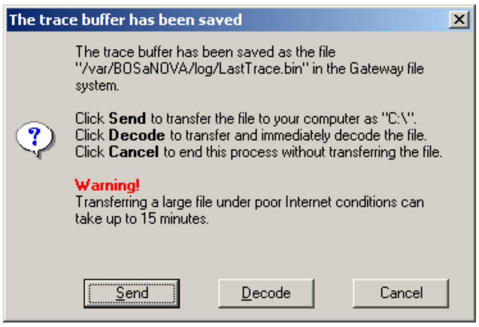
Clear — Erases all trace information from the trace buffer

Refresh — Updates the 'Current state of the trace buffer' display

Save trace buffer to this local file:

C:\A_Gateways

3. Enter the path to the location where the trace files are to be saved.
4. Click **Save** to flush the trace buffer to the LastTrace.bin file on the Gateway. The following information screen is displayed:



The trace buffer has been saved

The trace buffer has been saved as the file "/var/BOSaNOVA/log/LastTrace.bin" in the Gateway file system.

Click **Send** to transfer the file to your computer as "C:\".
Click **Decode** to transfer and immediately decode the file.
Click **Cancel** to end this process without transferring the file.

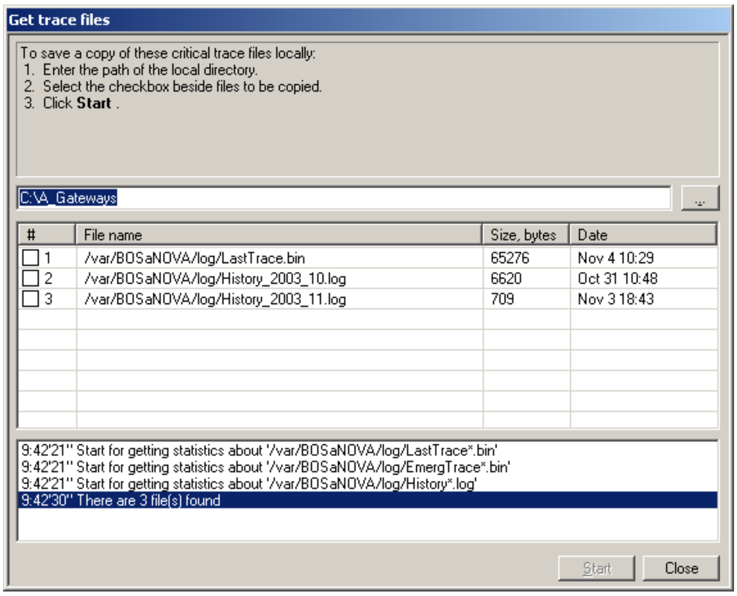
Warning!
Transferring a large file under poor Internet conditions can take up to 15 minutes.

5. Select one of the options:
   - Click **Send** to transfer the saved file to a PC.
   - Click **Decode** to transfer and decode this file immediately. The **Decoding the Binary Trace File** screen appears. Click **Close**.
6. The **Get the last Trace Buffer** screen reappears. Click **Exit**.

LISTING CRITICAL TRACE FILES

This task will list Emergency Trace files, History logs, and Last Trace files.

1. Complete steps 1–4 in the section entitled “Getting the Trace Files and Saving them Locally” on page 303.
2. From the Maintenance Wizard Get various trace files screen(5), select **List critical trace files** and click **Next**. The Get trace files screen is displayed.
3. Enter the path to the location where the trace files are to be saved.



Get trace files

To save a copy of these critical trace files locally:
1. Enter the path of the local directory.
2. Select the checkbox beside files to be copied.
3. Click **Start** .

C:\A_Gateways

#	File name	Size, bytes	Date
□ 1	/var/BOSaNOVA/log/LastTrace.bin	65276	Nov 4 10:29
□ 2	/var/BOSaNOVA/log/History_2003_10.log	6620	Oct 31 10:48
□ 3	/var/BOSaNOVA/log/History_2003_11.log	709	Nov 3 18:43

```
9:42'21'' Start for getting statistics about '/var/BOSaNOVA/log/LastTrace*.bin'
9:42'21'' Start for getting statistics about '/var/BOSaNOVA/log/EmergTrace*.bin'
9:42'21'' Start for getting statistics about '/var/BOSaNOVA/log/History*.log'
9:42'30'' There are 3 file(s) found
```

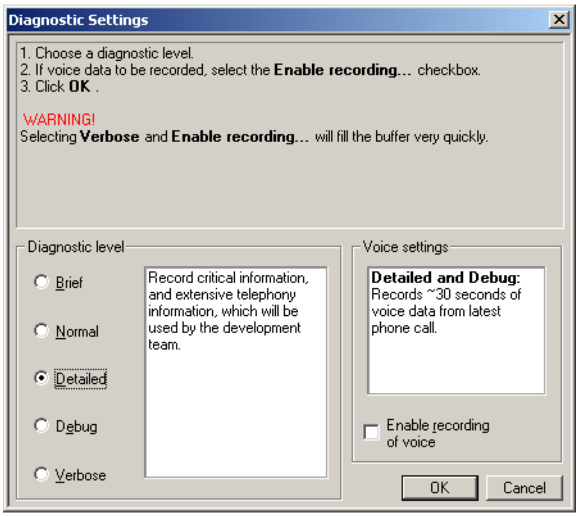
In the Emergency Trace file name, the numbers indicate the year_month_date_and time of the emergency trace. An Emergency Trace is generated only when there is a crash of the system or of a module of the system.

4. Select the checkboxes of the files to be saved locally.
5. Click **Start**. Confirmation of the transfer is indicated in the messages area at the bottom of the screen.
6. Click **Close**.

SETTING THE DIAGNOSTIC LEVELS

Use this task to set the diagnostic level.

1. Run the Maintenance Wizard. (If you need help, see "Running the Maintenance Wizard" on page 294.)
2. Connect to the required Gateway.
    - If you need help and know the Gateway's IP address, see "Connecting to a Gateway With a Known Address" on page 299.
    - If you need help and do not know the Gateway's IP address, see "Finding Gateways and Reviewing Their Status" on page 296.
3. Select **Diagnostics level**.
4. Click **Next**. The **Diagnostics Settings** screen appears.



Diagnostic Settings

1. Choose a diagnostic level.
2. If voice data to be recorded, select the **Enable recording...** checkbox.
3. Click **OK** .

WARNING!
Selecting **Verbose** and **Enable recording...** will fill the buffer very quickly.

Diagnostic level

○ Brief
○ Normal
● Detailed
○ Debug
○ Verbose

Record critical information, and extensive telephony information, which will be used by the development team.

Voice settings

Detailed and Debug: Records ~30 seconds of voice data from latest phone call.

□ Enable recording of voice

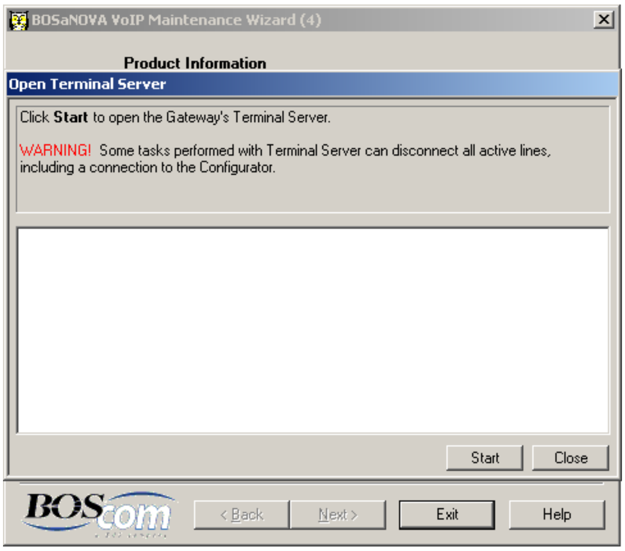
*Selecting **Verbose** and **Enable recording** will fill the buffer very quickly.*

5. Choose a diagnostic level from the left column.
6. Select or clear **Enable recording of voice**.

The results of these diagnostics will be written to the Binary Trace files, which can then be transferred to a local file and saved for inspection. These file can then be decoded and viewed as a text file.

OPENING THE TERMINAL SERVER

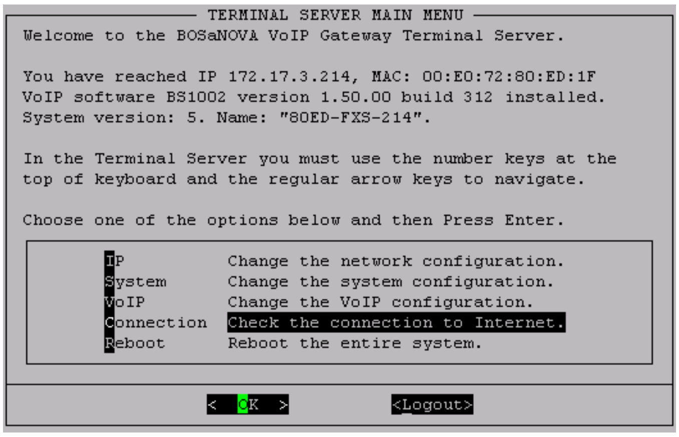
1. Run the Maintenance Wizard. (If you need help, see "Running the Maintenance Wizard" on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway's IP address, see "Connecting to a Gateway With a Known Address" on page 299.
   - If you need help and do not know the Gateway's IP address, see "Finding Gateways and Reviewing Their Status" on page 296.
3. Select **Open Terminal Server**.
4. Click **Next**. The **Open Terminal Server** screen appears.



Click **Start** to open the Gateway's Terminal Server.

WARNING! Some tasks performed with Terminal Server can disconnect all active lines, including a connection to the Configurator.

5. Click **Start**. The Terminal Server Main Menu is displayed.



```
                    TERMINAL SERVER MAIN MENU
Welcome to the BOSaNOVA VoIP Gateway Terminal Server.

You have reached IP 172.17.3.214, MAC: 00:E0:72:80:ED:1F
VoIP software BS1002 version 1.50.00 build 312 installed.
System version: 5. Name: "80ED-FXS-214".

In the Terminal Server you must use the number keys at the
top of keyboard and the regular arrow keys to navigate.

Choose one of the options below and then Press Enter.

        IP          Change the network configuration.
        System      Change the system configuration.
        VoIP        Change the VoIP configuration.
        Connection  Check the connection to Internet.
        Reboot      Reboot the entire system.

              <  OK  >              <Logout>
```

Terminal Server Options

Use the Terminal Server to:

Change the Network Configuration

- Change Basic Network Settings
- Change Internet Sharing Configuration
- Change VPN Client Settings
- Change Gateway Firewall Configuration

Change the System Configuration

- Change the Password p. 326
- Configure Modems p. 325
- Configure Network Time Protocol p. 312
- Edit / View Text Files
- Change HTTP Server Port
- Configure SNMP Alerts Servers p. 327

Change the VoIP Configuration

- Issue Internal Debug Commands
- Reset VoIP Configuration and Reboot
- Enable and Disable Quality of Service

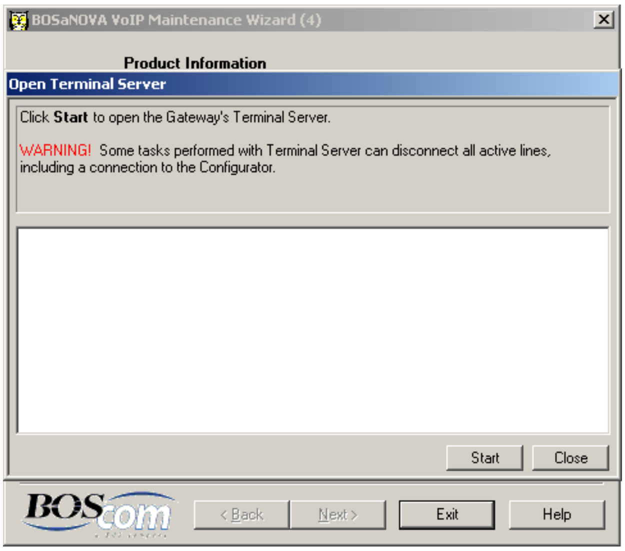
Check the internet connection p. 310

- Scan Relevant Ports on Remote Gateway

Reboot the entire system

CHECKING THE IP CONNECTION TO A GATEWAY OR COMPUTER

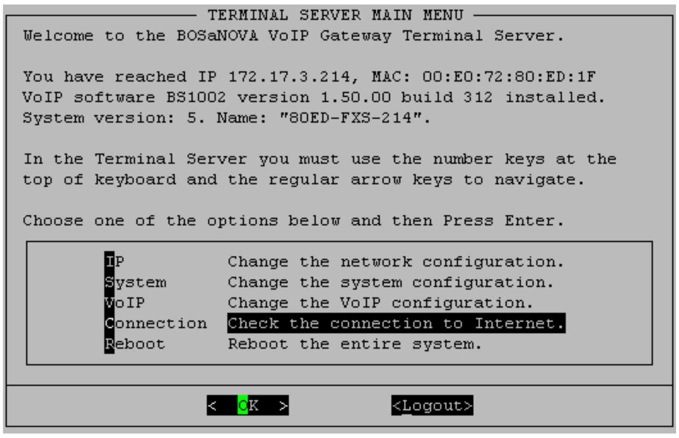
1. Run the Maintenance Wizard. (If you need help, see “Running the Maintenance Wizard” on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway’s IP address, see “Connecting to a Gateway With a Known Address” on page 299.
   - If you need help and do not know the Gateway’s IP address, see “Finding Gateways and Reviewing Their Status” on page 296.
3. Select **Open Terminal Server**.
4. Click **Next**. The **Open Terminal Server** screen appears.



Click **Start** to open the Gateway's Terminal Server.

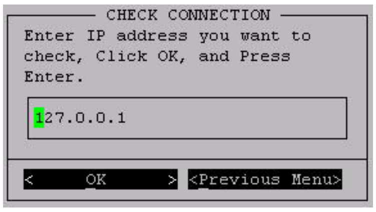
WARNING! Some tasks performed with Terminal Server can disconnect all active lines, including a connection to the Configurator.

5. Click **Start**. The Terminal Server Main Menu is displayed.



```
                    TERMINAL SERVER MAIN MENU
 Welcome to the BOSaNOVA VoIP Gateway Terminal Server.

 You have reached IP 172.17.3.214, MAC: 00:E0:72:80:ED:1F
 VoIP software BS1002 version 1.50.00 build 312 installed.
 System version: 5. Name: "80ED-FXS-214".

 In the Terminal Server you must use the number keys at the
 top of keyboard and the regular arrow keys to navigate.

 Choose one of the options below and then Press Enter.

         IP          Change the network configuration.
         System      Change the system configuration.
         VoIP        Change the VoIP configuration.
         Connection  Check the connection to Internet.
         Reboot      Reboot the entire system.

                  <  OK  >            <Logout>
```

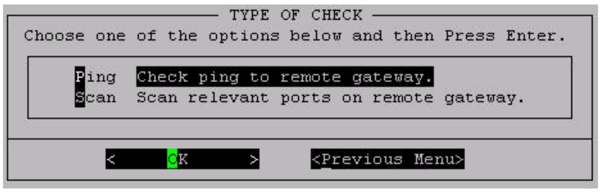
6. Select **Check the connection to Internet** and click **OK**. The **Check Connection** screen is displayed.



```
CHECK CONNECTION
Enter IP address you want to
check, Click OK, and Press
Enter.

127.0.0.1

<      OK      > <Previous Menu>
```

7. Enter the IP address to be checked.

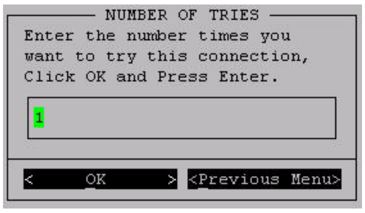
8. Select **OK** and press **Enter**. The Type of Check screen is displayed.



```
TYPE OF CHECK
Choose one of the options below and then Press Enter.

      Ping   Check ping to remote gateway.
      Scan   Scan relevant ports on remote gateway.

      <     OK     >     <Previous Menu>
```

9. Select **Check ping to remote Gateway**.

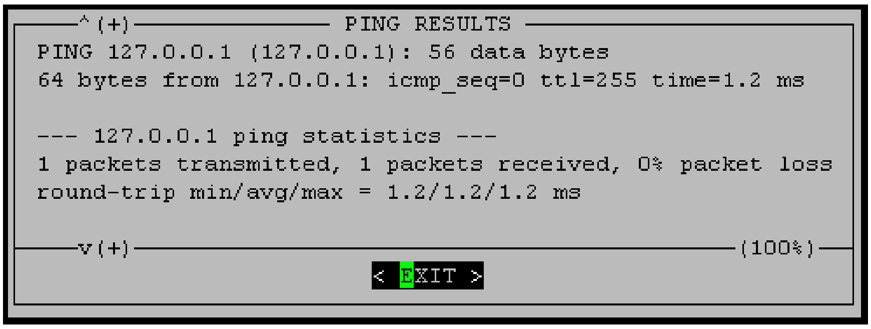
10. Select **OK** and press **Enter**. The Number of Tries screen is displayed.



```
NUMBER OF TRIES
Enter the number times you
want to try this connection,
Click OK and Press Enter.

1

<      OK      > <Previous Menu>
```

11. Enter the number of times you want to check this connection.

12. Select **OK** and press **Enter**. The ping results are displayed immediately.



```
^(+)                PING RESULTS
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=1.2 ms

--- 127.0.0.1 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.2/1.2/1.2 ms

v(+)                                              (100%)
                      < EXIT >
```

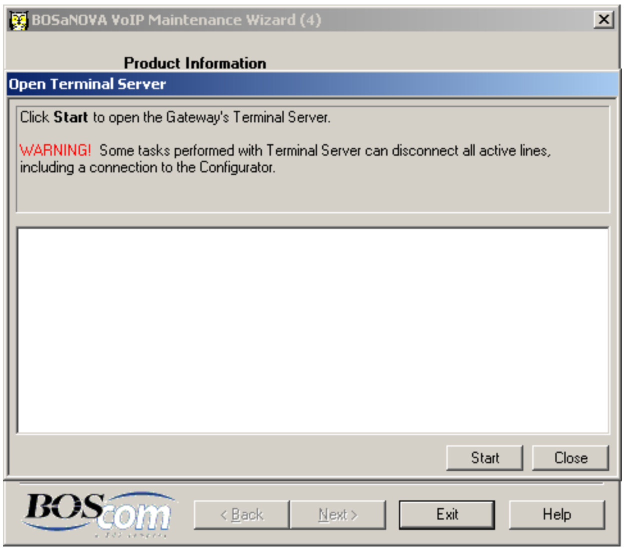
CONFIGURING NETWORK TIME PROTOCOL

The Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver or modem. NTP provides accuracies typically within a millisecond on LANs and up to a few tens of milliseconds on WANs relative to Coordinated Universal Time (UTC) via a Global Positioning Service (GPS) receiver, for example. Typical NTP configurations utilize multiple redundant servers and diverse network paths in order to achieve high accuracy and reliability.

For more information, see the NTP Web site: http://www.ntp.org

To configure time synchronization on a Gateway:

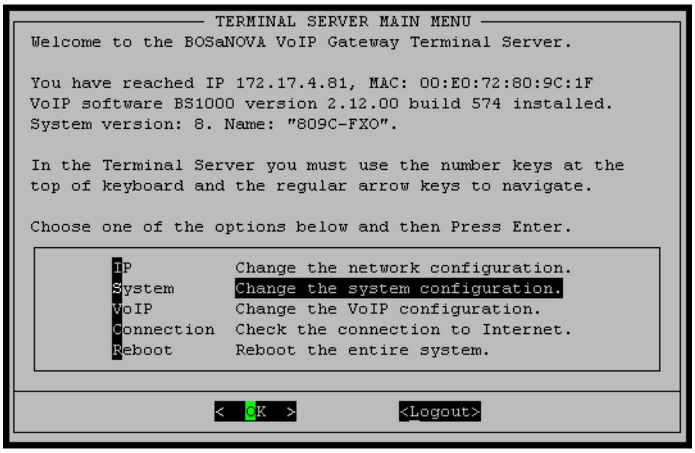
1. Run the Maintenance Wizard. (If you need help, see “Running the Maintenance Wizard” on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway’s IP address, see “Connecting to a Gateway With a Known Address” on page 299.
   - If you need help and do not know the Gateway’s IP address, see “Finding Gateways and Reviewing Their Status” on page 296.
3. Select **Open Terminal Server**.
4. Click **Next**. The **Open Terminal Server** screen appears.



Click **Start** to open the Gateway's Terminal Server.

WARNING! Some tasks performed with Terminal Server can disconnect all active lines, including a connection to the Configurator.

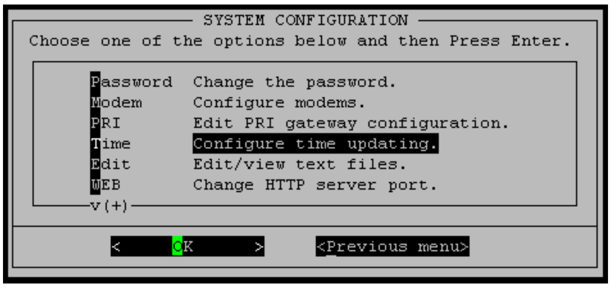
5. Click **Start**. The Terminal Server Main Menu is displayed.



```
TERMINAL SERVER MAIN MENU
Welcome to the BOSaNOVA VoIP Gateway Terminal Server.

You have reached IP 172.17.4.81, MAC: 00:E0:72:80:9C:1F
VoIP software BS1000 version 2.12.00 build 574 installed.
System version: 8. Name: "809C-FXO".

In the Terminal Server you must use the number keys at the
top of keyboard and the regular arrow keys to navigate.

Choose one of the options below and then Press Enter.

        IP           Change the network configuration.
        System       Change the system configuration.
        VoIP         Change the VoIP configuration.
        Connection   Check the connection to Internet.
        Reboot       Reboot the entire system.

              <  OK  >          <Logout>
```

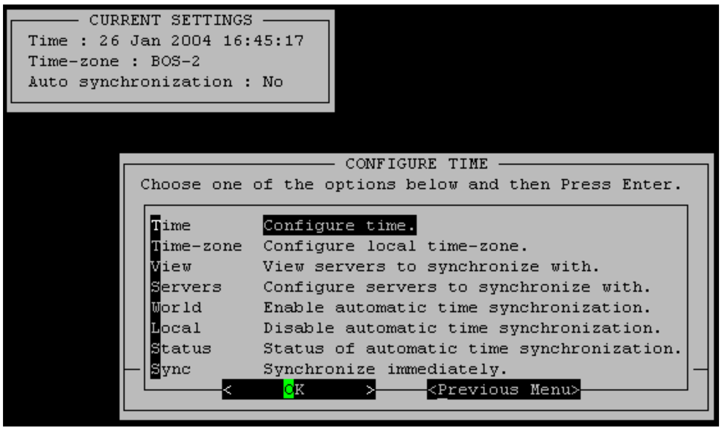
6. Select **Change the system configuration**.

7. Select **OK** and press **Enter**. The System Configuration screen is displayed.



```
SYSTEM CONFIGURATION
Choose one of the options below and then Press Enter.

        Password   Change the password.
        Modem      Configure modems.
        PRI        Edit PRI gateway configuration.
        Time       Configure time updating.
        Edit       Edit/view text files.
        WEB        Change HTTP server port.
        v(+)

        <      OK      >      <Previous menu>
```

8. Select **Configure time updating**. The Configure time screen is displayed.



```
CURRENT SETTINGS
Time : 26 Jan 2004 16:45:17
Time-zone : BOS-2
Auto synchronization : No

CONFIGURE TIME
Choose one of the options below and then Press Enter.

 Time        Configure time.
 Time-zone   Configure local time-zone.
 View        View servers to synchronize with.
 Servers     Configure servers to synchronize with.
 World       Enable automatic time synchronization.
 Local       Disable automatic time synchronization.
 Status      Status of automatic time synchronization.
 Sync        Synchronize immediately.
        <      OK      >      <Previous Menu>
```

9. Choose one of the options, select **OK**, and press **Enter**.

10. Instructions are provided in the prompts which appear on each screen. Upon completion, select **OK** and press **Enter**.

11. Select **Previous Menu** and press **Enter** until arriving at the main menu.

12. Select **Logout** and press **Enter** to close the Terminal Server.

SECTION 20: MAINTENANCE WIZARD’S SECONDARY APPLICATIONS

Use the Maintenance Wizard to fix problems with BOSâNOVA Gateways on an IP Telephony network. If your Gateways are running properly, use of the Maintenance Wizard is limited to occasional software upgrades.

This section contains useful procedures performed with the BOSâNOVA IP Telephony Gateway Maintenance Wizard, including:

- Getting the configuration files, see p. 315
- Changing and uploading the configuration files, see p. 317
- Setting Maximum Call Duration, see p. 318
- Getting the trace saved during the previous restart, see p. 320
- Setting the date and time (required when using CDR/QSR), see p. 321
- Getting and transferring the binary trace data from the Gateway’s trace buffer to a local PC file system, see see p. 322
- Configuring IP settings, see p. 324
- Changing the system password, see p. 326
- Configuring modems, see p. 325
- Checking open TCP/IP ports, see see p. 329

COPYING GATEWAY CONFIGURATION FILES TO ANOTHER LOCATION

It may be necessary to save one or more of the following Gateway configuration files:

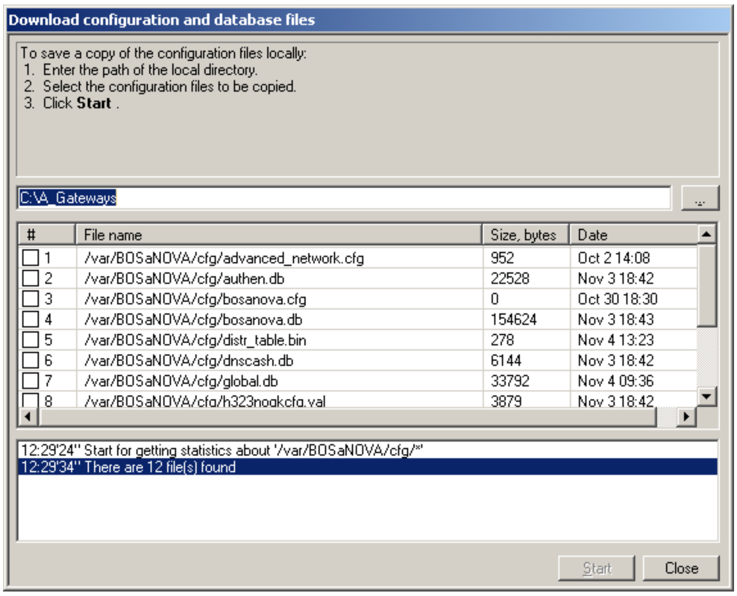
Table 59: Configuration files and their parameters

bosanova.db	VoIP parameters
h323nogkcfg.val	H.323 stack parameters
h323usegkcfg.val	
global.db	Numbering Plan parameters common to all Gateways sharing the same Officer
local.db	Local Numbering Plan parameters
local_temp.db	Local Numbering Plan parameters before synchronization with the Officer
authen.db	Authentication tables
dnscash.db	Cash of the internal DNS server used when working with 3rd party providers
signals.cfg	Parameters for generating signals and tones for the user, and for communication between telephony equipment

To save Gateway configuration files:

1. Run the Maintenance Wizard. (If you need help, see "Running the Maintenance Wizard" on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway's IP address, see "Connecting to a Gateway With a Known Address" on page 299.
   - If you need help and do not know the Gateway's IP address, see "Finding Gateways and Reviewing Their Status" on page 296.

3. Select **Download configuration and database files** and click **Next**. The Download configuration and database files screen is displayed.



To save a copy of the configuration files locally:
1. Enter the path of the local directory.
2. Select the configuration files to be copied.
3. Click **Start** .

C:\A_Gateways

#	File name	Size, bytes	Date
□ 1	/var/BOSaNOVA/cfg/advanced_network.cfg	952	Oct 2 14:08
□ 2	/var/BOSaNOVA/cfg/authen.db	22528	Nov 3 18:42
□ 3	/var/BOSaNOVA/cfg/bosanova.cfg	0	Oct 30 18:30
□ 4	/var/BOSaNOVA/cfg/bosanova.db	154624	Nov 3 18:43
□ 5	/var/BOSaNOVA/cfg/distr_table.bin	278	Nov 4 13:23
□ 6	/var/BOSaNOVA/cfg/dnscash.db	6144	Nov 3 18:42
□ 7	/var/BOSaNOVA/cfg/global.db	33792	Nov 4 09:36
□ 8	/var/BOSaNOVA/cfg/h323nogkcfg.val	3879	Nov 3 18:42

```
12:29'24" Start for getting statistics about '/var/BOSaNOVA/cfg/*'
12:29'34" There are 12 file(s) found
```

4. Enter the path of the location where the configuration files are to be saved.

5. Select the files you wish to save.

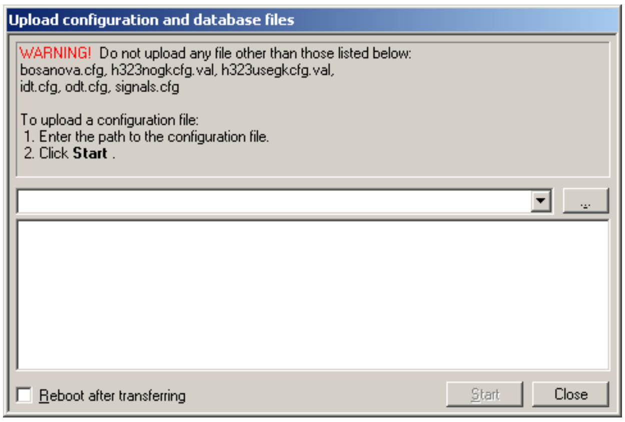
6. Click **Start**. Confirmation is reported in the messages area.

7. Click **Close** to return to the **Task Selection screen**.

UPLOADING CONFIGURATION FILES

If the configuration files are saved on a PC, they can be retrieved and reapplied to the Gateway.

1. Run the Maintenance Wizard. (If you need help, see "Running the Maintenance Wizard" on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway's IP address, see "Connecting to a Gateway With a Known Address" on page 299.
   - If you need help and do not know the Gateway's IP address, see "Finding Gateways and Reviewing Their Status" on page 296.
3. Select **Upload configuration and database files** and click **Next**. The Upload configuration and database files screen appears. (See Table 59 on page 315 for a description of the files and databases.)



Upload configuration and database files

WARNING! Do not upload any file other than those listed below:
bosanova.cfg, h323nogkcfg.val, h323usegkcfg.val,
idt.cfg, odt.cfg, signals.cfg

To upload a configuration file:
1. Enter the path to the configuration file.
2. Click **Start** .

Do not upload any files except the following: bosanova.db, h323nogkcfg.val, h323usegkcfg.val, global.db, local.db, authen.db, and signals.cfg.

4. Enter the path to the configuration file to be uploaded.
5. To reboot the Gateway immediately after uploading, select **Reboot after transferring**.

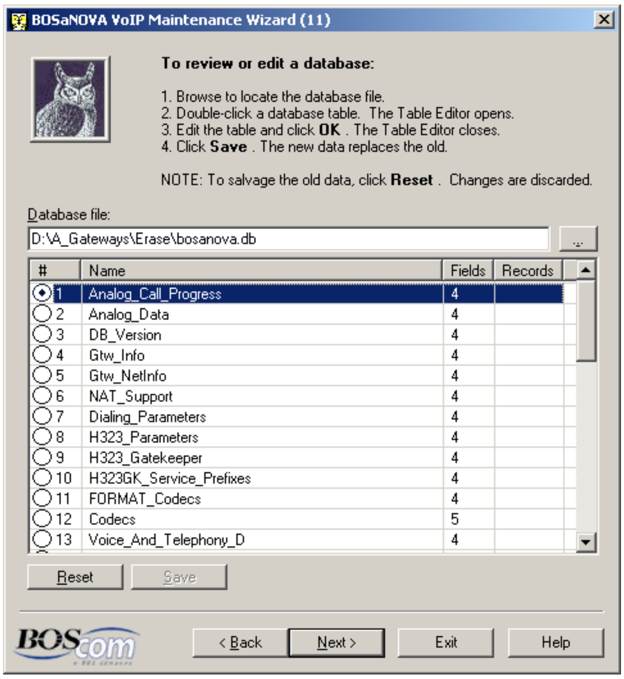
Rebooting the system will disconnect all active lines including the Configurator. Rebooting takes 1 to 2 minutes.

6. Click **Start**. Confirmation is reported in the messages area.
7. Click **Close**.

SETTING MAXIMUM CALL DURATION

The parameter MaximumCallDuration_U4 is not available from the Configurator. It is located in the configuration file named **`bosanova.db`**.

1. Download the configuration file bosanova.db. See “Copying Gateway Configuration Files to Another Location” on page 315.
2. Return to the Maintenance Wizard Welcome screen.
3. From the Maintenance Wizard Welcome screen, select **Database Maintenance**. The “review or edit page” of the Wizard is displayed.



BOSaNOVA VoIP Maintenance Wizard (11)

To review or edit a database:

1. Browse to locate the database file.
2. Double-click a database table. The Table Editor opens.
3. Edit the table and click **OK** . The Table Editor closes.
4. Click **Save** . The new data replaces the old.

NOTE: To salvage the old data, click **Reset** . Changes are discarded.

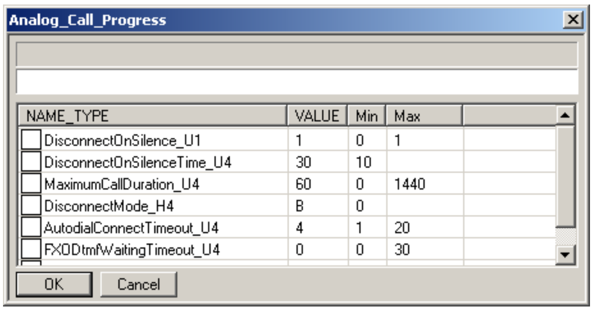
Database file: D:\A_Gateways\Erase\bosanova.db

#	Name	Fields	Records
● 1	Analog_Call_Progress	4	
○ 2	Analog_Data	4	
○ 3	DB_Version	4	
○ 4	Gtw_Info	4	
○ 5	Gtw_NetInfo	4	
○ 6	NAT_Support	4	
○ 7	Dialing_Parameters	4	
○ 8	H323_Parameters	4	
○ 9	H323_Gatekeeper	4	
○ 10	H323GK_Service_Prefixes	4	
○ 11	FORMAT_Codecs	4	
○ 12	Codecs	5	
○ 13	Voice_And_Telephony_D	4	

4. Define the location of the file that was downloaded in step #1.
5. Depending upon the Gateway type, double-click either the table named **Analog _Call_Progress** or the table named **PRI_Call_Progress**.

Do not click Next.

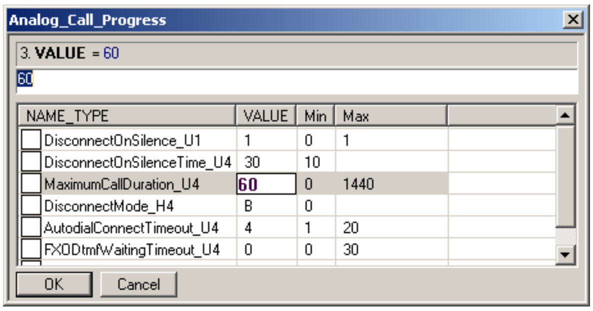
The table editor opens and the fields of the Call_Progress table are displayed.



Analog_Call_Progress

NAME_TYPE	VALUE	Min	Max
□ DisconnectOnSilence_U1	1	0	1
□ DisconnectOnSilenceTime_U4	30	10	
□ MaximumCallDuration_U4	60	0	1440
□ DisconnectMode_H4	B	0	
□ AutodialConnectTimeout_U4	4	1	20
□ FXODtmfWaitingTimeout_U4	0	0	30

6. Select the **Value** field of the Maximum_Call_Duration row.



3. VALUE = 60

60

	NAME_TYPE	VALUE	Min	Max
□	DisconnectOnSilence_U1	1	0	1
□	DisconnectOnSilenceTime_U4	30	10	
□	MaximumCallDuration_U4	60	0	1440
□	DisconnectMode_H4	B	0	
□	AutodialConnectTimeout_U4	4	1	20
□	FXODtmfWaitingTimeout_U4	0	0	30

7. Enter the new value and click **OK**. The table editor closes.

Value is measured in minutes. There, the value 120 equals two hours.

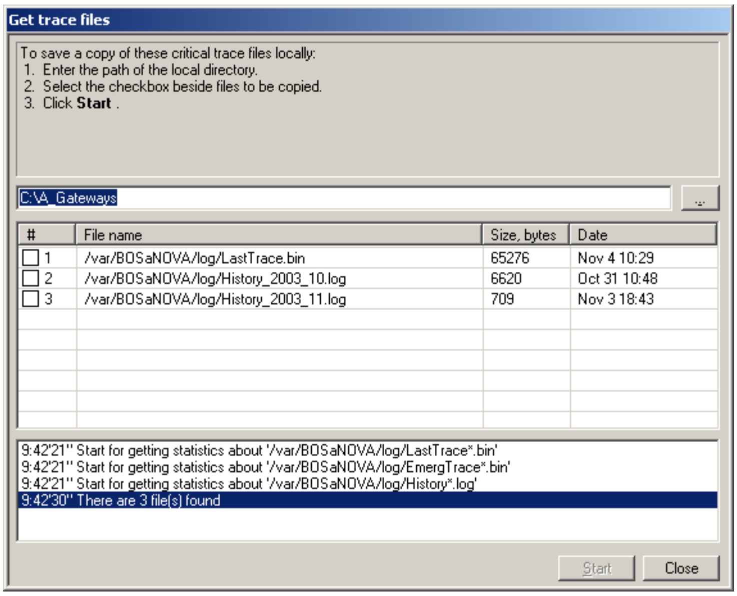
8. On the "review or edit" page of the Wizard (page 11), click **Save**.

9. Upload the configuration file. See "Uploading Configuration Files" on page 317.

GET THE TRACE FILES SAVED DURING THE PREVIOUS RESTART AND CHECK FOR EMERGENCY TRACES

This task gets and saves the trace files in LastTrace.bin to a location on your PC. Technical Support may ask for a copy of the trace files.

1. Run the Maintenance Wizard. (If you need help, see “Running the Maintenance Wizard” on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway’s IP address, see “Connecting to a Gateway With a Known Address” on page 299.
   - If you need help and do not know the Gateway’s IP address, see “Finding Gateways and Reviewing Their Status” on page 296.
3. From the Task Selection list, select **Get trace files** and click **Next**. The Get various trace files screen is displayed.
4. Select **List critical trace files** and click **Next**. A list of trace files is displayed.



To save a copy of these critical trace files locally:
1. Enter the path of the local directory.
2. Select the checkbox beside files to be copied.
3. Click **Start** .

C:\A_Gateways

#	File name	Size, bytes	Date
□ 1	/var/BOSaNOVA/log/LastTrace.bin	65276	Nov 4 10:29
□ 2	/var/BOSaNOVA/log/History_2003_10.log	6620	Oct 31 10:48
□ 3	/var/BOSaNOVA/log/History_2003_11.log	709	Nov 3 18:43

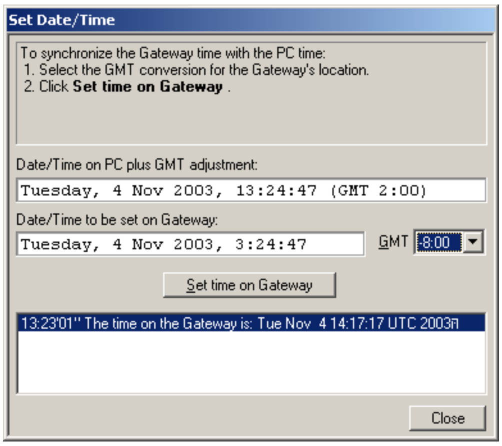
```
9:42'21'' Start for getting statistics about '/var/BOSaNOVA/log/LastTrace*.bin'
9:42'21'' Start for getting statistics about '/var/BOSaNOVA/log/EmergTrace*.bin'
9:42'21'' Start for getting statistics about '/var/BOSaNOVA/log/History*.log'
9:42'30'' There are 3 file(s) found
```

5. Enter the path of the location off of the Gateway where the files are to be saved.
6. Select the files to be saved.
7. Click **Start**. Confirmation appears both in the upper and lower pane.

SETTING THE DATE AND TIME

This tool synchronizes the clocks on the Gateway and on the local computers. You must know the GMT conversion factor for your local time zone. Time synchronization is required when using CDR/QSR.

1. Run the Maintenance Wizard. (If you need help, see "Running the Maintenance Wizard" on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway's IP address, see "Connecting to a Gateway With a Known Address" on page 299.
   - If you need help and do not know the Gateway's IP address, see "Finding Gateways and Reviewing Their Status" on page 296.
3. Select **Set Date/Time** and click **Next**. The **Set time on Gateway** screen appears with the current date and time displayed in the messages area.



Set Date/Time

To synchronize the Gateway time with the PC time:
1. Select the GMT conversion for the Gateway's location.
2. Click **Set time on Gateway** .

Date/Time on PC plus GMT adjustment:
Tuesday, 4 Nov 2003, 13:24:47 (GMT 2:00)

Date/Time to be set on Gateway:
Tuesday, 4 Nov 2003, 3:24:47

GMT -8:00

13:23'01'' The time on the Gateway is: Tue Nov 4 14:17:17 UTC 2003

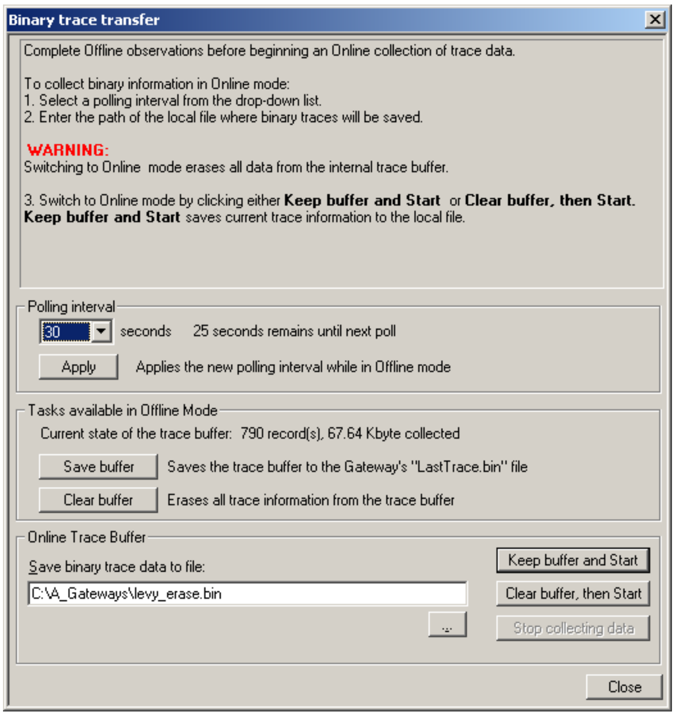
4. Select the GMT conversion factor for the time zone of the local Gateway from the drop down menu on the right. If you do not know this factor go to http://greenwichmeantime.com
5. Click **Set time on Gateway**.
6. Click **Close**.

BINARY TRACE TRANSFER

This task gathers binary trace data either while in offline mode or while in online mode. Data is transfered from the Gateway's trace buffer to a file on a local file PC. These files are updated according to the polling interval. This continues as long as the Maintenance Wizard is connected to the Gateway.

Online trace transfer can require extensive bandwidth. If you are connected remotely to the Gateway, be careful that the transfer rate of the binary trace file does not exceed the bandwidth.

1. Run the Maintenance Wizard. (If you need help, see "Running the Maintenance Wizard" on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway's IP address, see "Connecting to a Gateway With a Known Address" on page 299.
   - If you need help and do not know the Gateway's IP address, see "Finding Gateways and Reviewing Their Status" on page 296.
3. Select **Binary trace transfer**.
4. Click **Next**. The **Binary trace transfer** screen appears.



Complete Offline observations before beginning an Online collection of trace data.

To collect binary information in Online mode:
1. Select a polling interval from the drop-down list.
2. Enter the path of the local file where binary traces will be saved.

WARNING:
Switching to Online mode erases all data from the internal trace buffer.

3. Switch to Online mode by clicking either **Keep buffer and Start** or **Clear buffer, then Start.**
Keep buffer and Start saves current trace information to the local file.

30 seconds 25 seconds remains until next poll

Applies the new polling interval while in Offline mode

Current state of the trace buffer: 790 record(s), 67.64 Kbyte collected

Saves the trace buffer to the Gateway's "LastTrace.bin" file

Erases all trace information from the trace buffer

Save binary trace data to file:
C:\A_Gateways\levy_erase.bin

5. In offline mode, complete the following tasks:
   - Choose the polling interval. This polling interval can be 1, 5, 30, 120, or 600 seconds. Choose this parameter at the recommendation of the Technical support personnel and click **Apply.**

The polling interval must be small enough that the buffer does not overflow.

   - Click **Save buffer** to save the last trace from the trace buffer to the Gateway's LastTrace.bin file before you clear the buffer.
   - Click **Clear buffer** to erase all trace information from the trace buffer.

6. To switch to online mode:

   a. Enter the path to the location where you wish to save the trace files. You may browse to find a suitable folder.

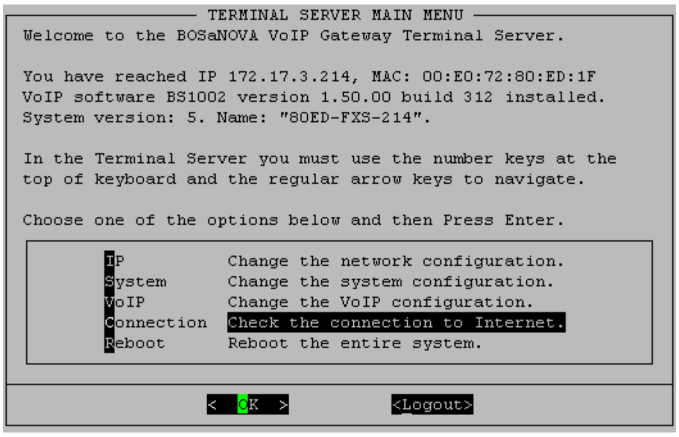
   b. Click either:

      - **Keep buffer** and **Start**
        Transfers the trace buffer and continues appending trace data.
      - **Clear buffer** and **Start**
        Erases the Gateway's buffer and start a new trace.

The file size is only limited by the size of the hard disk on the PC. A high level of verbosity can quickly enlarge a file.

CONFIGURING IP SETTINGS

1. Run the Maintenance Wizard. (If you need help, see “Running the Maintenance Wizard” on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway’s IP address, see “Connecting to a Gateway With a Known Address” on page 299.
   - If you need help and do not know the Gateway’s IP address, see “Finding Gateways and Reviewing Their Status” on page 296.
3. Select **Open Terminal Server** and click **Next**. The **Open Terminal Server** screen appears.
4. Click **Start**. The Terminal Server Main Menu is displayed.

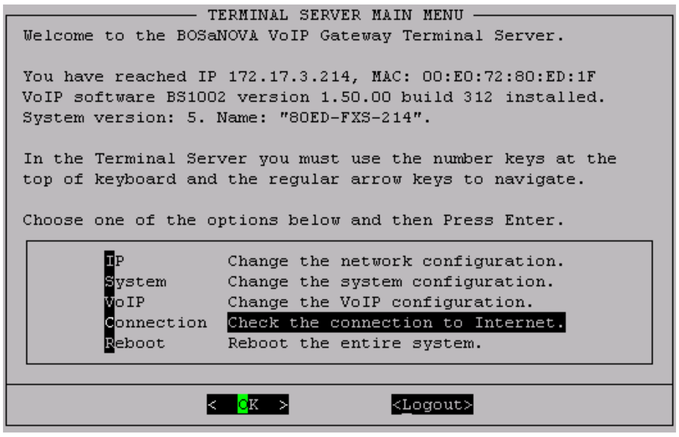


```
TERMINAL SERVER MAIN MENU
Welcome to the BOSaNOVA VoIP Gateway Terminal Server.

You have reached IP 172.17.3.214, MAC: 00:E0:72:80:ED:1F
VoIP software BS1002 version 1.50.00 build 312 installed.
System version: 5. Name: "80ED-FXS-214".

In the Terminal Server you must use the number keys at the
top of keyboard and the regular arrow keys to navigate.

Choose one of the options below and then Press Enter.

        IP          Change the network configuration.
        System      Change the system configuration.
        VoIP        Change the VoIP configuration.
        Connection  Check the connection to Internet.
        Reboot      Reboot the entire system.
```

5. From the Terminal Server Main Menu, choose the first option **Change the Network Configuration**.
6. Follow the wizard, filling in the dialog boxes as they pertain to your system.
7. At the confirmation screen, decide if you want to reboot and apply the changes to the setup configuration or leave without making any changes.

CONFIGURING A MODEM

1. Run the Maintenance Wizard. (If you need help, see "Running the Maintenance Wizard" on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway's IP address, see "Connecting to a Gateway With a Known Address" on page 299.
   - If you need help and do not know the Gateway's IP address, see "Finding Gateways and Reviewing Their Status" on page 296.
3. Select **Open Terminal Server** and click **Next**. The **Open Terminal Server** screen appears.
4. Click **Start**. The Terminal Server Main Menu is displayed.

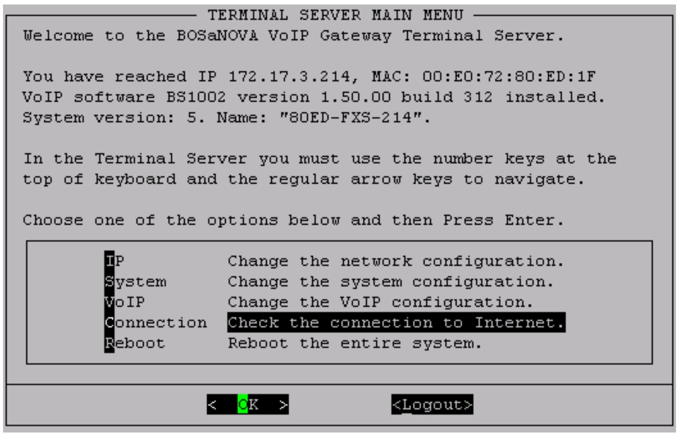


```
                     TERMINAL SERVER MAIN MENU
Welcome to the BOSaNOVA VoIP Gateway Terminal Server.

You have reached IP 172.17.3.214, MAC: 00:E0:72:80:ED:1F
VoIP software BS1002 version 1.50.00 build 312 installed.
System version: 5. Name: "80ED-FXS-214".

In the Terminal Server you must use the number keys at the
top of keyboard and the regular arrow keys to navigate.

Choose one of the options below and then Press Enter.

        IP          Change the network configuration.
        System      Change the system configuration.
        VoIP        Change the VoIP configuration.
        Connection  Check the connection to Internet.
        Reboot      Reboot the entire system.

                   <  OK  >          <Logout>
```

5. From the Terminal Server Main Menu, choose **Change the system configuration**.
6. Chose **Configure modems**.
7. Follow the wizard, filling in the dialog boxes as they pertain to your system.

CHANGING THE SYSTEM PASSWORD

1. Run the Maintenance Wizard. (If you need help, see “Running the Maintenance Wizard” on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway’s IP address, see “Connecting to a Gateway With a Known Address” on page 299.
   - If you need help and do not know the Gateway’s IP address, see “Finding Gateways and Reviewing Their Status” on page 296.
3. Select **Open Terminal Server** and click **Next**. The **Open Terminal Server** screen appears.
4. Click **Start**. The Terminal Server Main Menu is displayed.



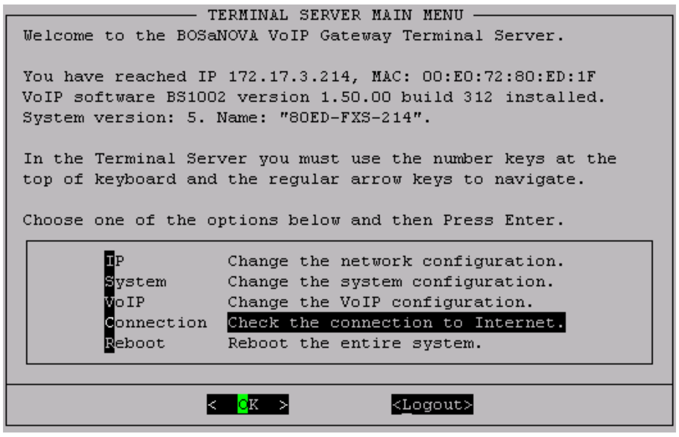
```
                 TERMINAL SERVER MAIN MENU
Welcome to the BOSaNOVA VoIP Gateway Terminal Server.

You have reached IP 172.17.3.214, MAC: 00:E0:72:80:ED:1F
VoIP software BS1002 version 1.50.00 build 312 installed.
System version: 5. Name: "80ED-FXS-214".

In the Terminal Server you must use the number keys at the
top of keyboard and the regular arrow keys to navigate.

Choose one of the options below and then Press Enter.

        IP          Change the network configuration.
        System      Change the system configuration.
        VoIP        Change the VoIP configuration.
        Connection  Check the connection to Internet.
        Reboot      Reboot the entire system.

                 <  OK  >          <Logout>
```

5. From the Terminal Server Main Menu, choose **Change the system configuration**.
6. Choose **Change the password**.
7. Enter the new password.
8. Press **Enter**.
9. Reenter new password and press **Enter**.
10. If you do not get confirmation of a successfully changed password, go back to Step 1.

CONFIGURING AN SNMP TRAPS AND ALARMS SERVER

Use this procedure to specify the IP address of computers that will receive the SNMP messages and traps.

1. Run the Maintenance Wizard. (If you need help, see "Running the Maintenance Wizard" on page 294.)
2. Connect to the required Gateway.
    - If you need help and know the Gateway's IP address, see "Connecting to a Gateway With a Known Address" on page 299.
    - If you need help and do not know the Gateway's IP address, see "Finding Gateways and Reviewing Their Status" on page 296.
3. Select **Open Terminal Server** and click **Next**. The **Open Terminal Server** screen appears.
4. Click **Start**. The Terminal Server Main Menu is displayed.



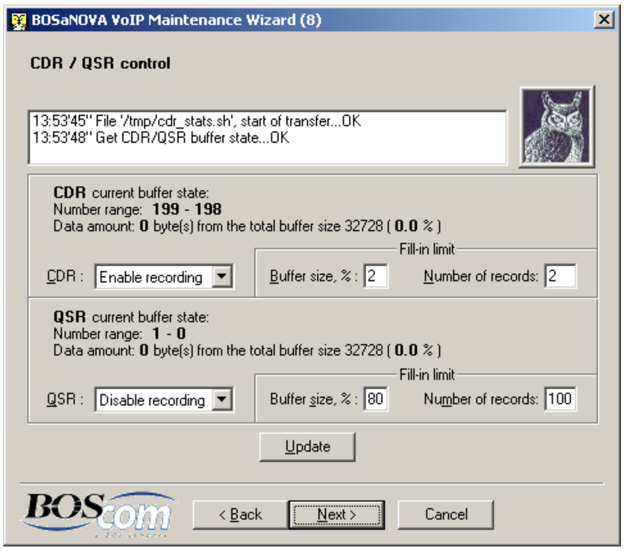
```
TERMINAL SERVER MAIN MENU
Welcome to the BOSaNOVA VoIP Gateway Terminal Server.

You have reached IP 172.17.3.214, MAC: 00:E0:72:80:ED:1F
VoIP software BS1002 version 1.50.00 build 312 installed.
System version: 5. Name: "80ED-FXS-214".

In the Terminal Server you must use the number keys at the
top of keyboard and the regular arrow keys to navigate.

Choose one of the options below and then Press Enter.

        IP          Change the network configuration.
        System      Change the system configuration.
        VoIP        Change the VoIP configuration.
        Connection  Check the connection to Internet.
        Reboot      Reboot the entire system.

                  <  OK  >          <Logout>
```

5. Select **Change the System Configuration** and press Enter.
6. Select **Configure SNMP alerts servers** and press Enter.
7. Enter the IP address of the computer that will host the SNMP manager. If there is more than one computer that will be able to receive SNMP messages, separate the IP addresses by one space.
8. Press **Enter**.

CONFIGURING CDR AND QSR BUFFERS

This screen allows you to enable and disable the CDR and the QSR trace buffers, along with setting the parameters that determine when the trace buffers are flushed to the CDR server (SSH server).

1. Run the Maintenance Wizard. (If you need help, see “Running the Maintenance Wizard” on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway’s IP address, see “Connecting to a Gateway With a Known Address” on page 299.
   - If you need help and do not know the Gateway’s IP address, see “Finding Gateways and Reviewing Their Status” on page 296.
3. Select **CDR/QSR Control**. The CDR/QSR control screen appears.



```
13:53'45'' File '/tmp/cdr_stats.sh', start of transfer...OK
13:53'48'' Get CDR/QSR buffer state...OK
```

CDR current buffer state:
Number range: **199 - 198**
Data amount: **0** byte(s) from the total buffer size 32728 (**0.0** %)

Fill-in limit

CDR : Enable recording — Buffer size, % : 2 — Number of records: 2

QSR current buffer state:
Number range: **1 - 0**
Data amount: **0** byte(s) from the total buffer size 32728 (**0.0** %)

Fill-in limit

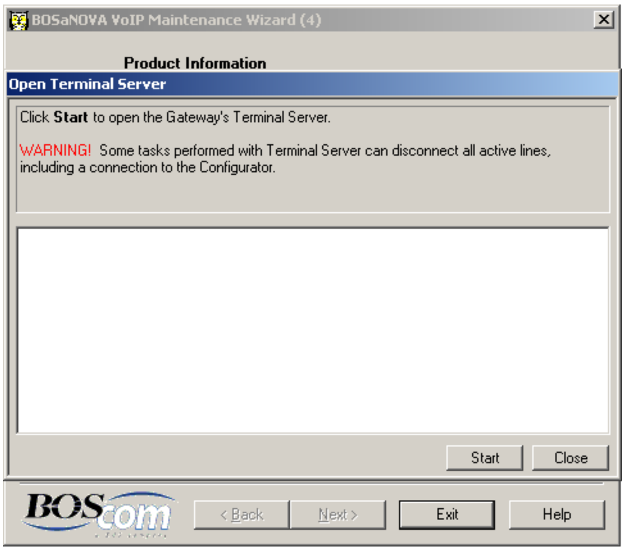
QSR : Disable recording — Buffer size, % : 80 — Number of records: 100

4. Configure the settings and click **Update**.

CHECKING OPEN TCP/IP PORTS

To verify which TCP/IP ports are opened on both sides of a network:

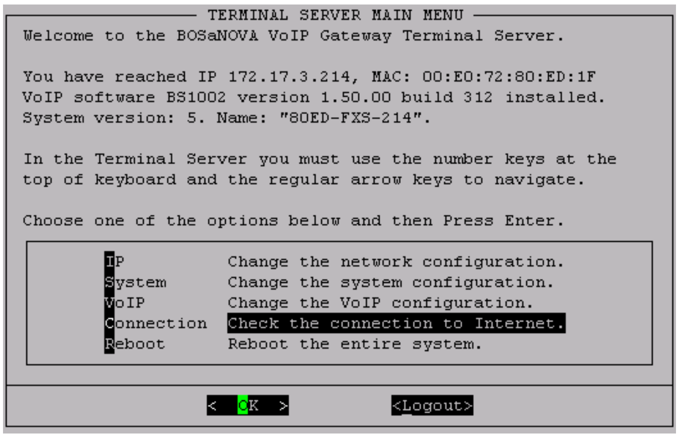
1. Run the Maintenance Wizard. (If you need help, see "Running the Maintenance Wizard" on page 294.)
2. Connect to the required Gateway.
   - If you need help and know the Gateway's IP address, see "Connecting to a Gateway With a Known Address" on page 299.
   - If you need help and do not know the Gateway's IP address, see "Finding Gateways and Reviewing Their Status" on page 296.
3. Select **Open Terminal Server** and click **Next**. The **Open Terminal Server** screen appears.



Click **Start** to open the Gateway's Terminal Server.

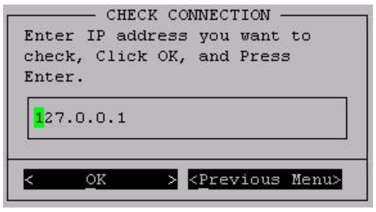
WARNING! Some tasks performed with Terminal Server can disconnect all active lines, including a connection to the Configurator.

4. Click **Start**. The Terminal Server Main Menu is displayed.



```
TERMINAL SERVER MAIN MENU
Welcome to the BOSaNOVA VoIP Gateway Terminal Server.

You have reached IP 172.17.3.214, MAC: 00:E0:72:80:ED:1F
VoIP software BS1002 version 1.50.00 build 312 installed.
System version: 5. Name: "80ED-FXS-214".

In the Terminal Server you must use the number keys at the
top of keyboard and the regular arrow keys to navigate.

Choose one of the options below and then Press Enter.

          IP          Change the network configuration.
          System      Change the system configuration.
          VoIP        Change the VoIP configuration.
          Connection  Check the connection to Internet.
          Reboot      Reboot the entire system.

                  <  OK  >              <Logout>
```

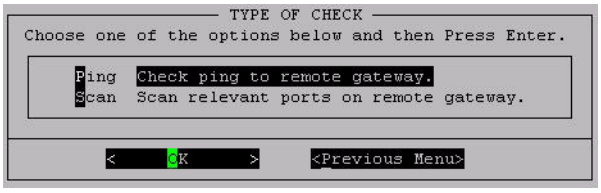
5. Select **Check the connection to Internet** and click **OK**. The **Check Connection** screen is displayed.



```
CHECK CONNECTION
Enter IP address you want to
check, Click OK, and Press
Enter.

127.0.0.1

<      OK      >  <Previous Menu>
```

6. Enter the IP address to be checked.

7. Select **OK** and press **Enter**. The Type of Check screen is displayed.

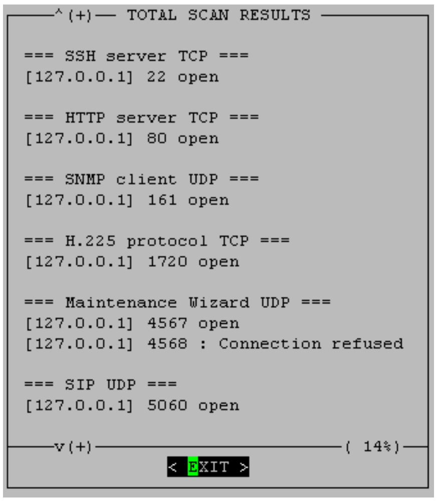


```
TYPE OF CHECK
Choose one of the options below and then Press Enter.

Ping   Check ping to remote gateway.
Scan   Scan relevant ports on remote gateway.

<     OK     >     <Previous Menu>
```

8. Select **Scan relevant ports on remote Gateway** and click **OK**.

The scan may take several minutes. Do not press any keys while the scan is running.

When the scan is complete, the Total Scan Results message is displayed.



```
^(+)── TOTAL SCAN RESULTS

=== SSH server TCP ===
[127.0.0.1] 22 open

=== HTTP server TCP ===
[127.0.0.1] 80 open

=== SNMP client UDP ===
[127.0.0.1] 161 open

=== H.225 protocol TCP ===
[127.0.0.1] 1720 open

=== Maintenance Wizard UDP ===
[127.0.0.1] 4567 open
[127.0.0.1] 4568 : Connection refused

=== SIP UDP ===
[127.0.0.1] 5060 open

v(+)                          ( 14%)
< EXIT >
```

SECTION 21:
SNMP

A Simple Network Management Protocol (SNMP) agent operates within every BOSâNOVA IP Telephony Gateway. The Gateways store data about themselves in the Gateway buffer. BOScom supplies Management Information Bases (MIBs) which solicit specific information from the Gateway buffer.

This allows the Gateway to be monitored by an SNMP network manager. That is, Gateways can be viewed by, and provide event notification to, an SNMP network manager. However, they cannot be managed by an SNMP network manager.

This section includes:

- Importing BOScom MIBs, see p. 332
- Defining to which SNMP Manager a Gateway sends traps, see p. 333
- The BOScom SNMP Manager Demo, see p. 334
- HP OpenView, see p. 340

Parts of this section are intended for personnel experienced in SNMP.

SUPPORT OF SNMP MANAGERS

BOSâNOVA IP Telephony Gateways can interact with SNMP Managers such as HP OpenView. In every case, you must complete these two steps first:

- Import the collection of BOScom and UCD private MIBs into the SNMP Manager
- Configure the Gateway to send traps to the correct SNMP Manager

BOScom and UCD MIBs are available on the BOSâNOVA IP Telephony Gateway CD-COM, in the SNMP\MIBs folder.

Importing BOScom Private MIBs

BOScom and UCD MIBs are available on the BOSâNOVA IP Telephony Gateway CD-ROM in the SNMP\MIBs folder.

1. Insert the CD-ROM into the CD-ROM drive of the computer running the SNMP Manager. The Welcome Screen appears.
2. Importing of MIBs is completed one of two ways:
   - Most SNMP Managers import MIBs from their source. Run the SNMP Manager's Import MIBs tool.
   - MIBs can also be copied and pasted into some SNMP Managers.

*The only **Community string** recognized by BOSâNOVA Gateways is* **1234**. *This allows Read-only access to all of the MIB tree.*
A Community string is the password that is needed to access an SNMP agent. The SNMP Community string is used by the device as a password to give the user clearance to read or write the information requested. If you don't have the correct community name, you cannot retrieve any data (get) or make any changes (sets). This includes attempts to browse the MIB.

The Gateway's general details can be retrieved when using the following Object Identifiers (OIDs):

- 1.3.6.1.4.1.8472.1.1.1.1.1.6.0 — Product description
- 1.3.6.1.4.1.8472.1.1.1.1.1.7.0 — Serial number
- 1.3.6.1.4.1.8472.1.1.1.1.1.8.0 — Software product ID
- 1.3.6.1.4.1.8472.1.1.1.1.1.9.0 — Build version

Defining to which SNMP Managers a Gateway Sends Traps

Skip this procedure when using the BOSâNOVA SNMP Manager Demo. BOSâNOVA SNMP Manager automatically registers itself on the Gateway while adding a Gateway to its Registered Gateways list.

All Gateways on the BOSâNOVA IP Telephony network must be configured to send traps to the computer hosting the SNMP Manager. This is done in the Terminal Server of each Gateway.

1. Open the Gateway's Terminal Server using the Maintenance Wizard (see see p. 310).
2. Enter the login name and press Enter. The default login name is: voip. The Terminal Server is case sensitive. Use only lower case letters
3. Enter the password and press Enter. The default password is: 1234. The Terminal Server Main Menu appears.

To select options in the Terminal Server, use the Up and Down arrows. To select either OK or Previous Menu, use the Tab key. To enter numbers use the number keys at the top of the keyboard.

4. Select **System— Change the System Configuration,** select **OK** and press Enter.
5. Select **SNMP— Configure SNMP alerts servers,** select **OK** and press Enter.
6. Enter the IP address of the computer running the SNMP Manager. More than one SNMP Managers can be listed. Separate the IP addresses of each SNMP Manager with a single space.
7. Select **OK** and press Enter. The Gateway's SNMP module restarts.To unregister the Gateway, repeat steps 1 to 5 and delete the IP address of the computer hosting the SNMP manager.

USING THE BOSCOM SNMP MANAGER DEMO

A demonstration SNMP Manager is provided on the BOSâNOVA IP Telephony Gateway CD-ROM. It offers limited functionality and is intended primarily to demonstrate the Gateway's ability to support SNMP.

Installing the BOScom SNMP Manager

To install the BOScom SNMP Manager:

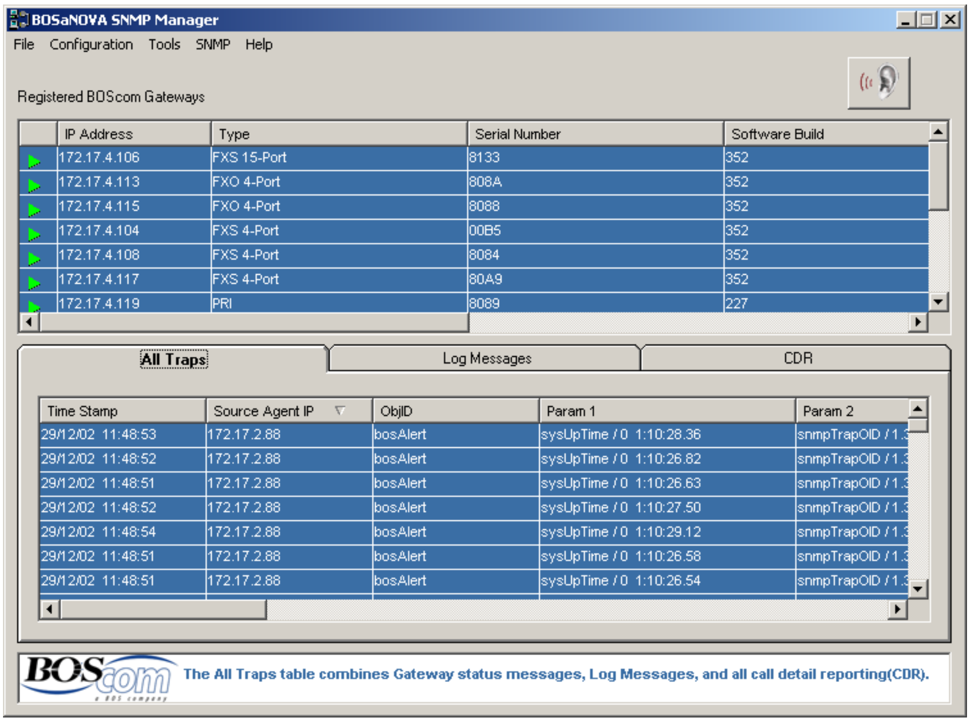
1. Insert the BOSâNOVA IP Telephony Gateway CD-ROM into the CD-ROM drive of the computer. The Welcome Screen appears.
2. Click **SNMP Manager Demo**. The installation program opens.

The installation program requires only that you confirm or change the destination folder.

Running the BOScom SNMP Manager

To run the BOScom SNMP Manager:

1. Click the Windows **Start** button.
2. Select **Programs > BOScom SNMP Manager.** The SNMP Manager main screen appears.



Registered BOScom Gateways

	IP Address	Type	Serial Number	Software Build
▶	172.17.4.106	FXS 15-Port	8133	352
▶	172.17.4.113	FXO 4-Port	808A	352
▶	172.17.4.115	FXO 4-Port	8088	352
▶	172.17.4.104	FXS 4-Port	00B5	352
▶	172.17.4.108	FXS 4-Port	8084	352
▶	172.17.4.117	FXS 4-Port	80A9	352
▶	172.17.4.119	PRI	8089	227

Time Stamp	Source Agent IP	ObjID	Param 1	Param 2
29/12/02 11:48:53	172.17.2.88	bosAlert	sysUpTime / 0 1:10:28.36	snmpTrapOID / 1.3
29/12/02 11:48:52	172.17.2.88	bosAlert	sysUpTime / 0 1:10:26.82	snmpTrapOID / 1.3
29/12/02 11:48:51	172.17.2.88	bosAlert	sysUpTime / 0 1:10:26.63	snmpTrapOID / 1.3
29/12/02 11:48:52	172.17.2.88	bosAlert	sysUpTime / 0 1:10:27.50	snmpTrapOID / 1.3
29/12/02 11:48:54	172.17.2.88	bosAlert	sysUpTime / 0 1:10:29.12	snmpTrapOID / 1.3
29/12/02 11:48:51	172.17.2.88	bosAlert	sysUpTime / 0 1:10:26.58	snmpTrapOID / 1.3
29/12/02 11:48:51	172.17.2.88	bosAlert	sysUpTime / 0 1:10:26.54	snmpTrapOID / 1.3

The All Traps table combines Gateway status messages, Log Messages, and all call detail reporting(CDR).

When opened, the SNMP Manager sends SNMP requests to all listed Gateways and waits for responses. Therefore, if there are many Gateways in the list, or if some do not respond, the SNMP Manager will open but there will be a delay before you will be able to begin working.

Using the BOScom SNMP Manager Main Screen

This SNMP Manager main screen is divided into two panes:

- **Upper pane**:
  Displays the IP address, and other information, about Gateways upon which your computer has registered itself. These Gateways have been registered to send traps to the IP address of your computer.

  Each Gateway with a ▶ (green triangle) beside it, can respond to SNMP requests.

- **Lower pane**:
  The lower pane is divided into three tabs:
  - **All Traps**:
    The table on the All Traps tab displays all standard traps as well as log messages and CDR records.
  - **Log Messages**:
    The table on the Log Messages tab displays only the log messages. The status of a log message is indicated by color.

⚠	Red indicates an error.
⚠	Yellow indicates a warning.
⚠	Green indicates an alert.

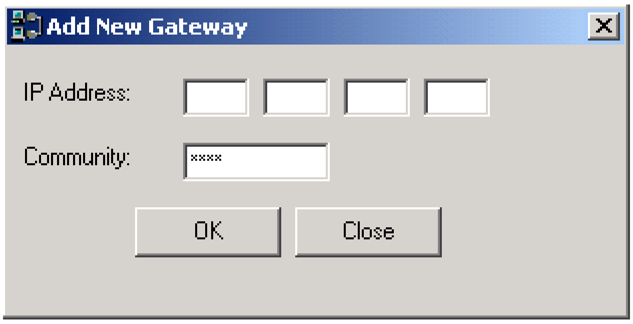
  - **CDR** (Call Detail Reporting):
    The table on the CDR tab displays information that the Gateway has recorded concerning all incoming and outgoing calls.

Sort the entries on each table by clicking the column headings.

Adding a Gateway to the Registered Gateway List

Use this procedure to add a Gateway to the Registered BOScom Gateways list.

1. From the **Configuration** menu, select **Gateways** > **Add New**. The Add New Gateway dialog box appears.



2. Enter the IP address of the new Gateway. Use the tab key to move from one section of the IP address to another.
3. Click **OK**. This registers the computer's IP address on the Gateway.
4. Click **Close**.

Deleting a Gateway

Use this procedure to delete a Gateway.

1. Select the Gateway to be deleted.
2. Right click the selected Gateway.
3. Click **Delete**.
4. A confirmation screen appears. Click **Yes**.

CDR Table Content

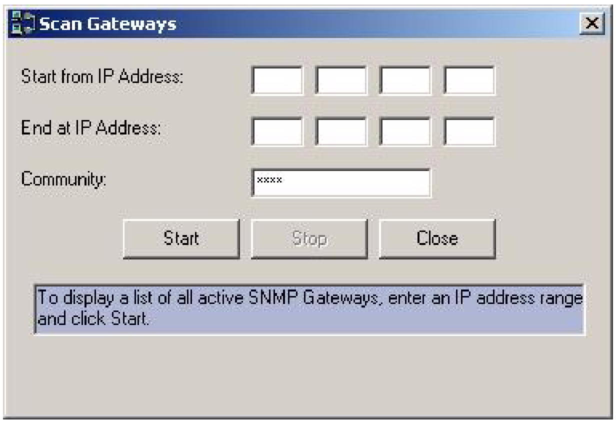
Use this procedure to include or exclude information from the CDR table.

1. From the **Configuration** menu, select **CDR Table Content**.
2. Select the checkboxes for each column of information to be displayed in the CDR table, or click **Select All Fields**. Clear the checkboxes for columns to be excluded.
3. Click **OK**.
4. On the BOSâNOVA SNMP Manager, click the **CDR** tab to view the CDR table.

Scanning the Network for Gateways

Use this procedure to identify operating BOSâNOVA Gateways. The scan excludes all other SNMP agents and identifies only BOSâNOVA Gateways. This simplifies network mapping.

1. From the **Tools** menu, select Scan Gateways. The **Scan Gateways** dialog box opens.



Community: xxxx

To display a list of all active SNMP Gateways, enter an IP address range and click Start.

2. Enter a starting IP address. Use the tab key to move from one section of the IP address to another.
3. Enter an end of range IP address. The maximum scanning range is 63.
4. The Community string is normally entered automatically. If the field is blank, enter **1234**, which is the BOScom Community string. This Community string permits monitoring only.

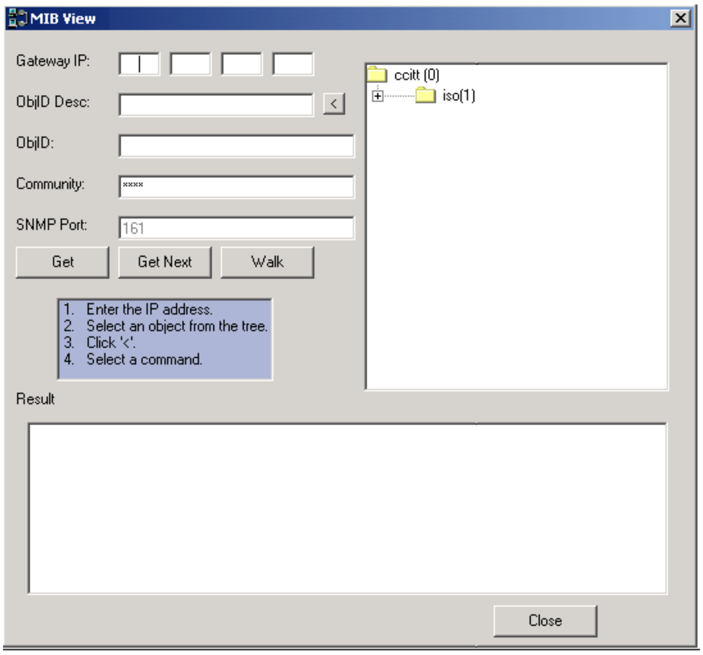
A Community string is the password that is needed to access an SNMP agent. The SNMP Community string is used by the device as a password to give the user clearance to read or write the information requested. If you don't have the correct community name, you cannot retrieve any data (get) or make any changes (sets). This includes attempts to browse the MIB.

5. Click **Start**. A list appears of all operating Gateways within the range specified.
6. To add these Gateways to the Registered BOScom Gateways list:
   - To add one Gateway, select a specific Gateway and click **Add to List**.
   - To add all of the Gateways click **Select All** and click **Add to List**.
7. If necessary, repeat steps 2 to 6 for other ranges of IP addresses.
8. Click **Close**.

Viewing MIBs

Use this procedure to obtain information about the MIB.

1. From the **Tools** menu, select **MIB View**. The MIB View dialog box appears.



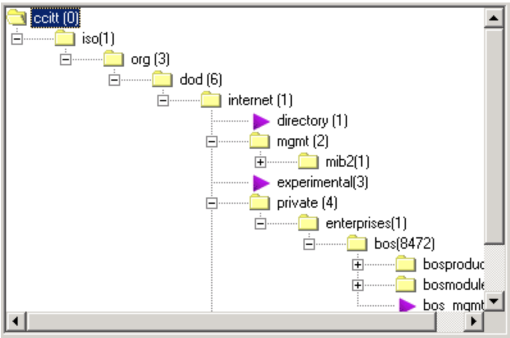
Community: ****

SNMP Port: 161

1. Enter the IP address.
2. Select an object from the tree.
3. Click '<'.
4. Select a command.

2. Enter an IP address. Use the tab key to move from one section of the IP address to another.

3. In the right pane, expand the Control, Command and Intelligence Technical Test (ccitt) tree. You can open the tree and select the any branch or leaf to view agent information.



4. Select a branch or leaf from the MIB Registered Tree. The MIB tree is a predetermined set of variables that is loaded into the BOScom SNMP Manager. The values of these variables is retrieved from the managed object when the information is requested by the SNMP Manager using a GET command.

5. Click <.

6. Choose a Command:

   - **Get**:
     This command requests, from the managed object, then displays the value of the object (node) specified in the MIB tree.

   - **Get Next**:
     This command requests, from the managed object, then displays the value of the next object (node) specified in the MIB tree.

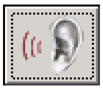
   - **Walk**:
     This command requests, from the managed object, then displays the value of all objects specified in a branch of the MIB tree.

A branch must be selected before the ***Walk*** *command is chosen.*

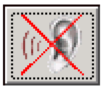
7. Click **Close**.

Listening for Traps

The ear button in the upper right of the SNMP Manager main screen is a toggle button. Use it to turn on and off the listening mode.



informs the user that the SNMP Manager is ***not*** listening for traps. When this button is clicked, the SNMP Manager will start listening for traps.



informs the user that the SNMP Manager ***is*** listening for traps. When when this button is clicked, the SNMP Manager will stop listening for traps.

Alternately, from the SNMP menu on the main screen, select **Listen for Traps**. If selected, there will be a check mark beside it.

Clearing the Traps Log

To erase all the information in the traps log, from the SNMP menu on the main screen, select **Clear Traps Log**.

The log files are backed up in the SNMP Manager’s backup directory.

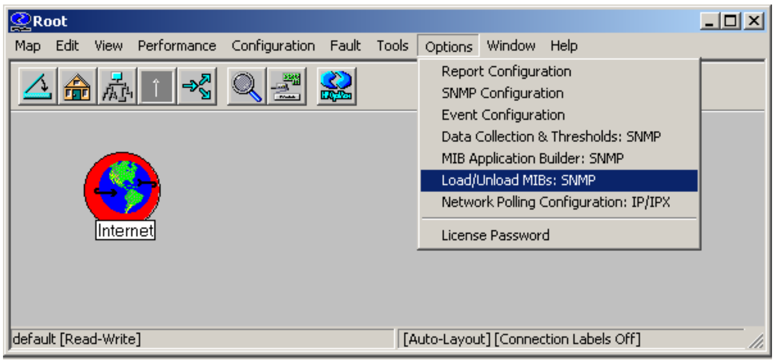
HP OpenView

HP OpenView is a popular family of products that Hewlett Packard produces for network and systems management. The following procedure explains how to use HP OpenView in conjunction with BOSâNOVA IP Telephony Gateways.

Importing MIBS into HP OpenView

To import BOScom private MIBs into the HP OpenView SNMP Manager:

1. Place the BOScom IP Telephony CD-ROM in the computer's CD-ROM drive.
2. Click the Windows **Start** button.
3. Select **Programs > HP OpenView manager**.
4. Select **Network Node Manager** from the HP OpenView program group. The **Roots** screen opens.
5. From the **Options** menu, open **Options > Load / Unload MIBs : SNMP**.



The Load/Unload MIBs:SNMP dialog box is displayed.

6. Click **Load**. The **"**Load/Unload MIBs:SNMP / Load MIB from File" dialog box appears.
7. Browse to the BOScom CD-ROM.
8. Open the **SNMP** folder.
9. Open the **MIBs** folder.
10. Open the **BOScom** folder.

11. Each of the following files is located in the BOScom folder. Select each file, one at a time, in the order listed, and click **Open**.

Import the MIBs in the exact order listed below. Deviating from the order will result in malfunctions.

   a. BOS-SMI.txt

   b. BOS-PRODUCTS-MIB.txt

   c. BOS-voip.txt

   d. BOS-MEDIAGATEWAY-MIB.txt

   e. BOS-MONITORING-MSG.txt

   f. BOS-GATEWAY-CHANNELS.txt

   g. BOS-TRAPS-FILTER.txt

12. Click 📁 to navigate up one level.

13. Open the **UCD** folder.

14. Each of the following files is located in the UCD folder. Select each file, one at a time, in the order listed, and click **Open**.

Import the MIBs in the exact order listed below. Deviating from the order will result in malfunctions.

   a. UCD-SNMP-MIB.txt

   b. UCD-IPFWACC-MIB.txt

   c. UCD-DLMOD-MIB.txt

   d. UCD-DISKIO-MIB.txt

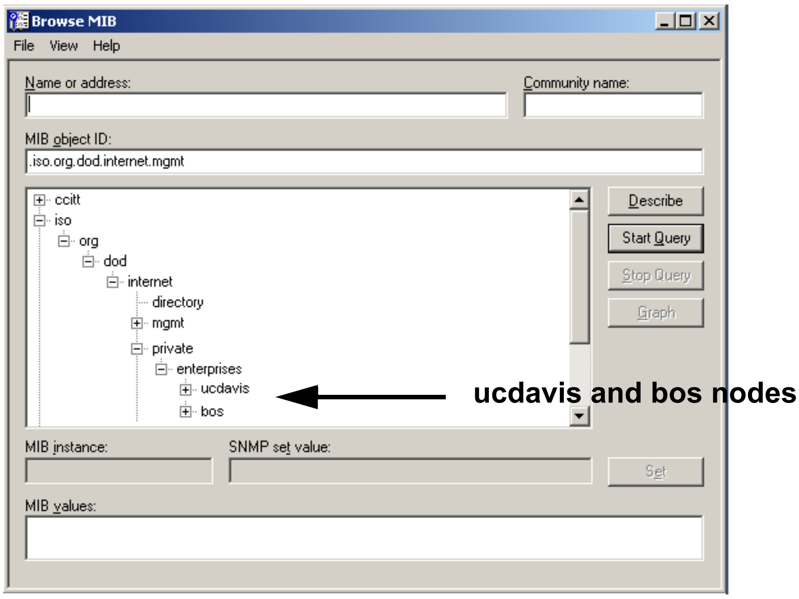
15. Click **Close**. HP OpenView returns to the **Root** screen.

16. After loading the BOScom MIBs, ensure that they appear in the MIB Registration tree. The procedure for checking the MIB Registration tree follows.

Checking the MIB Registration Tree

The procedure is a continuation of the preceding procedure.

1. Select **SNMP MIB Browser** from the **Tools** menu of the HP OpenView **Root** screen. The Browse MIB screen opens.
2. Expand the branches of the tree to **internet** > **private** > **enterprise**.
3. Check that **ucdavis** and **bos** are nodes on the tree.



Checking Data Values of BOScom Private MIBs

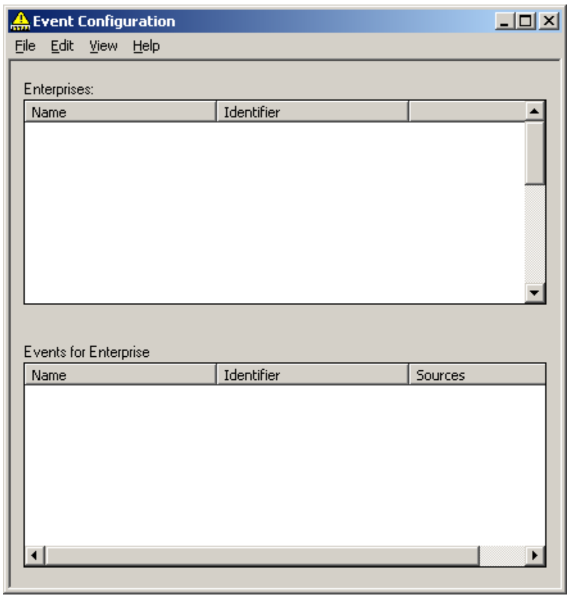
To check the data values of BOScom Private MIBs:

1. Enter the IP address of a Gateway in the **Name or address** field in the Browse MIB screen.
2. Enter the Community Name in the **Community name** field. The default BOScom community name is 1234.
3. Select a node of the tree.
4. Click **Start Query**.

Setting Traps and Alarms in HP OpenView

To set traps and alarms:

1. Click the Windows **Start** button.
2. Select **Programs > HP OpenView manager**.
3. Select **Network Node Manager** from the HP OpenView program group. The **Roots** screen opens.
4. From the **Fault** menu, select **Alarm.** The **Alarms Categories** and the **Alarms Browser** screens open.
5. From the **Options** menu, select **Event Configuration**. The **Event Configuration** screen opens.
6. From the upper pane of the Event Configuration screen, select an enterprise (the MIB whose values you want to trap).



7. To add or modify a trap:
   - To add a new trap:
     i. From the Event Configuration screen's **Edit** menu, select **Event > New**:
     ii. Fill in the fields as required by the **New Events Wizard**.
   - To modify an existing trap:
     i. Select an enterprise from the top pane.
     ii. Select an event from the bottom pane.
     iii. From the Event Configuration screen's **Edit** menu, select **Event > Modify**. The **Modify Events** screen opens.

iv. Open each tab and modify the fields. If you want to see a message of the event, open the **Event Message** tab and under **Actions** choose the **Log and Display** button.

v. Modify or fill in the rest of the fields.

8. Click **Apply**.
9. Click **OK**.
10. Select **File > Save**.

SECTION 22:
CALL DETAIL RECORDS

BOSâNOVA Gateways include a Call Detail Records (CDR) module. The CDR module keeps track of information pertaining to incoming and outgoing calls.

This section contains:

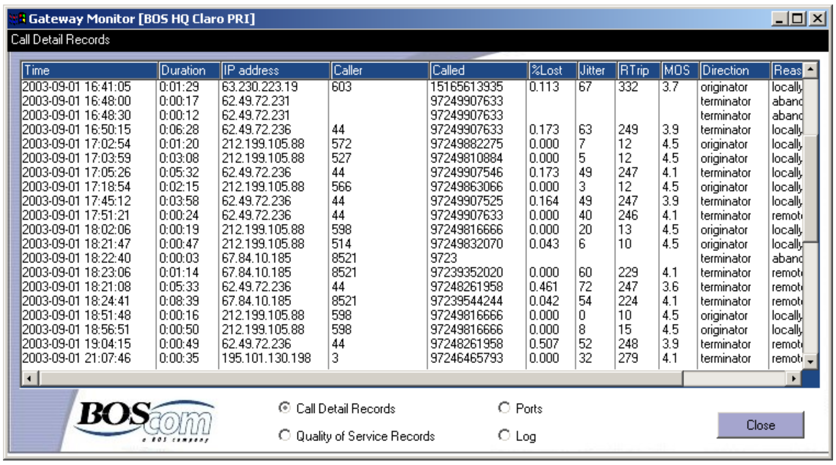
- An overview of the CDR components, see p. 346
- An explanation how CDR works, see p. 347
- Procedures regarding the installation of software components, see p. 348
- CDR file formats and structure, see p. 352

OVERVIEW

Call Detail Records (CDR) is a program that keeps track of a Gateway's incoming and outgoing calls. The CDR module is made up of some or all of the following software components.

CDR Buffer

Call Detail Records (CDR) are stored in a buffer on the Gateway. The CDR buffer contains extensive information about the calls that go through the Gateway. A small portion of the most recent information is displayed on the Gateway Monitor's Call Detail Records screen. (For information on the CDR Monitor, see page 267.) A complete list of the categories of information stored in the buffer is found beginning on page 352.



Gateway Monitor [BOS HQ Claro PRI]

Call Detail Records

Time	Duration	IP address	Caller	Called	%Lost	Jitter	RTrip	MOS	Direction	Reas
2003-09-01 16:41:05	0:01:29	63.230.223.19	603	15165613935	0.113	67	332	3.7	originator	locally
2003-09-01 16:48:00	0:00:17	62.49.72.231		97249907633					terminator	aband
2003-09-01 16:48:30	0:00:12	62.49.72.231		97249907633					terminator	aband
2003-09-01 16:50:15	0:06:28	62.49.72.236	44	97249907633	0.173	63	249	3.9	terminator	locally
2003-09-01 17:02:54	0:01:20	212.199.105.88	572	97249882275	0.000	7	12	4.5	originator	locally
2003-09-01 17:03:59	0:03:08	212.199.105.88	527	97249810884	0.000	5	12	4.5	originator	locally
2003-09-01 17:05:26	0:05:32	62.49.72.236	44	97249907546	0.173	49	247	4.1	terminator	locally
2003-09-01 17:18:54	0:02:15	212.199.105.88	566	97249863066	0.000	3	12	4.5	originator	locally
2003-09-01 17:45:12	0:03:58	62.49.72.236	44	97249907525	0.164	49	247	3.9	terminator	locally
2003-09-01 17:51:21	0:00:24	62.49.72.236	44	97249907633	0.000	40	246	4.1	terminator	remot
2003-09-01 18:02:06	0:00:19	212.199.105.88	598	97249816666	0.000	20	13	4.5	originator	locally
2003-09-01 18:21:47	0:00:47	212.199.105.88	514	97249832070	0.043	6	10	4.5	originator	locally
2003-09-01 18:22:40	0:00:03	67.84.10.185	8521	9723					terminator	aband
2003-09-01 18:23:06	0:01:14	67.84.10.185	8521	97239352020	0.000	60	229	4.1	terminator	remot
2003-09-01 18:21:08	0:05:33	62.49.72.236	44	97248261958	0.461	72	247	3.6	terminator	remot
2003-09-01 18:24:41	0:08:39	67.84.10.185	8521	97239544244	0.042	54	224	4.1	terminator	remot
2003-09-01 18:51:48	0:00:16	212.199.105.88	598	97249816666	0.000	0	10	4.5	originator	locally
2003-09-01 18:56:51	0:00:50	212.199.105.88	598	97249816666	0.000	8	15	4.5	originator	locally
2003-09-01 19:04:15	0:00:49	62.49.72.236	44	97248261958	0.507	52	248	3.9	terminator	remot
2003-09-01 21:07:46	0:00:35	195.101.130.198	3	97246465793	0.000	32	279	4.1	terminator	remot

● Call Detail Records ○ Ports

○ Quality of Service Records ○ Log

If—in the VoIP Configurator (see *Statistic Servers* on page 64)—CDR sending is enabled and the CDR Server IP address is defined, then at predefined intervals the content of the buffer is sent as a file to the CDR Server. If not, once the buffer is full the oldest information is replaced by the newest.

CDR Server

The **CDR** Server is the computer upon which the following programs are running:

- **The CDR Depository:**
  This is the program that receives the CDR buffer files from the Gateways. The Depository stores the information contained in the buffer files for future use.
- **The SSH software:**
  The **SSH** (Secure **SH**ell) software ensures a secure, encrypted transfer of information and provides secure, remote logon for Windows and Linux clients and servers. The Gateways are SSH clients.

- **The CDR Parser:**
  The CDR Parser monitors the hard drive in the CDR Server. When a new CDR buffer file arrives in the hard drive, the CDR Parser takes the new file, parses it, and inserts the data into the MS SQL Server.

  The information is put into a file containing header information and data records. General information including the name and serial number of the Gateway sending the buffer, a unique ID number generated by the MS SQL Server, an end number (record ID), and a start number (record ID) for the records in this trace file is in the header. The rest of the file contains information regarding the call records of calls through the specified Gateway.
- **SQL Server:**
  A database is required to collect and arrange the information, and make the information available to a report generator. The MSD developer Edition of Microsoft SQL Server database is one example.

How CDR Works—A Summary

All of the Gateways on the IP Telephony network must enable CDR sending and have the IP address of a CDR Server entered in the VoIP configurator. See Statistic Servers on page 64.

Each Gateway gathers information about calls in its CDR buffer. When the CDR buffer reaches a predefined limit (see “Configuring CDR and QSR buffers” on page 328), or at least once a day, the CDR buffer file is sent, via SSH, to the CDR Depository running on the CDR Server.

The information is then parsed and inserted into an SQL database. A CDR report generator then accesses the SQL database and retrieves the information necessary to generate the requested tables and graphs. These graphs and tables can be used to track calls, trace initiation and destination numbers, calculate call duration, check call traffic through the network, etc.

Since each Gateway transmits its buffer, there are 2 records for each call:

- One record from the originating Gateway which initiated the call
- One record from the terminating Gateway which received the call

All outgoing calls show up in the Originator list and all incoming calls show up in the Terminator list.

Only calls going through a Gateway are counted. Therefore, calls that bypass a Gateway (for example, PSTN to PBX) are not counted unless the Gateway is a Claro. Calls that go through only one Gateway (e.g. from a PBX through a Claro to the PSTN) will generate only one record.

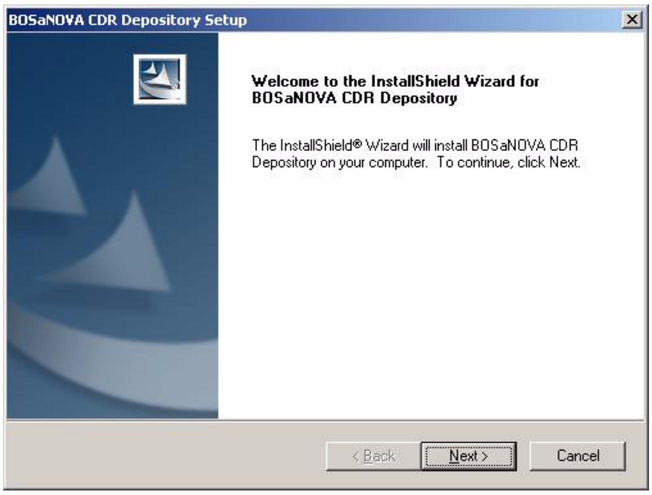
CDR COMPONENTS

Some of the CDR components are installed from the BOSâNOVA IP Telephony Gateway CD-ROM Welcome screen. Others must be obtained separately.

Installing the CDR Depository and SSH Software

The CDR Depository and SSH software are installed during a single setup procedure and are available from the BOSâNOVA IP Telephony Gateway CD-ROM.

1. Insert the BOSâNOVA IP Telephony Gateway CD-ROM into the CD-ROM drive of the computer that will serve as the CDR Server. The CD-ROM Welcome screen is displayed.
2. Select **Install the BOSâNOVA CDR Depository**. The CDR Depository Setup Welcome screen is displayed.



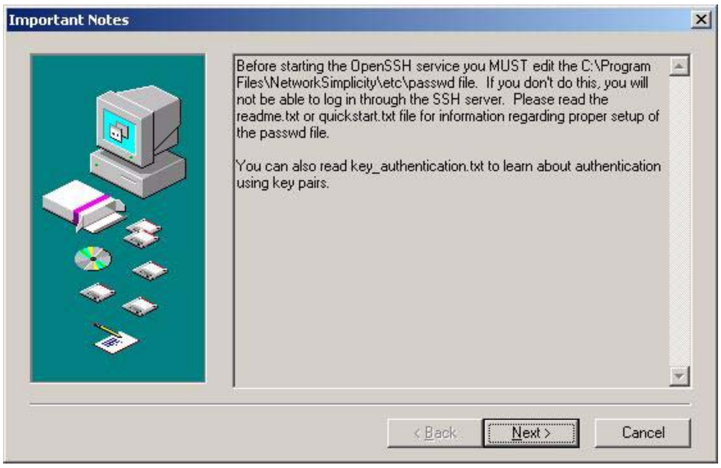
BOSaNOVA CDR Depository Setup

Welcome to the InstallShield Wizard for BOSaNOVA CDR Depository

The InstallShield® Wizard will install BOSaNOVA CDR Depository on your computer. To continue, click Next.

3. Click **Next**. The Choose Destination screen is displayed.
4. Click **Next** or browse to select a different destination. The Start Copying Files screen is displayed.
5. Click **Next**. The OpenSSH on Windows (v.3.2.3-1) splash screen is displayed.
6. Click the center of the screen. The OpenSSH on Windows (v.3.2.3-1) Setup Welcome screen is displayed.
7. Click **Next**. The Choose Destination screen is displayed.
8. Click **Next** or browse to select a different destination. The Select Components screen is displayed.
9. Ensure that the **Server** checkbox is selected. Clear the Client checkbox.

10. Click **Next**. Setup begins. When finished, a DOS type window opens indicating that the key is being created. When finished, the following message box appears:



Before starting the OpenSSH service you MUST edit the C:\Program Files\NetworkSimplicity\etc\passwd file. If you don't do this, you will not be able to log in through the SSH server. Please read the readme.txt or quickstart.txt file for information regarding proper setup of the passwd file.

You can also read key_authentication.txt to learn about authentication using key pairs.

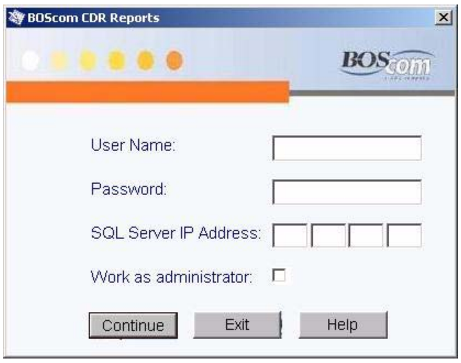
11. Note the information and click **Next**. Setup continues.
12. Click **Close**. Setup continues.
13. Click **Finish**.

The CDR Parser

The CDR Parser must be acquired separately. Options for acquiring a CDR Parser include:

- Using the description of fields contained in a BOSâNOVA CDR buffer file, independently develop a CDR Parser. See *CDR File Formats and Structures* beginning on page 352.
- Order the BOSâNOVA CDR Parser described in the following section (see p. 350). The BOSâNOVA CDR Parser includes:
  - The file **`BSCDRAPI.DLL`** that monitors the hard drive in the CDR Server and identifies the arrival of a new CDR buffer file.
  - An application that, after a new CDR buffer file arrives, parses the new file and inserts the data into the MS SQL database.
  - Scripts for creating the MS SQL database.
- To save the CDRs in a different database—for example, Oracle, Sybase, etc.—order the file **`BSCDRAPI.DLL`** which monitors the hard drive in the CDR and identifies the arrival of a new CDR buffer file. It can then be integrated with other databases and, subsequently, with most third-party billing software.

- Order the BOScom CDR Reports Generator. The BOScom CDR Reports Generator is an SQL based query processor that displays the results of the query in Microsoft Excel. To take full advantage of the CDR Reports Generator you must be familiar with Excel.



The BOScom CDR Reports Generator can be used only with the BOSâNOVA CDR Parser and the database fields supported by the MS SQL Server.

The BOSâNOVA CDR Parser

The following description is intended for programmers using the CDR Parser.

The BOSâNOVA CDR Parser includes the BSCDR.DLL Application Programing Interface (API). The BSCDR.DLL API may be integrated to a user CDR handling application and allows very easy reading of CDR files. The module monitors a specified folder on the hard disk and when a new CDR or QSR file appears, it copies the file's content to a memory buffer, calls the application call-back function, and removes the file.

Here is a list of the API functions.

- **BSCDRDLL_API BOOL DLLInit (BS_RECORDS_INIT *pBsInit);**
  The application calls this function to initialize the DLL.
  The BS_RECORDS_INIT is the structure that contains pointers to two callback functions. The prototype of the function is as follows.

  BOOL CdrDllCallBackProc (CDRDLL_CONTROL control, void *pvParam);
  If the callback function returns FALSE then the file will be automatically copied to the Error directory.

- **BSCDRDLL_API BOOL DLLClose (void);**
  The application calls this function when finished.

- **BSCDRDLL_API BOOL StartCDRFilesWait (char * pCDRPath, BOOL bBackup);**
  The application calls this function to start the waiting process for new CDR files.
  - **pCDRPath**
    pointer to the zero-terminated string that contains the path to the directory where the new CDR files will appear.
  - **bBackup**
    if it is set TRUE, then BsCdrApi.Dll will automatically copy the parsed file to the Backup directory.
- **BSCDRDLL_API BOOL StartQSRFilesWait (char * pQSRPath, BOOL bBackup);**
  The application calls this function to start the waiting process for new CDR files.
  - **pQSRPath**
    pointer to the zero-terminated string that contains the path to the directory where the new QSR files will appear.
  - **bBackup**
    if it is set TRUE, then BsCdrApi.Dll will automatically copy the parsed files to the Backup directory.
- **BSCDRDLL_API void StopCDRFilesWait ();**
  The application calls this function to stop the waiting process for new CDR files.
- **BSCDRDLL_API void StopQSRFilesWait ();**
  The application calls this function to stop the waiting process for new QSR files.

The function prototypes described above are listed in the **bscdrapi.h** file.

The MS SQL Server

The SQL Server is the Microsoft version of an SQL database. Although it can be installed on any computer on the network, having the SSH software, the CDR Parser, and the MS SQL Server on the same computer will enhance the speed of these programs.

CDR FILE FORMATS AND STRUCTURES

The CDR file name structure is as follows:

CDR_<Gateway Serial Number>_<First record ID>_<Last record ID>

For example:

CDR_820D_18852_18860

Where:

- 820D is the serial number of the Gateway sending the file
- 18852 is Record Identification Number of the first CDR in the file
- 18860 is Record Identification Number of the last CDR in the file

The CDR file consists of:

- the header record
- multiple CDRs

Structure of the CDR File Header

The fields in the header and in the CDRs are separated by a semicolon (;).

The header structure is as follows:

1.02;CDR;820D;212.117.156.6;Claro PRI BOS-IL;18852;18860;1036;

Table 60: Structure of CDR File Header

Field Description	Maximum Length	Format
Record version version: 1.0.0.3	4	n.nn
Record type	3	ccc
Gateway Serial Number	4	hhhh
IP address of the Gateway sending the file	15	nnn.nnn.nnn.nnn
Name of the Gateway sending the file	32	
First Record ID # in the file	10	n.......n
Last Record ID # in the file	10	n.......n
The file length (bytes)	10	n.......n

Structure of the CDR Buffer File

These table shows the information gathered from the CDR buffer file after it is parsed and inserted into the MS SQL Server.

Table 61: Structure of CDR Buffer File: Records Which Always Appear

#	Field Description	Format	Max Length	Description
1	RecordID			The ID number of the first record sent in this file
2	Call Start day and time	yyyy-mm-dd hh:mm:ss	19	Starting date and time of the call measured in the GW that created the record
3.	Call End day and time	yyyy-mm-dd hh:mm:ss	19	End date and time of the call measured in the GW that created the record
4	Call Originator IP	nnn.nnn.nnn.nnn	15	IP Address of the originating GW or other IP device
5	Originator port	nn	2	The port on the call origination Gateway
6	Terminator IP	nnn.nnn.nnn.nnn	15	IP Address of the terminating GW
7	Terminator port	nn	2	The port on the call termination Gateway
8	Remote Party Serial Number	String	4	Serial Number of the remote call party (originator or terminator depending on call direction)
9.	User ID	Free	20	For future use (e.g., pre-paid service etc.)
10	Call Originator phone number (E.164)	n...n	30	Call originator # in E.164 format.

Table 61: Structure of CDR Buffer File: Records Which Always Appear

11	Called phone number (E.164)	Number	30	Called # in E.164 format For the origination Gateway it is the number that is sent to IP or to PSTN interface of Claro Gateway.For the termination Gateway it is the number that is received from IP.
12	Dialed DTMF #s	n...n	30	Dialed DTMFs. For the origination Gateway it is number that was dialed by the user. For the termination Gateway it is number that was dialed by the Gateway to the telephony interface.
13	Call direction	n	1	1 –In, 2 – Out
14	Call type	n	1	1(voice), 2(fax), 3(modem)
15	Call Originator	n	1	1 - IP 2 - PBX 3 - PSTN
16	Call termination type	Enumerated	1	1 - IP 2 - PBX 3 - PSTN
17	Call termination reason	Enumerated	2	1 – Normal locally 2 – Normal remotely 3 – Abandoned (User disconnected the call before it was answered) 4 – Busy 5 – Not resolved 6- Other
18	Call Code	nn	2	For future use

Table 62: Structure of CDR Buffer File:
Records Which Appear Only After a Call is Answered

1	Call ID	Characters	50	Unique call identifier
19	Modem backup	Enumerated	1	0 – was not active 1 – was active
20	Codec type	Enumerated	1	0 – G.723 1 – G.711 a-law 2 – G.711 u-law 3 – G.729 4 – NetCoder
21	JB handling	Enumerated	1	0 – disabled 1 – enabled
22	Start JB size	Number	3	Measurement in milliseconds of the jitter buffer start size
23	Average JB size	Number	4	Measurement in milliseconds of the average jitter buffer used by the Gateway.
24	JB size standard deviation	Float	7	Measurement in milliseconds of the standard deviation of the jitter buffer
25	JB packets loss	Number	2	Integral estimation
26	% of voice packets	Float	5	% of voice packets received
27	% of lost packets	Float	5	% of lost packets
28	Average Call Quality	Float	4	Average Mean Opinion Score
29	Sigma Call Quality	Float	4	Mean Opinion Score standard deviation
30	Average Round-Trip Delay	Number	4	Calculated for IP calls only and during the call. Field is not available if 3rd party gateway participates.
31	Sigma of Round-Trip delay	nnnn.nn	7	Standard deviation calculated for IP calls only and during the call. Field is not available if 3rd party gateway participates.

Description of CDR Fields as Presented in MS SQL

Table 63: CDR Fields in MS SQL

#	Field	Format	Presen-tation	Max length	Appear in Java	Description
1	CdrID	Number				Unique ID created by MS SQL.
2	GtwName	string		35		Name of origination gateway
3	GtwSN	string	nnnn	4		Serial number of origination gateway
4	CDRVersion	Number				
5	RecordID					
6	CallStartTime	yyyy-mm-dd hh:mm:ss		19	V	Starting date and time of the call measured in the local GW.
7	CallEndTime	yyyy-mm-dd hh:mm:ss		19	V - duration	End date and time of the call measured in the local GW.
8	OrigIP	nnn.nnn.nnn.nnn	Numeric + dot	15	V - if call direction is 1	IP Address of the originating GW or other IP device
9	OrigLine	nn		2		
10	TermIP	nnn.nnn.nnn.nnn	Numeric + dot	15	V- if call direction is 2	IP Address of the terminating GW
11	TermLine	nn		2		
12	RmtSN	String	Nnnn	4		Serial Number of the remote call party (originator or terminator depending on call direction)
13	UserID	Free	Printable ASCII string	20 / 15-from ver.1.04		PIN code that was entered during authentication process.
14	CallingE164	Number	Numeric	30	V	Call originator # in E.164 format.

Table 63: CDR Fields in MS SQL

#	Field	Format	Presen-tation	Max length	Appear in Java	Description
15	CalledE164	Number	Numeric	30	V	Called # in E.164 format. For the origination gateway it is the number that is sent to IP or to PSTN interface of Claro gateway. For the termination gateway it is the number that is received from IP.
16	DialedDTMF	Number, #, *	Numeric + special	30	V	Called # in E.164 format. For the origination gateway it is number that was dialed by the user. For the termination gateway it is number that was dialed by the gateway to the telephony interface.
16	CallDirection	Enumerated	Numeric	1	V	1 – Terminator 2 – Originator
18	CallType	Enumerated	Numeric	1		1(voice), 2(fax), 3(modem)
19	CallOrigType	Enumerated	Numeric	1		1- IP 2- PBX 3- PSTN
20	CallTermType	Enumerated	Numeric	1		1- IP 2- PBX 3- PSTN
21	CallTermReason	Enumerated	Numeric	2	V	1 – Normal locally 2 – Normal remotely 3 – Abandoned (User disconnected the call before it was answered) 4 – Busy 5 – Not resolved 6- Other 10 – Authentication failed

Table 63: CDR Fields in MS SQL

#	Field	Format	Presen-tation	Max length	Appear in Java	Description
22	CallCode	Set of flags	Numeric	2		Until ver. 1.04 was not used. Ver.1.04: · lowest bit=0- H.323 call lowest bit=1 – SIP call
23	ModemBackup-Mode	Enumerated	Numeric	1		0 – was not active; 1 – was active
24	CodecType	Enumerated		1	V	0 – g.723 1 – g.711 a-law 2 – g.711 u-law 3 – g.729 4 – NetCoder
25	JBHandling	Enumerated		1		0 – disabled 1 – enabled
26	StartJBSize	Number	Numeric	3		In ms
27	AverageJBSize	Number		4	V	In ms
28	JBSizeSD	Float	Nnnn.nn	7		In ms
29	JBPacketsLoss	Number	nn	2		Integral estimation
30	VoicePackets	Float	nn.nn	5		% of voice packets received
31	LostPackets	Float	nn.nn	5	V	% of lost packets
32	Average VoiceQuality	Float	n.nn	4	V	MOS.
33	VoiceQualitySD	Float	n.nn	4		MOS SD.
34	AverageRTDelay	Number	nnnn	4	V	RTD (ms).
35	RTDelaySD	Float	nnnn.nn	7		RTD SD.
36	CallID	16 bytes (50 from v.1.04)		16 / 50-from v.1.04		VoIP Call ID

IP Telephony...
Clear and Simple

SECTION 23:
WEB SUPPORT and FAQs

This section introduces the BOScom VoIP Web Support site and includes answers to some frequently asked questions.

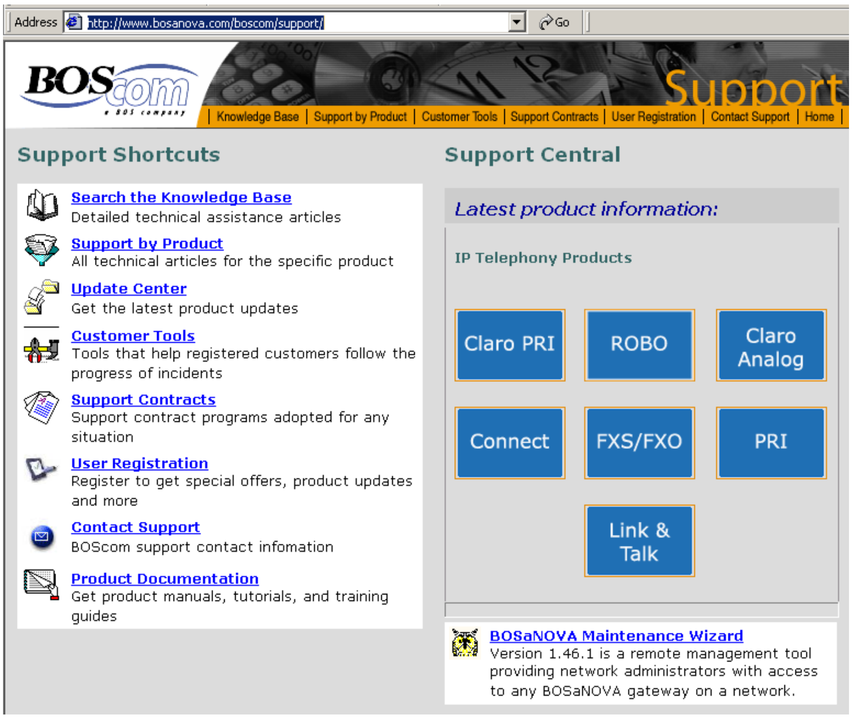
USING THE BOScom VoIP WEB SITE

To access the BOScom VoIP Web site:

1. Open a web browser.
2. In the address field, enter:

   `http://www.bosanova.com/boscom/support/`

   and click **Go**. The Support site is displayed.


Address http://www.bosanova.com/boscom/support/
Go
BOScom a BOS company
Support
Knowledge Base | Support by Product | Customer Tools | Support Contracts | User Registration | Contact Support | Home

Support Shortcuts

Search the Knowledge Base
Detailed technical assistance articles

Support by Product
All technical articles for the specific product

Update Center
Get the latest product updates

Customer Tools
Tools that help registered customers follow the progress of incidents

Support Contracts
Support contract programs adopted for any situation

User Registration
Register to get special offers, product updates and more

Contact Support
BOScom support contact infomation

Product Documentation
Get product manuals, tutorials, and training guides

Support Central

Latest product information:

IP Telephony Products

BOSaNOVA Maintenance Wizard
Version 1.46.1 is a remote management tool providing network administrators with access to any BOSaNOVA gateway on a network.

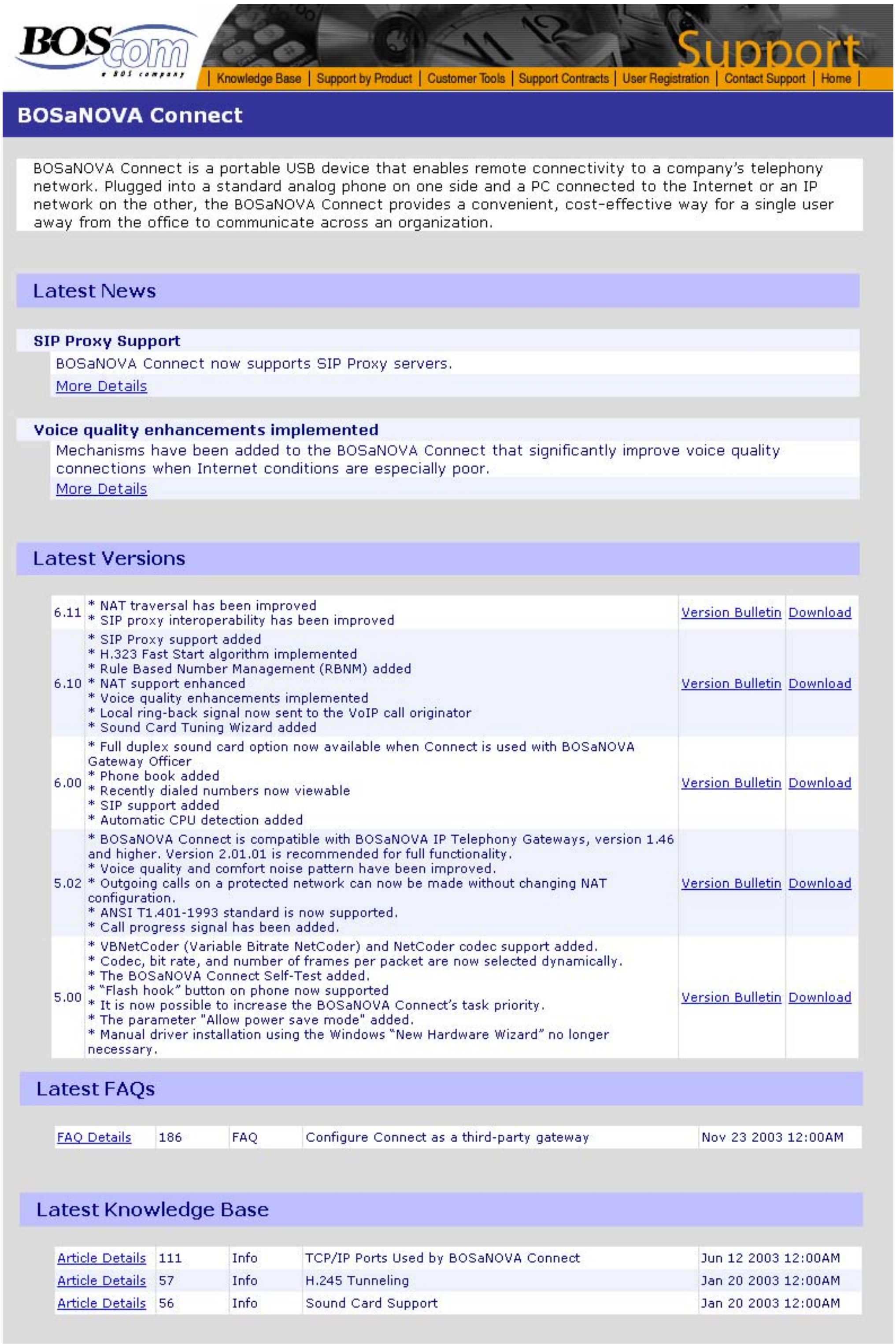
3. The site is divided into:

   - **Support Shortcuts**
     These links connect to pages described by the prompts provided:

     - Search the Knowledge Base:
       Search engines for finding information based on the search parameters. Also includes a list of recently added articles.
     - Support by Product:
       Opens a list of all Knowledge Base technical articles for the selected product.
     - Update Center:
       Get the latest product updates. This option is the same as selecting a product from Support Central except that more products are listed here.

  - Customer Tools:
    Tools that help registered customers follow the progress of incidents.
  - Support Contracts:
    Support contract programs adopted for any situation. (This link is under construction.)
  - User Registration:
    Register to get special offers, product updates and more. (This link is under construction.)
  - Contact Support:
    BOScom support contact information and web form.
  - Product Documentation:
    List of downloadable product manuals, tutorials, and training guides.
- **Support Central**
  As illustrated by the example on the next page, Support Central links connect to web-pages containing the product's:
  - Latest News
  - Latest Versions
  - Latest FAQs
  - Latest Knowledge Base

Sample Support Central Page


BOScom
a BOS company
Support
| Knowledge Base | Support by Product | Customer Tools | Support Contracts | User Registration | Contact Support | Home |

BOSaNOVA Connect

BOSaNOVA Connect is a portable USB device that enables remote connectivity to a company's telephony network. Plugged into a standard analog phone on one side and a PC connected to the Internet or an IP network on the other, the BOSaNOVA Connect provides a convenient, cost-effective way for a single user away from the office to communicate across an organization.

Latest News

SIP Proxy Support

BOSaNOVA Connect now supports SIP Proxy servers.

More Details

Voice quality enhancements implemented

Mechanisms have been added to the BOSaNOVA Connect that significantly improve voice quality connections when Internet conditions are especially poor.

More Details

Latest Versions

6.11	* NAT traversal has been improved * SIP proxy interoperability has been improved	Version Bulletin	Download
6.10	* SIP Proxy support added * H.323 Fast Start algorithm implemented * Rule Based Number Management (RBNM) added * NAT support enhanced * Voice quality enhancements implemented * Local ring-back signal now sent to the VoIP call originator * Sound Card Tuning Wizard added	Version Bulletin	Download
6.00	* Full duplex sound card option now available when Connect is used with BOSaNOVA Gateway Officer * Phone book added * Recently dialed numbers now viewable * SIP support added * Automatic CPU detection added	Version Bulletin	Download
5.02	* BOSaNOVA Connect is compatible with BOSaNOVA IP Telephony Gateways, version 1.46 and higher. Version 2.01.01 is recommended for full functionality. * Voice quality and comfort noise pattern have been improved. * Outgoing calls on a protected network can now be made without changing NAT configuration. * ANSI T1.401-1993 standard is now supported. * Call progress signal has been added.	Version Bulletin	Download
5.00	* VBNetCoder (Variable Bitrate NetCoder) and NetCoder codec support added. * Codec, bit rate, and number of frames per packet are now selected dynamically. * The BOSaNOVA Connect Self-Test added. * "Flash hook" button on phone now supported * It is now possible to increase the BOSaNOVA Connect's task priority. * The parameter "Allow power save mode" added. * Manual driver installation using the Windows "New Hardware Wizard" no longer necessary.	Version Bulletin	Download

Latest FAQs

FAQ Details	186	FAQ	Configure Connect as a third-party gateway	Nov 23 2003 12:00AM

Latest Knowledge Base

Article Details	111	Info	TCP/IP Ports Used by BOSaNOVA Connect	Jun 12 2003 12:00AM
Article Details	57	Info	H.245 Tunneling	Jan 20 2003 12:00AM
Article Details	56	Info	Sound Card Support	Jan 20 2003 12:00AM

FREQUENTLY ASKED QUESTIONS

Following are responses to frequently asked questions concerning BOSâNOVA Gateways. Answers to some of these questions already appear elsewhere in this document. In those cases, cross-references are provided.

1. Which ports do the CDR Server and the Q-CDR use?

   Port usage information is available from Table 45 on page 232. The BOScom CDR module uses the standard SSH port, which is port number 22. However, the port assignment for the Q-CDR is configurable.

2. How is Maximum Call Duration configured?

   As of version 2.13, Maximum Call Duration can be set using either the Command Line Configurator or using the Maintenance Wizard. For the Maintenance Wizard procedure, see “Setting Maximum Call Duration” on page 318.

3. Which encryption standard do the Gateways employ?

   We use the Advanced Encryption Standard (AES). See “Encryption” on page 41.

4. How to use the special signal to indicate the Gateway path?

   See “BOS Tones” on page 59.

5. How do you reset the factory default parameters?

   a. From the Configurator main menu, select **VoIP Configuration**.

   b. Click **Defaults**. The Gateway’s IP settings will ***not*** be reset.

6. Can Gateways tag packets so that traffic shaping devices can prioritize accordingly?

   Tagging packets assigns the VoIP packets a higher ***priority*** than other packets delivered on the same network. Therefore, this feature is called Voice Packet Priority.

   Gateways can send tagged packets according to either DiffServ (RFC-2597) or ToS (RFC7-791). For the procedure and recommended settings, see “Voice Packet Priority—Tagging Packets” on page 62.

7. Why is Force Overlap required for PRI and Claro PRI Gateways? How does it work?

   Normally, the BOSâNOVA PRI Gateway automatically distinguishes between en bloc and overlap signaling. However, in some circumstances, the Gateway should be forced to use overlap signaling. See “Forced Overlap Mode” on page 159.

8. What can we say about BOSâNOVA Gateway interoperability?

   Our Gateways work according to both H.323, version 4 and SIP protocol and use standard ports when they communicate with third-party gateways. BOSâNOVA Gateways use some additional ports when they communicate with other BOSâNOVA Gateways—for example, communication with the Officer gateway, continuous QoS tests, etc. Port usage information is available from Table 45 on page 232. In addition, you can refer to the "BOSâNOVA Gateway Ports Assignment" document which also includes detailed port usage information.

   Interoperability with third-party gateways is always an issue. In the vast majority of the cases, if the user defines G.723 codec as the default and disables H.245 tunneling then the BOSâNOVA Gateway will work with third-party gateways. If that fails, we usually adjust some parameters on both gateways in order to gain the best voice quality and performance.

9. Why doesn't the Java 1.1. applet load if SUN's Java 1.3.x or 1.4.x Plug-in is installed over Windows?

   When a Java 1.3.x or 1.4.x Plug-in is installed on Windows, before running a Java 1.1 applet, configure the Plug-in as follows:

   a. Open the Control Panel.

   b. Double-click **Java Plug-in**. The Java Plug-in Control Panel opens.

   c. Select the **Browser** tab.

   d. Clear the checkbox beside the browser you want to use with the Java 1.1 applet.

   e. Click **Apply**.

It is possible for there to be more than one SUN Java Plug-in installed on the same PC. Configure all of them to run the Java 1.1 applet.

10. How do you configure NAT pass-through?

    For a complete discussion of Network Address Translation, including procedures for configuring NAT pass-through, see the chapter entitled "Network Address Translation" which begins on page 226.

11. What is Least Cost Routing via the PSTN and can our Claro Gateways support Least Cost Routing?

LCR via the PSTN is different than LCR between Gateways. Documentation on configuring LCR per Gateway begins on page 166.

Some companies use one carrier for local calls, another carrier for Subscribers Trunk Dialing (STD), and yet another for International Subscriber Dialing (ISD). The routing is usually performed by the PBX, often by modifying the number.

Our Claro Gateways can support this kind of LCR. Sometimes, it is necessary to configure Rule Based Number Management (see page 174). Following is an example of LCR enabled using RBNM:

> All company employees dial 00 for international calls. However, we want to route calls to the UK (44) through 012, calls to France (33) through 013, and all other calls through 014. To accomplish this, we enter three **Gateway to PBX** rules as follows:
>
> - s0044a01244ct
> - s0033a01322ct
> - s00a014ct

12. Sometimes, when third-party gateways are used, there is no voice in either one or both directions. When that occurs, try the following:
    - If the partner gateway is a Quintum, ensure that the same codec type is defined on both gateways.
    - If the G.723 codec is used, then make sure that the G.723 codec on the third-party gateway is configured for 6.3 kbps.
    - If you have a BOSâNOVA Gateway with software earlier than version 2.13.xx:
        - If the G.711 codec is used, then make sure that the third-party gateway sends RTP with 160 bytes of payload (20 ms frames).
        - Check if the third-party gateway sends RTP with a payload number of frames less or equal to that defined in the BOSâNOVA Gateway configuration. To review the BOSâNOVA Gateway definition, see “Max (maximum) Frames” on page 45.
    - If the gateway is located behind a firewall or NAT system:
        - Ensure that the correct ports are open in the firewall.
        - If the third-party gateway equipment supports *symmetric RTP*, enable it.

13. What are Call Detail Records (CDRs) and why are they useful?

Call Detail Records (CDR) contain extensive information about the calls that go through the Gateway. A small portion of the most recent information is displayed on the Gateway Monitor's Call Detail Records screen. (For information on the CDR Monitor, see page 267.) A complete list of the categories of information stored in the buffer is found beginning on page 352.

Here is some of the useful information that can be gleaned from the CDRs:

On all types of Gateways for IP calls:

- Origination (for PRI gateways) and destination phone number and IP addresses
- Duration and quality (MOS) of each IP call, that is, the quality of the IP network
- Other parameters related to the call such as codec used, reason for call termination, digits received and/or dialed, etc.

On Gateways with authentication enabled, the CDRs show:

- The PIN code used for authentication
- Calls rejected because of an invalid PIN code (shows phone number and PIN code)

On Claro PRI and Analog, and on ROBO, it is possible to get CDRs for PSTN-PBX or PBX-PSTN calls. (On PRI Gateways, these CDRs also contain CallerID and Called number.) Although these calls are not routed via IP, it may be useful to see duration other information about calls made from PBX to PSTN.

IP Telephony...
Clear and Simple

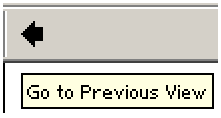
SECTION 24:
INDEX to the
BOSâNOVA GATEWAY ADMINISTRATOR'S GUIDE

Links to Index Headings												
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

All entries in this index are links.

Place the cursor over any page number and the cursor will turn into a hand, similar to this:

Click any index entry and the focus will jump to the designated area of the document. To return to the previous focus, click the **Go To Previous View** button.



For additional navigation tips, see "Using this Document" on page 4.

A

accepting
- a phone number 201
- a phone number inter-digit timeout 202

access code 84
adding
- new privates via dialing server 220
- service prefix 151

address resolution for Connect 248
advanced parameters, VoIP dialing 41
analyzer
- dial tone 70
- disconnect signal 68

announcements 32, 33
answer supervision
- battery reversal 51
- voice detection 50

area code 83
assigning private number prefixes, procedure 125
assigning private numbers, procedure 122
audible tone, duration 57
audio, non-interoperability 37
authentication 210
- caller ID 213
- Connects 214
- Link & Talk 214
- third party gateways 215

automatic dialing
- configuring procedure 134
- numbering plan 98
- reroute off of PSTN (hop-on) 162

B

back panel
- Claro Analog 20
- Claro E1/T1 PRI 18
- FXO 4 & 8 port 15
- FXS 13
- FXS 4 port 15
- PRI 16

back to back automatic dialing 100
battery reversal 51
B-channel selection 77
binary trace transfer 322
Blue Seal Security Lock
- location on Claro Analog 20
- remote management 274
- settings 272

BOScom SNMP manager demo 334
browser
- configuring the IP address 26
- requirements 4

bypass mode 7, 73

C

call
- completion testing 200
- maximum duration 318
- routing testing 200

call disconnect 68
call progress
- optional tone 59, 289
- port 41

caller ID
- and RBNM 177
- authentication 213
- displayed on ports monitor 266

carrier selection prefix 176
CDR 64
- BOScom CDR Reports Generator 350
- buffer 346
- buffer file structure 353
- configuring buffer flush 328
- enabling CDR sending 64
- field structure in MS SQL 356
- header structure 352
- installing the parser 349
- module 345
- monitor 267
- parser 347
- server 346
- server IP address 64
- table content, SNMP 336
- third party administration 64

changing
- codec settings 46
- password 326
- service prefix 152

choosing the officer Gateway 102
clearing clause parameters 289
codec 44
- changing settings 46
- enabling 45
- enabling and disabling 46
- setting the maximum frames 46
- type 44

command line configurator
- accessing 279
- commands 280, 281
- overview 278
- running scripts 285

common tables
  numbering plan 85
  private number prefixes 127
  updating via dialing server 224
configuration
  advanced parameters 41
  automatic dialing procedure 134
  Connect 246
  dialing parameters 31
  digital Gateway, PRI 71
  IP address between COM ports 24
  IP address using a browser 26
  IP address using Maintenance Wizard 22
  IP address using the terminal server 23
  IP settings 7, 324
  modem 325
  network 82
  numbering plan 109
  PRI 71
    restore default 77
    restore previous 77
  voice and telephony parameters 43
  VoIP dialing parameters 31
configuration files
  getting and saving 315
  uploading 317
configuring an officer
  dialing server 218, 225
Connect
  adding to Officer Gateway 246
  authentication 214
  configuring on PC 248
  installation with Connect 237
  modifying configuration 247
  reviewing current configuration 245
  serial number 247
  TCP/IP ports used by 234
  upgrading 242
connecting to a Gateway 299
connection types 81, 112, 145
  gatekeeper 147
  SIP proxy 153, 183
connections
  Claro Analog front panel 20
  Claro PRI back panel 18
  FXO 4 and 8 port back panel 15
  FXS 4 port back panel 15
  FXS back panel 13
  PRI back panel 16
conversion rules
  for SIP proxy 188
  third party IP telephony providers 196
country
  code 83
  impedance 58
creating private to public number associations
  procedure 172

D

deleting a Gateway, SNMP 336
descriptive name 111
designating a new officer
  dialing server 218, 225
diagnostic levels, setting 307
diagnostic, VoIP configuration 62
dial tone analyzer 70
dialing parameters configuration 31
dialing public numbers procedure 132
dialing server
  adding a new private 220
  configuring an officer 218, 225
  designating a new officer 218, 225
  updating common dialing tables 224
dialing tables 85
  synchronization 85, 143
DiffServ 62
disconnect signal analyzer 68
disconnect supervision 52
  battery reversal 51
  Claro Gateways 56
  PBX tones 52
  power denial 56
  silence detection 55
  threshold 54
DTMF timeout 57
duration of audible tones 57

E

E.164 83
E.164 alias 125, 148, 149
echo canceller 59
electrical noise 9
electrical requirements 9
electrostatic discharge damage prevention 9
emergency phone numbers and IP bypass 164
emergency traces 320
en bloc signaling 159
enabling a codec 45
encryption 41

F

fast start, H.323 37
fax parameters 39
finding
  and saving configuration files 315
  and saving current trace buffer 305
  and saving last trace buffer 305
  and saving trace files 301
finding all Gateways on the network 296
firewall
  Blue Seal Security Lock specifications 276
  NAT traversal of 232, 233
  remote configuration 274
flash 99
force dialout direction 106, 142
forced overlap mode 159
FXS back panel 13

G

Gatekeeper 147
Gateway
  connecting to 299
  descriptive name 111
  finding all Gateways on the network 296
  log monitor 264
  ports, monitor 266
  rebooting 7
  serial number 7
  software version 7
  telephony interface 7
Gateway monitor 263
  CDR 267
  QSR 269
getting
  and saving trace files 301
  configuration files 315
  current trace buffer 305
  last trace buffer 305
grounding requirements 9

H

H.245, tunneling 37
H.323
  fast start 37
  ID for gatekeeper 148
  preferred protocol 113
  with encryption 41
hang up 68
hidden parameters 286
hop-off
  calls, overview 96
  calls, procedure 128
  least cost routing 166
  PIN authentication 210
  prioritizing shared prefixes 167
  schemes 216
hop-on 162
HP OpenView
  alarms in 343
  importing MIBS 340
  registration tree MIB 342
  setting traps and alarms 343

I

impedance, country 58
inspecting the PRI cable 11
installation
  Connect 237
  general 8
  Link & Talk plug-in 260
  modem 28
  troubleshooting 30
installation key 252
inter-digit timeout 41
  accepting a phone number 202
  setting procedure 202
international
  access code 84
  direct dialing prefix 84
  numbering plan 83
IP
  checking connection to computer 310
  third party IP telephony providers 193
IP bypass 106, 163
  adding caller to 164
  adding phone number to 163
IP settings
  Configurator main menu 7
  configure from Maintenance Wizard 324
  maximum simultaneous IP calls 42
ITU E.164 standard 83
IVR 33

J

java scripts 255
jitter buffer 61

K

keep alive signal 230

L

last trace buffer, getting 305
least cost routing
  BOSaNOVA Gateway 166
  global priorities 206
  third-party gateways 169
  uniqueness check 204, 205
LED display 21
Link & Talk
  adding to Officer Gateway 252
  authentication 214
  description of files 254
  installation key 252
  installing the plug-in 260
  interface components 261
  java scripts associated with 255
  modifying configuration 253
  reviewing current configuration 259
  software download 252, 254, 255
  system requirements 251
  uninstalling the plug-in 260
local
  dialing table 85
  parameters
    private number prefixes 127
  PSTN parameters 129
  telephone number, E.164 standard 83
location requirements 9
log monitor 264
login to Configurator 5

M

maintenance wizard 293
  and Blue Seal Security Lock management 274
  call duration 318
  configuring the IP address 22
  online monitoring 302
  recording voice announcements 34
  scanning TCP/IP ports 329
  time configuration and synchronization 312
  voice announcement libraries 36
masks 169, 191
maximum call duration 282, 318
maximum private number length
  assigning 171
  overview 94
maximum simultaneous IP calls 42
MIB
  importing into HP OpenView 340
  private 332
  registration tree 342
  viewing 338
modem
  backup threshold setting 66
  configuring 325
  installation 28
monitor
  CDR 267
  log 264
  ports 266
  QSR 269
monitor Gateway 263
monitoring online via maintenance wizard 302
mounting the Gateway 10
MS SQL
  CDR field structure in 356
  installing on CDR server 351
multi-packet 46
multiplexing, Q.931 page 37

N

naming a Gateway 111
NAT
  configuration 229
  location of Officer within 229
  planning Net IDs 228
  TCP/IP ports used by Connect 234
  TCP/IP ports used by Gateways 232
national destination code 83
national direct dialing prefix 84
national trunk prefix 84
native dialing 96
Net ID 228
NetCoder codec advanced parameters 46
network configuration 82
network time protocol 312
noise filtration 54
NTP 312
number length, maximum, private 94
number testing procedure 200
numbering plan
  and Connect 248
  authentication 210
  H.323 or SIP 113
  initial configuration 109
  international standard 83
  overview 85–103
  saving as CSV 89
  validation 198
  verification 143, 198

O

officer and private Gateway assignment
    procedure 218
officer Gateway 85
    adding Connect to 246
    and NAT configuration 229
    modifying Connect configuration 247
    selecting 102
online monitoring 302
operands for RBNM 180
operation code for RBNM 180
outside line 84
overlap signaling 159

P

parameters
    100rel 38
    advanced 58
    answer supervision 50
    clearing clause 289
    codec 44
    dialing, configuring 31
    disconnect supervision 52
    early media 38
    fax support 39
    force dialout direction 106, 142
    H.323 or SIP 113
    hidden 286
    IP bypass 106, 163
    local PSTN 129
    NetCoder codec advanced 46
    rport 230
    silence detection 55
    timeout 57
    voice and telephony 43
    voice packet priority 62
    volume 49
parser installation 349
password
    changing via Configurator main menu 7
    changing via Maintenance Wizard 326
PBX
    extension and flash 99
    private number prefixes 91
phone number prefix for SIP proxy 186
port
    configuration detail screen 121
    enable auto dialing per port 135
    enable hop-off per port 120
    information page of the Wizard 119
    phone numbers for Claro Analog 139
    private numbers page of Wizard 122
ports
    see also TCP/IP ports 329
ports monitor 266
power denial 56
preferred protocol 113
prefixes, private number 91
PRI
    cable pin out 11
    Claro interface 72, 74
    configuration 71
    configuration settings
        restore default settings 77
        restore previous 77
    tester 10
private and officer Gateway assigning procedure 218
private Gateway 85
private MIB 332
private number prefixes 91
    common tables 127
    local parameters 127
    procedure 125
    PSTN 92
    telephones 91
private numbers 87
    local parameters, procedure 121, 124
    maximum length 94
    procedure 122
private to public number associations 103
procedure
    assigning maximum private number length 171
    assigning private number prefixes 125
    assigning private numbers 122
    configuring automatic dialing 134
    creating private to public number associations 172
    dialing public numbers configuration 132
    officer and private Gateway assigning 218
    terminating hop-off calls 128
product information 295
providers 193
PSTN
    local parameters 129
    private number prefixes 92
    reroute off of (hop-on) 162
PuTTY and CLC 279

Q

Q.931, multiplexing 37
Q-CDR 64
QoS
    enabling 65
    frequency of test 66
    modem threshold 66

QSR 64
QSR monitor 269
quality of service module 65

R

RBNM 88
    and forced overlap mode 158, 159
    caller ID authentication 177
    creating a rule 178
    examples 176
    for SIP proxy 188
    operands 180
    operation code 180
realtime transport protocol 41
rebooting a Gateway 7
registration parameters
    E.164 alias 125, 148, 149
    H.323 ID 148
    service prefixes 150
removing a service prefix 152
requirements
    browser 4
    for modem installation 28
    for officer Gateway 102
    PC system 4
restore
    previous PRI configuration settings 77
    previous PRI default settings 77
reviewing
    numbering plan configuration wizard 143
    PRI configuration 72
    the status of Gateways on the network 296
RJ45 socket pin out 11
RJ45 tester 10
rport parameter 230
RS-232 connection between COM ports 24
RTP 41, 45, 233, 251, 276, 277
rule based number management 88, 174

S

safety recommendations 9
saving
    and getting trace files 301
    configuration files 315
    numbering plan 89
scanning TCP/IP ports 329
service prefixes 150
setting
    diagnostic levels 307
    time and date 321
short-cut dialing 103
signal analyzer wizard 67
silence detection 55
silence suppression 61
SIP 38, 113
SIP proxy
    adding a new 154, 184
    connection type 153, 183
    conversion rules 188
    keep alive signal 230
    phone number prefix 186
SNMP
    adding a Gateway 337
    CDR table content 336
    clear traps log 339
    deleting a Gateway 336
    demo 334
    listening for traps 339
    manager 331
    scanning for Gateways 337
    traps 333
software updating 301
sounds
    dial tone, ring-back 37
    preceding call connection 37
SQL database 347, 351
SSH client and CLC 279
startup procedure 22
statistic servers 64
status of Gateways on the network 296
subscriber number, E164 standard 83
synchronization
    dialing tables 85, 143
    of time and date 321
    verify status checkbox 143
system name 7, 148
system password, changing 326
system requirements 4

T

tables
    dialing, synchronized 85
    service prefix 150
tagging packets 62
TCP/IP ports
    scanning with maintenance wizard 329
    used by Connect 234
    used by Gateways 232
    used by Link & Talk 251
telephone number, E.164 standard 83
terminal server 308
terminating hop-off calls procedure 128
test button, for call routing and completion 200
tester for Claro PRI RJ-45 10

third party
- billing software and CDR parser 349
- CDR administration 64
- gateway authentication 210, 215
- gateways, configuring 189
- gateways, least cost routing 169
- gateways, masks 169, 191
- gateways, prioritizing for LCR 169
- IP telephony providers 193

threshold 54
time and date
- automatic synchronization 312
- NTP servers 312
- setting 321
- synchronization 321

timeout 57
tones
- BOS call progress tone 59
- routing tones 59

ToS 62
trace buffer, getting the current 305
trace files 305
- from previous start 320
- getting 320
- getting and saving 301

trace, binary 322
transfer, binary trace file 322
traps
- clear log 339
- listening for, SNMP 339
- setting in HP Openview 343

traps SNMP 333
troubleshooting
- installation 30

tunneling, H.245 page 37
type of service 62

U

uniqueness check 204, 205
updating
- common dialing tables 224

updating software 301
uploading configuration files 317

V

variable bit-rate 46
verifying a numbering plan 143, 198
viewing MIB 338
virtual
- private network 96
- remote PBX extension 99

voice announcements
- downloading and uploading 36
- enabling and disabling 33
- library of 32
- recording 34

voice detection 50
voice packet priority 62
VoIP configuration, dialing parameters 31
volume 49

W

wizard
- dial tone analyzer 70
- disconnect signal analyzer 68
- maintenance wizard 293
- numbering plan short wizard 109
- numbering plan wizard guide 108