

---

# ***WEB UI***

# ***Operation Guide***

## ***BSGX4e***

## ***Business Services Gateway***

NN47928-502  
Software Release 2.1.1

---

## **BSGX4e 1.2**

### **Business Services Gateway**

Document Status: **Standard**

Document Version: **01.01**

Document Number: **NN47928-502**

Date: **July 2008**

---

**Copyright © 2008 Nortel Networks, All Rights Reserved**

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

---

#### **Trademarks**

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

Microsoft, MS, MS-DOS, Windows, and Windows NT are trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

---

# CONTENTS

---

<b>About this guide</b>	<b>15</b>
Introduction . . . . .	15
Intended audience . . . . .	15
Organization . . . . .	16
Text conventions . . . . .	17
Documentation . . . . .	17
How to get help . . . . .	18
Getting help from the Nortel Web site . . . . .	18
Getting help over the phone from a Nortel Solutions Center . . . . .	18
Getting help from a specialist by using an Express Routing Code . . . . .	18
Getting help through a Nortel distributor or reseller . . . . .	19
 <b>1 Web UI introduction</b>	 <b>21</b>
Window components . . . . .	22
Button bar . . . . .	22
Assistance icons . . . . .	22
Menu pane . . . . .	23
System button . . . . .	23
Data button . . . . .	23
Quality button . . . . .	23
Security button . . . . .	23
Voice button . . . . .	23
Monitor button . . . . .	23
Operations pane . . . . .	24
Display pane . . . . .	24
Usage notes . . . . .	25
Browser Requirements . . . . .	25
Connecting to the BSGX4e . . . . .	25
Notes . . . . .	25
Entering numerical data . . . . .	26
 <b>2 System pages</b>	 <b>27</b>
Status page . . . . .	29
System > Status > Current Calls panel . . . . .	29
System > Status > System panel . . . . .	30
System > Status > Call Quality History panel . . . . .	30
System > Status > Routing PPS panel . . . . .	30
System > Status > System Log panel . . . . .	30
Overview page . . . . .	31

---

System > Overview > System Information panel . . . . .	32
System > Overview > Shell panel . . . . .	32
System > Overview > System Hardware panel . . . . .	32
Services page . . . . .	33
System > Services > Web Configuration panel . . . . .	34
System > Services > Telnet Configuration panel . . . . .	34
System > Services > SNTP Configuration panel . . . . .	35
System > Services > SSH Configuration panel . . . . .	35
System > Services > DNS Configuration panel . . . . .	36
Configuration . . . . .	36
DNS server sources . . . . .	37
Application scenario – DNS backup configuration . . . . .	38
System > Services > Dynamic DNS Settings . . . . .	39
Configuration . . . . .	39
User accounts page . . . . .	41
Technical reference . . . . .	41
Terminology . . . . .	41
Default configuration . . . . .	42
Rights . . . . .	42
Passwords . . . . .	43
Configuration . . . . .	43
System > User Accounts > Users tab . . . . .	43
System > User Accounts > Groups tab . . . . .	45
System > User Accounts > Rights . . . . .	46
DHCP server . . . . .	47
Functional characteristics . . . . .	48
Configuration . . . . .	48
System > DHCP Server > Pool tab . . . . .	48
System > DHCP Server > Lease tab . . . . .	49
System > DHCP Server > Option tab . . . . .	49
System > DHCP Server > Host tab . . . . .	52
System > DHCP Server > VendorClass tab . . . . .	52
RADIUS and TACACS+ . . . . .	53
Technical reference . . . . .	53
Configuration . . . . .	54
System > Radius . . . . .	54
System > TACACS+ . . . . .	55
SNMP . . . . .	56
Configuration . . . . .	57
System > SNMP > Agent tab . . . . .	57
System > SNMP > Traps tab . . . . .	57
System > SNMP > Community tab . . . . .	57
System > SNMP > Statistics tab . . . . .	58
SSL . . . . .	59
Application notes . . . . .	59
Configuration . . . . .	60
System > SSL > Key tab . . . . .	60

---

System > SSL > Cert Reqs tab . . . . .	61
System > SSL > Certificates tab . . . . .	61
Upgrade . . . . .	62
System > Upgrade . . . . .	62
Configuration . . . . .	63
System > Configuration > Save /Restore . . . . .	63
Save . . . . .	63
Restore . . . . .	63
License . . . . .	64
Logging information . . . . .	64
System > Logging Info > Logging Destination panel . . . . .	65
System > Logging Info > Counters Info panel . . . . .	65
System > Logging Info > Logging Map panel . . . . .	66
Logging modules . . . . .	67

---

### 3 Data pages 69

WAN . . . . .	70
Interfaces . . . . .	70
Data > Interfaces > IP page . . . . .	70
IP display pane . . . . .	71
IP configuration . . . . .	71
IP statistic . . . . .	72
VLAN configuration . . . . .	73
Data > Interfaces > PPP page . . . . .	73
PPP configuration summary . . . . .	74
Configuring a PPP profile . . . . .	74
Data > Interfaces > VLAN . . . . .	75
Technical reference . . . . .	76
Configuration overview . . . . .	76
Configuration procedure – Virtual interface . . . . .	77
Relays . . . . .	78
Data > Relays > DNS page . . . . .	78
Settings tab . . . . .	79
Sessions and cache tabs . . . . .	80
Data > Relays > TFTP page . . . . .	80
Settings tab . . . . .	82
Sessions tab . . . . .	82
Cache tab . . . . .	82
Files tab . . . . .	83
Data > Relays > SNTP page . . . . .	83
Settings tab . . . . .	84
Sessions tab . . . . .	84
Data > Relays > DHCP page . . . . .	85
Routing . . . . .	86
Technical reference . . . . .	86
Data > Routing > Routes Table . . . . .	87

Data > Routing > ARP . . . . .	88
ARP Table tab . . . . .	88
Proxy ARP tab . . . . .	89
Data > Routing > RIP . . . . .	94
Functional characteristics . . . . .	94
Configuration . . . . .	94
Switch . . . . .	95
Data > Switch > Status page . . . . .	95
Port page . . . . .	96
Data > Switch > Ports tab . . . . .	96
Data > Switch > Mirror tab . . . . .	97
Data > Switch > Stats tab . . . . .	97
QoS page . . . . .	98
Data > Switch > IEEE tab . . . . .	100
Data > Switch > Port tab . . . . .	100
Data > Switch > ToS tab . . . . .	100
Data > Switch > Settings tab . . . . .	100
Data > Switch > ARL . . . . .	101
Technical reference . . . . .	101
Configuration procedure . . . . .	102
Clearing the table . . . . .	102
Data > Switch > VLAN . . . . .	103
Technical reference . . . . .	103
Configuration procedure . . . . .	104

---

## 4 Quality pages 105

Introduction . . . . .	105
Calls page . . . . .	106
Quality > Calls > Quality tab . . . . .	107
Quality > Calls > Alarms tab . . . . .	107
Quality > Calls > Analyser tab . . . . .	107
Link page . . . . .	110
Quality > Link > Link tab . . . . .	110
Quality > Link > Stats tab . . . . .	111
Group page . . . . .	112
Quality > Group > Group tab . . . . .	112
Configuring a new quality group . . . . .	114
Using wizards . . . . .	115
Quality > Group > Stats . . . . .	116
Quality > Group > Live . . . . .	117
Downstream QoS page . . . . .	118
Quality > Downstream QoS > Link tab . . . . .	119
Quality > Downstream QoS > Status tab . . . . .	120
Quality > Downstream QoS > Stats tab . . . . .	120
ARP/PPP page . . . . .	121
Configuration . . . . .	122

<b>5 Security pages</b>	<b>123</b>
Security overview . . . . .	124
Policy . . . . .	125
Technical reference . . . . .	125
Default security policies . . . . .	126
Additional security policies . . . . .	126
This section describes additional policies that you must add for various features in the BSGX4e. . . . .	126
QoS quality groups . . . . .	126
Relay security policies . . . . .	129
RIP security policy . . . . .	129
Security > Policy page . . . . .	130
Security > Policy > Static tab . . . . .	130
Dynamic tab . . . . .	131
NAT . . . . .	132
Technical reference . . . . .	132
Configuration . . . . .	133
Security > NAT > Interfaces tab . . . . .	134
Security > NAT > Policy tab . . . . .	134
Security > NAT > Public tab . . . . .	135
Application scenarios . . . . .	136
ALG . . . . .	139
Security > ALG page . . . . .	139
QoS and PPTP . . . . .	140
IDS . . . . .	140
Security > IDS > Anomaly tab . . . . .	141
Security > IDS > Protection tab . . . . .	142
IDS flood activity . . . . .	142
IDS flood settings . . . . .	143
IDS scan . . . . .	144
IDS spoof . . . . .	144
Security > IDS > Attacks tab . . . . .	145
Voice ACL . . . . .	145
Configuration . . . . .	146
IPSec/IKE and VPN . . . . .	147
IPSec . . . . .	147
Security > IPSec > Policy tab . . . . .	147
Security > IPSec > Proposals tab . . . . .	148
Security > IPSec > Parameters tab . . . . .	149
Security > IPSec > SA tab . . . . .	149
IKE . . . . .	150
Security > IKE > Policy tab . . . . .	150
Security > IKE > Preshared tab . . . . .	150
Security > IKE > Parameters tab . . . . .	151
Security > IKE > SA tab . . . . .	152
VPN . . . . .	152
Configuration examples . . . . .	152

<b>6 Voice pages</b>	<b>159</b>
Media . . . . .	161
Voice > Media > Settings . . . . .	161
Configuration . . . . .	161
Voice > Media > Gain . . . . .	162
Voice > Media > Local Jitter Buffer . . . . .	162
Settings tab . . . . .	162
Stats tab . . . . .	163
Session control . . . . .	164
Voice > Session Control > SIP Server . . . . .	164
Configuration tab . . . . .	165
Status tab . . . . .	166
Voice > Session Control > SIP Control . . . . .	167
Control tab . . . . .	167
Status tab . . . . .	169
Calls tab . . . . .	169
Endpoints tab . . . . .	169
Voice > Session Control > SIP Statistics . . . . .	171
Voice > Session Control > SIP LAN Gateway . . . . .	171
Voice > Session Control > MGCP Server . . . . .	171
Configuration tab . . . . .	172
Status tab . . . . .	172
Voice > Session Control > MGCP Control . . . . .	172
Control tab . . . . .	172
Status tab . . . . .	173
Calls tab . . . . .	173
Endpoints tab . . . . .	173
Voice > Session Control > MGCP Statistics . . . . .	174
User agent . . . . .	175
Dependencies . . . . .	175
SIP page . . . . .	176
Voice > User Agent > SIP > Configuration tab . . . . .	176
Voice > User Agent > SIP > Settings tab . . . . .	178
Voice > User Agent > SIP > Status tab . . . . .	179
MGCP page . . . . .	179
Voice > User Agent > MGCP > Configuration tab . . . . .	179
Voice > User Agent > MGCP > Settings tab . . . . .	180
Voice > User Agent > MGCP > Status tab . . . . .	181
Voice > User Agent > Numbering Plan . . . . .	181
Configuration . . . . .	182
Configuration and application examples . . . . .	182
Local call routing . . . . .	185
Voice > Local Call Routing > Account tab . . . . .	185
Configuration . . . . .	186
Voice > Local Call Routing > Connection tab . . . . .	186
Voice > Local Call Routing > Settings tab . . . . .	186



---

<b>Appendix 12–Quality of service</b>	<b>189</b>
Configuration summary . . . . .	189
SIP / MGCP Traffic . . . . .	189
Other traffic. . . . .	190
QoS overview . . . . .	190
Quality of service – Layer 2 . . . . .	191
Priority classification. . . . .	191
Priority scheduling . . . . .	192
Guarantee of service – Layer 3 . . . . .	193
Functional characteristics. . . . .	195
Media and control signals . . . . .	196
Managing other traffic . . . . .	197
Call capacity . . . . .	198
<b>Appendix 13–Glossary</b>	<b>199</b>
<b>Index</b>	<b>203</b>

---



# LIST OF FIGURES

Figure 1 Components of the Web UI page	22
Figure 2 Status page	29
Figure 3 Overview page	31
Figure 4 Services page	33
Figure 5 User Accounts Page	41
Figure 6 DHCP Server Pages	47
Figure 7 SNMP agent configuration	56
Figure 8 SSL configuration	59
Figure 9 Upgrade system image	62
Figure 10 Configuration file Save / Restore	63
Figure 11 Logging information	64
Figure 12 IP Interface display pages	70
Figure 13 PPP interface page	73
Figure 14 VLAN interface page	75
Figure 15 Relay – DNS page	78
Figure 16 Relay – TFTP page	81
Figure 17 Relay – SNTP page	83
Figure 18 Relay – DHCP page	85
Figure 19 Routing Table page	87
Figure 20 ARP Table page	88
Figure 21 Proxy ARP page	89
Figure 22 Proxy ARP – General configuration example	91
Figure 23 Proxy ARP – Subnet with firewall	93
Figure 24 RIP page	94
Figure 25 LAN status page	95
Figure 26 LAN ports page	96
Figure 27 LAN Port QoS Page	98
Figure 28 Layer 2 QoS functionality	99
Figure 29 ARL page	101
Figure 30 VLAN – LAN switch	103
Figure 31 Quality calls page	106
Figure 32 Calls analyzer flows	108
Figure 33 Quality link page	110
Figure 34 Quality group page	112
Figure 35 Downstream QoS page	119
Figure 36 ARP / PPP QoS page	121
Figure 37 NAT page	132
Figure 38 Security ALG page	139

Figure 39 IDS page .....	140
Figure 40 Voice ACL page .....	145
Figure 41 IPSec page .....	147
Figure 42 IKE page .....	150
Figure 43 Layer 2 QoS contention .....	191
Figure 44 Layer 2 QoS Application Scenarios .....	193
Figure 45 GoS Quality Class Matrix .....	194
Figure 46 GoS process flow .....	195

## ***LIST OF TABLES***

Table 1	Web UI operation guide organization	16
Table 2	Text conventions	17
Table 3	System > Status > System panel information	30
Table 4	User rights permissions	42
Table 5	System message severity	67
Table 6	WAN interfaces	70
Table 7	DHCP client status by interface	72
Table 8	Sources for DNS relay configuration	80
Table 9	Sources for SNTP relay configuration	84
Table 10	Default priority classification settings	99
Table 11	Qos link rate defaults	116
Table 12	QoS groups defaults – BSGX4e	116
Table 13	WAN encapsulation options	120
Table 14	Packet security processing	124
Table 15	Default firewall policies – BSGX4e	126
Table 16	Firewall policies for PPP	127
Table 17	Firewall policies for VLAN	127
Table 18	Firewall Policies for SNMP	128
Table 19	Firewall policies for DHCP relay	128
Table 20	Firewall policies for VPN	128
Table 21	Security policies for relay	129
Table 22	Security policy for RIP	129
Table 23	WAN subnet configuration	135
Table 24	Protocols for which IDS attack protection applies	141
Table 25	Packet anomaly attacks	142
Table 26	Bandwidth for each call	198



---

# ABOUT THIS GUIDE

This section provides information about the intended audience for this guide, how this guide is organized, typographical conventions, and how to get help.

---

## Introduction

This document describes the operation of the Web User Interface (Web UI) for the BSGX4e model. For a list of all BSGX4e technical documents, see [Documentation on page 17](#).

The BSGX4e device is deployed as customer premise equipment and provides a unified solution for voice and data services. BSGX4e is designed for use in small- and medium-sized enterprises.

---

## Intended audience

This document is designed for use by network managers, administrators, and technicians who are responsible for the installation and operation of networking equipment in enterprise and service provider environments. Knowledge of telecommunication and internet protocol (IP) technologies is assumed.

# Organization

The following table describes the organization and content of this Web User Interface (UI) Operation Guide.

**Table 1** Web UI operation guide organization



Chapters	Contents
<a href="#">1 Web UI introduction</a>	Layout, organization and navigation features of the Web UI
<a href="#">2 System pages</a>	Configuration and status pages available from the System button: Network services; User accounts; LAN DHCP server; External authentications; SNMP; SSL; System upgrade; Logging
<a href="#">3 Data pages</a>	Configuration and status pages available from the Data button: IP interfaces; WAN interface options; Network relay services; Routing tables, ARP and RIP; LAN switch configurations; VLAN
<a href="#">4 Quality pages</a>	Configuration and status pages available from the Quality button: Quality of Service (QoS) configuration
<a href="#">5 Security pages</a>	Configuration and status pages available from the Security button: Firewall policies; NAT; ALG; ACL; IPSec/IKE
<a href="#">6 Voice pages</a>	Configuration and status pages available from the Voice button: QoS associations; FXS/FXO ports; Session controller; User agent; Local call routing
<a href="#">Appendix 12–Quality of service</a>	A technical description of the theory and application of QoS
<a href="#">Appendix 13–Glossary</a>	Glossary of industry and BSGX4e terminology
<a href="#">Appendix 13–Glossary</a>	
<a href="#">Index</a>	



## Text conventions

This guide uses the ftext font conventions described in the following table.

**Table 2** Text conventions

Font	Purpose
<b>NOTE:</b>	Emphasizes information to improve product use.
 <b>Caution:</b>	Indicates how to avoid equipment damage or faulty application.
 <b>Warning</b>	Issues warnings to avoid personal injury.
<i>italic</i>	Shows book titles, special terms, or emphasis.
<b>label</b>	Shows on-screen labels and commands.
<code>screen font</code>	Shows screen font as displayed in a terminal, and command option choices.
<b>screen font</b> <b>bold</b>	Shows a command to enter exactly as written.
<code>screen font</code> <i>italic</i>	Indicates a command variable that is replaced with a value.
<a href="#">cross reference</a>	Indicates a hypertext link to another section, or to a Web page.
<a href="#">glossary</a>	Indicates a hypertext link to the glossary entry that defines the marked term.

## Documentation

BSGX4e documentation is on the BSGX4e Series Documentation CD-ROM shipped with the unit. The following guides are available on the CD-ROM.

- ❑ *BSGX4e Hardware Installation Guide*
- ❑ *BSGX4e Initial Configuration Guide*
- ❑ *BSGX4e Quick Start Guide*
- ❑ *BSGX4e Web UI Operation Guide*
- ❑ *BSGX4e CLI Reference Guide*

The guides are provided in portable document format (PDF). The PDF files are also available on the Nortel Web site: [www.nortel.com](http://www.nortel.com)

To view PDF files, use Adobe Acrobat® Reader® 5.0, or newer, from your workstation. If you do not have the Adobe Acrobat Reader installed on your system, you can obtain it free from the Adobe Web site: [www.adobe.com](http://www.adobe.com).

---

## How to get help

This section explains how to get help for Nortel products and services.

### Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

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

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

### Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

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

### Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

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

---

## Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.



# 1 WEB UI INTRODUCTION

This chapter describes the layout, organization, and navigation features of the BSGX4e Web User Interface (Web UI).

The Web UI is a graphical, interactive interface accessible through a Web browser. It allows for interactive administration and monitoring of the BSGX4e functions and is accessed through either HTTP or HTTPS protocols. For more information about remote Web access, see [System > Services > Web Configuration panel on page 34](#).

Use the Web UI to perform various configuration tasks on the BSGX4e. The following list demonstrates some of the common tasks:

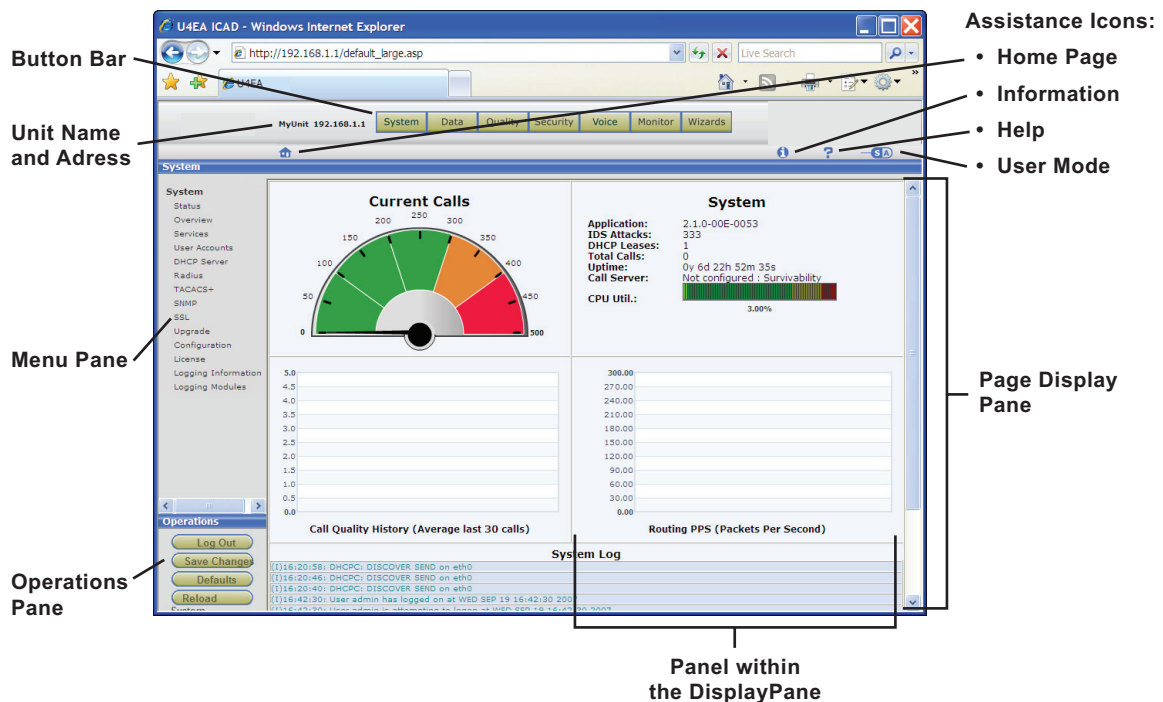
- ❑ manage user accounts and access levels
- ❑ set up VoIP components and other voice-related parameters
- ❑ establish VPN or VLAN configurations
- ❑ configure network services such as DNS, DHCP, SNTP, and SNMP
- ❑ configure LAN and WAN ports
- ❑ configure firewall, intrusion detection, IPsec, and security policies
- ❑ monitor performance
- ❑ upgrade software

The Web UI accesses most BSGX4e configuration parameters. However, you must use CLI commands for some variable settings. See the *CLI Reference* document.

# Window components

This section describes the main components that are visible in the Web UI window.

**Figure 1** Components of the Web UI page



## Button bar

Each button represents a category of functions, which appear as links in the menu pane on the left side of the window. The Web UI is open when the System > Status page appears.

## Assistance icons

Assistance icons provide the following services:

- **Information**—Provides product information by opening a new browser window and connecting to the Web page of the manufacturer.
- **Help**—Displays an overview of the BSGX4e features and services.
- **User mode**—Selects the desired user mode:
  - S = Simple mode. Field explanations are displayed in the Web UI pages.
  - A = Advanced mode. Field explanations are not provided.
- **Home**—Returns the Web UI to its home page, which is the System > Status page.

## Menu pane

Click a link in the menu pane to load a corresponding configuration page in the display pane. A list of menus changes appears with each button on the button bar.

### System button

System
<b>System</b>
Status
Overview
Services
User Accounts
DHCP Server
Radius
TACACS+
SNMP
SSL
Upgrade
Configuration
License
Logging Information
Logging Modules

### Data button

Data
<b>WAN</b>
<b>Interfaces</b>
IP
PPP
VLAN
<b>Relays</b>
DNS
TFTP
SNTP
DHCP
<b>Routing</b>
Routes Table
ARP
RIP
<b>Switch</b>
Status
Port
QoS
ARL
VLAN

### Quality button

Quality
<b>Quality</b>
Calls
Link
Group
Downstream QoS
ARP/PPP

### Security button

Security
<b>Security</b>
Policy
NAT
ALG
IDS
Voice ACL
IPSec
IKE

### Voice button

Voice
<b>Media</b>
Settings
Gain
Local Jitter Buffer
<b>Session Control</b>
SIP Server
SIP Control
SIP Statistics
SIP LAN Gateway
MGCP Server
MGCP Control
MGCP Statistics
<b>User Agent</b>
SIP
MGCP
Numbering Plan
<b>Local Call Routing</b>
Account

### Monitor button

Monitor
<b>Protocol</b>
Pmon
CDP
<b>Netflow</b>
Agent
Filter
Stats
<b>Calls</b>
Current
History
Statistics
<b>Statistics</b>
IP
<b>TCP</b>
UDP
ICMP
IKE
ESP
<b>Audit</b>
Status

## Operations pane

The following links perform system operations for the current session:

- **Log Out** – Logs out the user and returns to the log in screen. Unsaved configuration changes are kept unless the unit restarts.
- **Save Changes** – Saves configuration changes to nonvolatile memory. (When configuration changes are pending, the Save Changes button turns red.)
- **Factory Defaults** – Erases the current configuration stored in memory and restores the original, default configuration of the unit.
- **Reboot System** – Logs out the user and restarts the BSGX4e with the configuration stored in memory. Unsaved configuration changes are discarded and the browser connection to the unit is lost.

### Operation pane notes

- Configuration changes

Any configuration change you make takes effect immediately when you click an Update or Apply button in the page that appears. However, those buttons do not store the change in memory, so unsaved changes are lost if the unit reboots. You must use the Save Changes button for permanent storage.

- Reloading defaults

The Factory Defaults button erases any configuration changes you have made and saved into memory. This button also resets the eth1 (LAN) interface to the default address of 192.168.1.1. Added user accounts are erased, leaving the two default accounts: *admin* and *user*.



**CAUTION:** After configuring the BSGX4e for your site, export a configuration file and store it on a separate host so that you can retrieve the configuration if problems arise. See [Configuration on page 63](#).

## Display pane

The display pane displays the Web pages as you click on functional buttons or menu links. These pages can be interactive configuration pages or informational status pages.

The page in the display pane can be segmented into *panels* for different types of data.



---

## Usage notes

This section provides helpful notes on using the Web UI.

### Browser Requirements

The BSGX4e has been tested with Microsoft®, Internet Explorer®, and Mozilla® FireFox® browsers.

Internet Explorer must have the Adobe®, Shockwave®, Flash Object add-on. Firefox must have the Adobe Flash Player plugin. Use the browser's Manage Add-ons (Explorer) or Add-ons (FireFox) command to obtain the plugin.

### Connecting to the BSGX4e

The basic BSGX4e installation and cabling is covered in the *Quick Start Guide* and the *Installation Guide* on the *Documentation CD*. The following steps instruct you on accessing the Web UI:

1. Connect a PC to one of the BSGX4e LAN ports, labeled **1** through **4** on the box.
2. Open a Web browser. The BSGX4e has been tested with Microsoft® Internet Explorer® and Mozilla® FireFox®.
3. Enter **http://192.168.1.1** in the address bar of your browser.
4. On the User log in page, enter the default log in codes:

**User name:** admin

**Password:** PlsChgMe!

If you want to use the Initial Setup Wizard for the basic configurations tasks, select the Setup Wizard check box to immediately open the wizard. See the *Initial Setup Guide* on the *Documentation CD* for more information.

### Notes

- **Font size** – You may have to adjust the font size in the browser. If the text appears to be overrunning its boundaries or overlapping other areas, decrease the text size. Use the command on the **View** menu, or the keyboard shortcuts: **Ctrl+ +** and **Ctrl+ -**.
- **Log in failure** – If your log in fails on a new unit, retry the log in procedure to ensure you did not make a typing error. Also, your PC can have a static IP address rather than using DHCP to obtain a dynamic address.

If log in fails after having configured the unit, likely causes are a VLAN assigned to the port to which your PC is connected, or the IP address of the LAN switch has been changed. Use the CLI (connected to the serial port) to view or change parameters to re-establish the Web UI connection.

- **Connection failure** – If you are working on more than one BSGX4e you must clear the private data from the browser before connecting your PC to a different BSGX4e. The BSGX4e places cookies and browser history records into your browser. The cookies and browser history records prevent you from successfully connecting to a new BSGX4e unit.

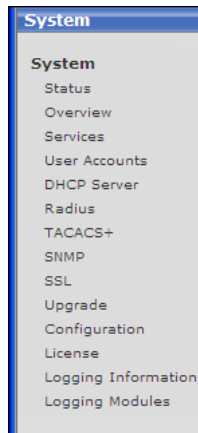
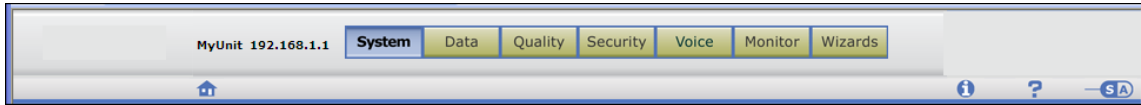
## Entering numerical data

The underlying architecture of the Web UI allows you enter numerical data in decimal, hexadecimal, or octal format. If you enter configuration data in hexadecimal or octal and then view the corresponding display page, you see the number has been converted to decimal.

This can cause confusion for an ID field where the number is used only to identify a record or profile. Nortel recommends that you use decimal numbers in these fields.

The Web UI processes any number that begins with 0x as hexadecimal and processes as any number that begins with 0 as octal.

## 2 SYSTEM PAGES



This chapter describes the configuration and status pages available from the **System** button on the button bar. The functional topics of the pages are listed in the menu pane of the Web UI window, as shown in the figure on the left.

The **System > Status** page is the home page of the Web UI and is the page appears when you log in.

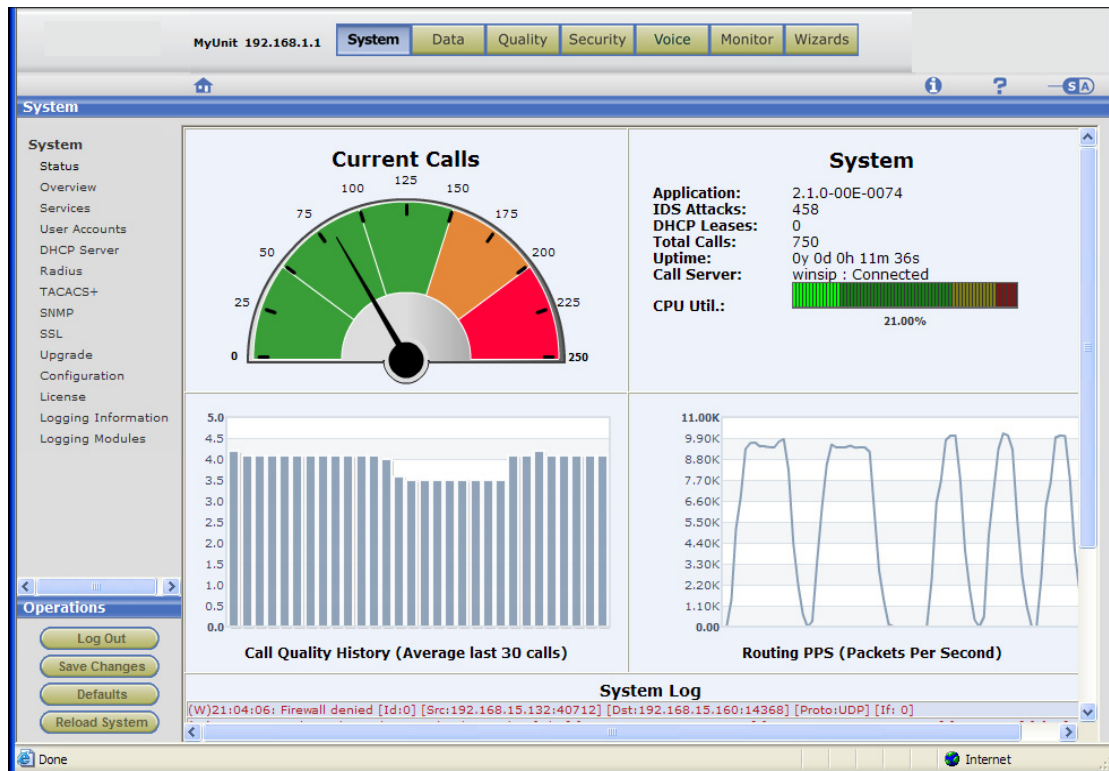
The following list provides an overview of the configuration and status functions on the System menu:

- **Status** ([page 29](#))  
Graphical displays showing call load and other operational data. Software version and other system data displayed. A system log viewer shows the latest log entries.
- **Overview** ([page 31](#))  
Listing of more detailed system data. Change the unit name and country. Set parameters of the command shell (used for CLI).
- **Services** ([page 33](#))  
Enable and configure ports for HTTP(S) and telnet connections. Configure DNS, SNMP, and SSH services.
- **User accounts** ([page 41](#))  
Create and modify user accounts. Assign groups and privileges. Assign passwords.
- **DHCP server** ([page 47](#))  
The BSGX4e can provide DHCP service for devices connected to the LAN (eth1/vifn). Modify the default profile or create a new one.
- **RADIUS** ([page 53](#))  
Configure RADIUS authentication service.
- **TACACS+** ([page 53](#))  
Configure TACACS+ authentication service.

- **SNMP** ([page 56](#))  
Configuration for remote monitoring of the system.
- **SSL** ([page 59](#))  
Configure key and certificates for SSL encryption.
- **Upgrade** ([page 62](#))  
Load software and bootloader upgrades. Switch between software configurations.
- **Configuration** ([page 63](#))  
Display current system configuration parameters. Export or import a configuration file.
- **License** ([page 64](#))  
Copyright statements from developers whose code is used in the Web UI.
- **Logging information** ([page 64](#))  
Configure message logging for which types of messages are sent to which destinations.
- **Logging modules** ([page 67](#))  
Configure modules (system functions) for which message types are logged.

# Status page

**Figure 2** Status page



The system status page is display-only, there are no configuration items.

Descriptions of the panels in the display pane follow.

## System > Status > Current Calls panel

This panel is a speedometer-type display that gives visual indication of the current call load.

You can change the scale of the display by setting the maximum calls parameter in the Session Controller, located under the Voice button in the Web UI. The default display is set for 50 calls. See the section, [Voice > Session Control > SIP Control on page 167](#), for configuration details.

Perform the following steps to set the maximum call limit in either SIP or MGCP protocols:

1. Click the **Voice** button and navigate to the **Session Control** section in the menu pane.
2. Configure the SIP or MGCP server.
3. Select that server on the SIP or MGCP control page.
4. Set the **Max Calls** field on the SIP or MGCP control page.

## System > Status > System panel

This panel displays the information shown in the following table.

**Table 3** System > Status > System panel information

<b>Application</b>	The software version running in the unit.
<b>IDS attacks</b>	The number of attempted attacks detected by the Intrusion Detection System.
<b>DHCP leases</b>	The number of IP address leases issued when the BSGX4e functions as a DHCP server to LAN devices.
<b>Total calls</b>	The cumulative number of calls processed by the BSGX4e during the indicated uptime.
<b>Uptime</b>	Cumulative running time since the last bootup. Displayed in years (y), days (d), hours (h), minutes (m), and seconds (s).
<b>Call server</b>	The call server (SIP or MGCP) currently configured and operational status of the connection.  Survivability status – If VoIP services are unreachable, the BSGX4e still provides service between IP phones on its LAN, and can send some number of calls to the PSTN through the FXO port or an FXO gateway.  Connected status – VoIP services are reachable.
<b>CPU Util</b>	Graphical presentation of current CPU utilization.

## System > Status > Call Quality History panel

Graphical display of call quality, based on Mean Opinion Score, averaged from the last 30 calls.

## System > Status > Routing PPS panel

Graphical display of data packet rate through the BSGX4e routing engine.

The routing engine in the BSGX4e consists of the QoS quality groups, the routing table, and NAT.

## System > Status > System Log panel

Displays last 15 messages sent to the internal log.

Each log entry begins with a letter in parentheses, which maps to the first letter of the severity level of the log entry (listed here in descending order of severity):

Emergency	Notice
Alert	Inform
Critical	Debug
Error	Trace

See [Logging information on page 64](#) for related information.

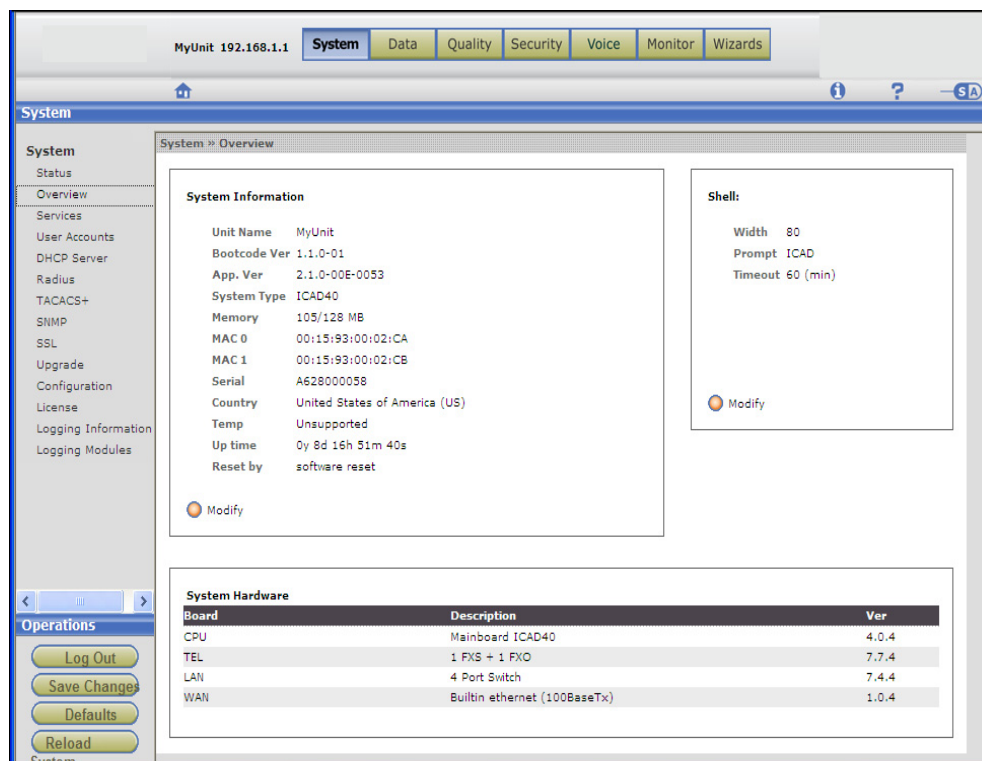
Warning

## Overview page

The system overview page displays system information, and it contains the following configurable parameters:

- ❑ the unit name displayed on the Web UI (left of the button bar)
- ❑ the country of operation, which affects telephony settings
- ❑ configuration of the CLI command shell

**Figure 3** Overview page



The panels in the display pane are described in the following sections.

## System > Overview > System Information panel

The System Information panel shows various high-level system configuration items. Further detail for some of the items:

Bootcode Ver – Version of the bootloader program

App. Ver – System software version

System Type – Model designation of this unit

Memory – RAM expressed as used/available

Up time – Cumulative running time since the last bootup Displayed in years (y), days (d), hours (h), minutes (m), and seconds (s)

MAC 0 – MAC address for the WAN interface

MAC 1 – MAC address for the LAN interface

You can configure the following parameters with the **Modify** button, click **Update** when finished:

<b>Unit name</b>	The BSGX4e unit name displayed to the left of the button bar.
<b>Country</b>	<p>The country of operation. Default is USA.</p> <p>This selection sets several parameters that affect the characteristics of an analog phone connected to the Phone port. See the paragraph below for more details.</p> <p><b>NOTE:</b> The drop-down list of names has a divider line (-----). The BSGX4e is certified for operation in those countries above the line. In those countries listed below the line, the BSGX4e is not certified for operation but you can use it for activities such as lab tests and field trials.</p>

**NOTE:** After changing the Country parameter, **Save** the change and **Reboot** the system to implement the change.

Countries have differing telephony standards including ring tones, ring cadence, and emergency numbers. The Country parameter loads country-specific default values into the unit. This affects Phone port parameters and LCR settings. See [Voice > Local Call Routing > Settings tab on page 186](#).

You can create ring tone patterns that override the country defaults using the CLI command `conf voice fxs ring`.

## System > Overview > Shell panel

This panel displays the configurable characteristics of the command shell used for the CLI.

You can configure the Width, Prompt, and Timeout parameters with the **Modify** button. The configuration page is self-explanatory. Click **Update** when finished.

## System > Overview > System Hardware panel

This pane displays version levels the main hardware components of the BSGX4e.

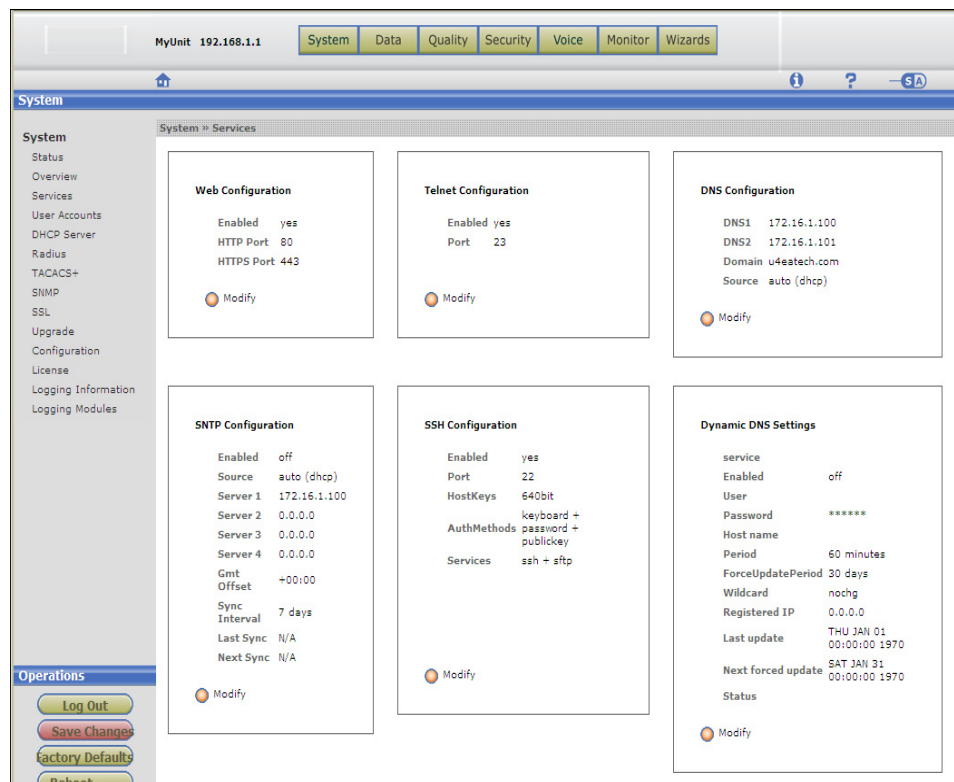


## Services page

The services page is where you enable and configure various network services:

- ❑ Web server – Enabled by default
- ❑ Telnet server – Enabled by default
- ❑ SNTP client – Disabled by default
- ❑ SSH server – Enabled by default
- ❑ DNS servers – Disabled by default
- ❑ Dynamic DNS client – Disabled by default

**Figure 4** Services page



Note that with some of these services (DNS, SNTP, DHCP), rather than having the BSGX4e act as the service client, you can configure it as a relay that forwards LAN requests to an external server. See the section [Relays on page 78](#).

The panels in the services page are described under the following headings.

## System > Services > Web Configuration panel

The Web server allows remote administration of the BSGX4e using the Web UI connected through the WAN or LAN ports. The server supports HTTP and HTTPS (HTTP over SSL) protocols.

The BSGX4e Web server is enabled by default and is configured to use the standard ports 80 (HTTP) and 443 (HTTPS). The Web UI uses the HTTP port by default. You can disable the server or change the access ports with the **Modify** button. Click **Update** when finished.

Firewall security policies must allow Web access from the WAN (eth0/ppp0/vif0) terminating in the BSGX4e (self). This requires access for TCP traffic being routed to ports 80 and 443. These security policies already exist by default. If you change the port configuration for the Web server you must create new security policies.

## System > Services > Telnet Configuration panel

Telnet allows access to the BSGX4e through a remote terminal session. This is required to access the CLI. The workstation connected to the BSGX4e WAN or LAN must have a Telnet client.

The BSGX4e Telnet server is enabled by default and is configured to use the standard port 23. You can disable the server or change the port with the **Modify** button. Click **Update** when finished.

A firewall security policy must allow Telnet access from the WAN terminating in the BSGX4e (self). This requires access for TCP traffic being routed to ports 23. A security policy already exists by default. If you change the port configuration for the Telnet server you must create a new security policy.

## System > Services > SNTP Configuration panel

You can use the SNTP client to automatically set the time in the BSGX4e. The SNTP client is disabled by default, requiring the time to be set manually. Use the Initial Setup Wizard to set the time manually.

Rather than using this client service, you can configure the BSGX4e as an SNTP relay. See [Data > Relays > SNTP page on page 83](#) for the SNTP relay function.

Configure the following parameters to enable the SNTP client, click **Update** when finished:

<b>Enabled</b>	Enables or disables the SNTP client
<b>Source</b>	Source of the SNTP server configuration { <b>auto</b>   <b>dhcp</b>   <b>user</b> }. <ul style="list-style-type: none"> <li>• <b>auto</b> – From the DHCP server if possible; otherwise, the last user-provided configuration. (Default)</li> <li>• <b>dhcp</b> – From the DHCP server. If the DHCP server cannot provide a configuration, the server address is set to 0.0.0.0.</li> <li>• <b>user</b> – User-provided configuration.</li> </ul>
<b>Server 1</b>	IP address or FQDN of an SNTP server.
<b>Server 2</b>	Optional backup IP address or FQDN of an SNTP server.
<b>Server 3</b>	Optional backup IP address or FQDN of an SNTP server.
<b>Server 4</b>	Optional backup IP address or FQDN of an SNTP server.
<b>Gmt Offset</b>	Time zone offset from Greenwich Mean Time (GMT). {+   -} <hh:mm> positive or negative; hours and minutes Default is +00:00.
<b>Sync Interval</b>	Interval for re-synchronization of the internal clock to the network time (external clock) in days. Range is 1 – 31. Default is 7.

## System > Services > SSH Configuration panel

The SSH server in the BSGX4e provides secure remote access to the BSGX4e client device over an insecure network, such as the Internet. SSH version 2 is supported.

The BSGX4e SSH server is enabled by default. The default configuration is:

**Port** – 22  
**Host Keys** – 640-bit DSA  
**Authentication Methods** – keyboard, password and public key  
**Services** – SSH and SFTP

You can disable the server or change the configuration parameters with the **Modify** button. Click **Update** when finished.

A firewall security policy must allow SSH access from the WAN terminating in the BSGX4e (self). This requires access for TCP traffic being routed to port 22. A security policy already exist by default. If you change the port configuration for the SSH server you must create a new security policy.

A workstation connected to the BSGX4e's WAN or LAN must provide an SSH client, such as PuTTY and SSH secure shell.

## System > Services > DNS Configuration panel

The Domain Name Service (DNS) client in the BSGX4e sends requests to a DNS server on the WAN. A DNS request is used to obtain an IP address required by the BSGX4e, such as the IP address of a server that was specified by an FQDN. Two DNS servers can be configured: a primary server and a secondary.

The DNS client is always active.

The default configuration of the DNS client is:

**DNS1** – <address supplied by DHCP client>

**DNS2** – <address supplied by DHCP client>

**Domain** – <name supplied by DHCP client>

**Source** – **auto** (**dhcp**)

The default configuration relies on the DHCP client to provide the DNS server addresses. The DHCP client is enabled by default on WAN interfaces that use a dynamic address. For WAN interfaces that use a static address, the DHCP client is disabled and you must manually configure the DNS client. See the appropriate section in [WAN on page 70](#) for specifics on WAN configuration.

The BSGX4e also includes a DNS relay feature that can be used to override the DNS client with a specific server address. For more information, see [Data > Relays > DNS page on page 78](#).

### Configuration

The parameters can be set as follows, click **Update** when finished:

<b>DNS1</b>	<p>Default is 0.0.0.0 with the <b>Source</b> is set to <b>auto</b>.  Leave blank (0.0.0.0) if <b>Source</b> is set to <b>auto</b>, <b>dhcp</b>, or <b>ppp</b>.  Enter an IP address for the primary DNS server if <b>Source</b> is set to <b>user</b>.</p> <p><b>NOTE:</b> If <b>Source</b> is set to <b>auto</b>, you can enter an address here that is applied if a DHCP or PPP server cannot be found. See <a href="#">Application scenario – DNS backup configuration</a>.</p>
<b>DNS2</b>	<p>This is a backup server to <b>DNS1</b>.  The description for <b>DNS1</b> also applies here.</p>
<b>Domain</b>	<p>Domain name for the unit. Enter a name if <b>Source</b> is set to <b>user</b>.  This value is cleared if <b>Source</b> is set to <b>auto</b>, <b>dhcp</b>, or <b>ppp</b>.  The DNS client adds the domain to the host before querying the DNS server. Example: If the specified name is <b>host</b> and the specified domain is <b>domain.com</b>, the query is for <b>host.domain.com</b>.</p>
<b>Source</b>	<p>Source of the DNS configuration profile {<b>user</b>   <b>dhcp</b>   <b>ppp</b>   <b>auto</b>}. See the following paragraph for details.  Default is <b>auto</b>.</p>

The DNS client determines the DNS configuration to use based on the current value of its **Source** parameter:

<b>user</b>	The DNS client retrieves the latest address/domain entered by the user.
<b>dhcp</b>	The DNS client uses the address provided by an external DHCP server that was discovered by the BSGX4e's DHCP client. The DHCP client must be enabled on the interface where the DHCP server is located. If a DHCP server cannot provide an address, the DNS1 and DNS2 fields are set to 0.0.0.0.
<b>ppp</b>	The DNS client uses the DNS address provided by a PPP server on the WAN. A PPP interface must be active on the WAN port. If the PPP server cannot provide an address, DNS1 and DNS2 fields are set to 0.0.0.0.
<b>auto</b> (default)	The DNS client gets its configuration automatically. It first attempts to get the configuration from a DHCP or PPP server. If that fails, it uses the latest user-defined configuration stored in memory. See the following section, <a href="#">DNS server sources</a> , for more detail. The auto parameter displays in one of three variations indicating the source of DNS configuration in use: <ul style="list-style-type: none"> <li>• auto (dhcp)</li> <li>• auto (ppp)</li> <li>• auto (user)</li> </ul>

## DNS server sources

Determining the DNS server on the WAN that the client points to depends on a combination of configuration settings:

- The BSGX4e *default configuration* includes the DNS client **Source** set to **auto**. The DNS client looks for a server address first from a DHCP server, then from a PPP server, and finally from the last stored user-defined address. If no address can be found from any source, the displayed address is 0.0.0.0.

The DHCP client on the WAN port is also enabled by default. The DHCP client searches for a DHCP server on the WAN for all interface types except PPP. With the DNS client **Source** set to **auto**, the DNS client obtains an address from the DHCP server found by the search. If none is found, the DNS client searches for a PPP server, which cannot be found if a PPP interface is not defined. The DNS client then looks for the last user-defined address.

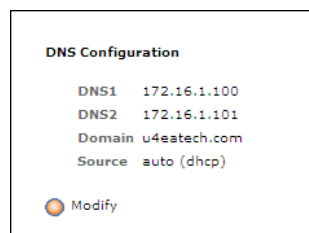
- If a PPP interface has been configured on the WAN port, the DHCP client has to be disabled. The DNS client cannot contact the DHCP client, so it next attempts to get a DNS address from the PPP server. If the PPP server does not provide a DNS address, the DNS client looks for the last user-defined address. If no address can be found from any source, the displayed address is 0.0.0.0.
- If **Source** is set to **dhcp**, the DNS client relies on the DHCP client to obtain a server address, as in the preceding paragraphs. If the DHCP client fails to obtain an address, there are no further searches and the displayed address is 0.0.0.0.
- If **Source** is set to **ppp** and a PPP interface is configured on the WAN port, the DNS client uses the PPP server to obtain an address. If the PPP server fails to provide an address, there are no further searches and the displayed address is 0.0.0.0.

- If **Source** is set to **user**, you must enter an address into the **DNS1** field. The DNS client does not perform any further address searches.

## Application scenario – DNS backup configuration


This example shows how a user configuration can be stored as a backup while using the auto-DHCP or auto-PPP configuration. If a DHCP or PPP server cannot provide a DNS address, the user configuration is automatically implemented by the DNS client.

1. The default configuration tries to auto-connect to a DHCP server, then a PPP server. The server provides the DNS addresses and the domain name.

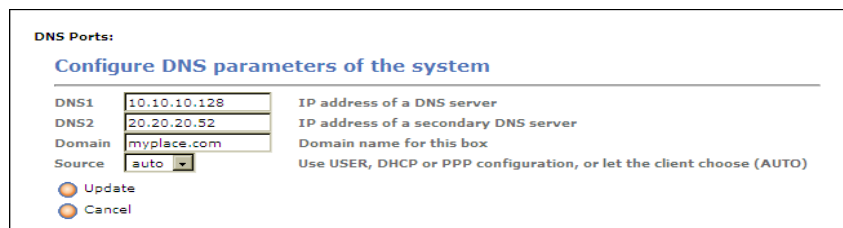


**DNS Configuration**

DNS1 172.16.1.100  
 DNS2 172.16.1.101  
 Domain u4eattech.com  
 Source auto (dhcp)

 Modify



2. Click **Modify** to open the configuration page. Enter a known DNS server address into the **DNS1** field, and a secondary server into **DNS2** if desired.



**DNS Ports:**

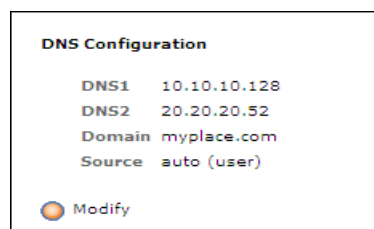
**Configure DNS parameters of the system**

DNS1  IP address of a DNS server  
 DNS2  IP address of a secondary DNS server  
 Domain  Domain name for this box  
 Source  Use USER, DHCP or PPP configuration, or let the client choose (AUTO)

 Update  
 Cancel


3. Leave the **Source** as **auto**.
4. Click **Update** to store this as a user configuration. A warning message displays stating the changes are to be applied when **Source** is user or auto (user).
5. Click **OK** to return to the configuration page. Click **Cancel** to close the configuration page.

Since **Source** is left at **auto**, the user configuration is not activated unless a DHCP or PPP server cannot be located. When this occurs, the DNS Configuration panel displays the user-defined configuration.



**DNS Configuration**

DNS1 10.10.10.128  
 DNS2 20.20.20.52  
 Domain myplace.com  
 Source auto (user)

 Modify

## System > Services > Dynamic DNS Settings

### Attention:

Dynamic DNS is not yet supported.

The Dynamic DNS service allows a remote host on the Internet to stay connected to the BSGX4e WAN port. When the BSGX4e is configured with a dynamic IP address on its WAN port, remote hosts cannot stay connected as the address of the BSGX4e changes. Dynamic DNS allows the domain name data held in a name server to be updated in real time. This allows the BSGX4e, servers, and other network devices to use a dynamic IP address but still have a permanent domain name.

**NOTE:** To use this feature, open an account with a dynamic DNS service and register a host name alias for the BSGX4e with the service provider. Two dynamic DNS services have been qualified for use with the BSGX4e: [dyndns.org](http://dyndns.org) and [no-ip.com](http://no-ip.com).

Dynamic DNS is disabled by default.

### Configuration

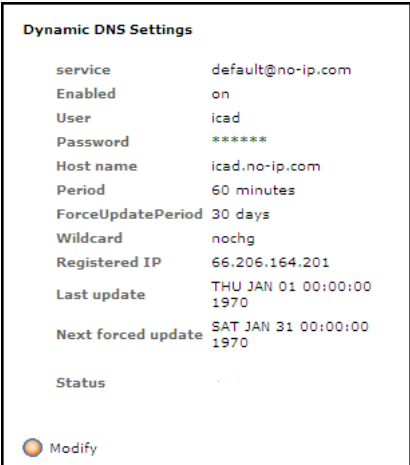
Configure the BSGX4e's dynamic DNS after opening an account with one of the qualified service providers. Click the **Modify** button in the display pane and fill in the fields as follows, click **Update** when finished:



<b>Service</b>	Select the service, from the pull-down list, with which you opened an account.
<b>Enabled</b>	Disabled by default. Select <b>yes</b> to enable.
<b>User</b>	The user name of the dynamic DNS account.
<b>Password</b>	The password of the dynamic DNS account.
<b>Host name</b>	Host name = user name + domain of the dynamic DNS account. user.domain@ext
<b>Period</b>	Refresh period. Update with current IP address if it does not match the registered IP address. Range is 10 to 1440 min. Default is 60.
<b>ForcedUpdate Period</b>	Forced refresh, whether or not IP address has changed, to avoid expiration of host name. Range is 24 to 35 days. Default is 30.
<b>Wildcard</b>	When enabled, resolves *.domain.ext to the same IP address as domain.ext. Wildcards must be enabled on both the server and client. Choices are: nochg – Use when wildcard is not enabled on server (default) on – Client enabled off – Client disabled

When configured and enabled, the display panel appears, similar to the Dynamic DNS Settings panel in the figure to the right.

Most of the fields are self-explanatory. The **Status** field displays the following comments:

- GOOD
- GOOD: Additional nochg updates cause the hostname to become blocked.
- ERROR: The hostname specified is not a fully-qualified domain name.
- ERROR: The hostname specified does not exist or is not in this user account.
- ERROR: The hostname specified does not exist or not in this user account.
- ERROR: When talking to IP server
- ERROR: The username and password pair do not match a real user.



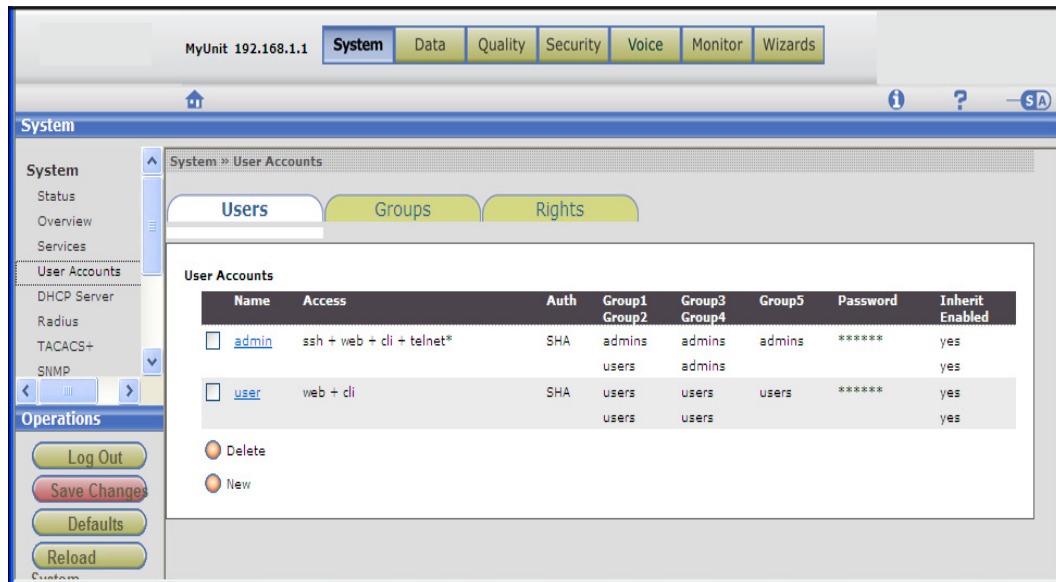
Dynamic DNS Settings	
service	default@no-ip.com
Enabled	on
User	icad
Password	*****
Host name	icad.no-ip.com
Period	60 minutes
ForceUpdatePeriod	30 days
Wildcard	nochg
Registered IP	66.206.164.201
Last update	THU JAN 01 00:00:00 1970
Next forced update	SAT JAN 31 00:00:00 1970
Status	
 Modify	



## User accounts page

This page is where you manage the user account security features of the BSGX4e. The user accounts determine who can access the BSGX4e and what permissions they are granted.

**Figure 5** User Accounts Page



## Technical reference

This section contains technical descriptions and reference information.

### Terminology

Terminology applicable to user accounts:

Access – How you connect to the BSGX4e: Web, CLI, SSH, Telnet, FTP

Authorization – log in security protocol: SHA, RADIUS, TACACS+

Rights – Operation permissions: read, write

## Default configuration

User interface with the BSGX4e is managed with *user accounts*, *user groups*, and *user rights*. The BSGX4e is delivered with following predefined configurations:

- **Two user groups** – One for administrators (`admins`) and one for other users (`users`). The `admins` user group is granted all access modes, and the `users` user group is granted only Web and CLI access.
- **Two user accounts** – One for administrators (`admin`) and one for other users (`user`). The `admin` account belongs to both predefined user groups (`admins` and `users`); the `user` account belongs only to the `users` user group. Access passwords are controlled in the user accounts.
- **Three rights identifiers** – One for the `admins` user group (`admin`) and the other two for the `users` user group (`useradv` and `userbasic`). These identifiers are displayed on the Rights tab page.

All rights are granted to `admins`; the two identifiers for the `users` user group grant read-only permission to some commands, and read + write permission to other commands. See [Table 4](#).

Each field on a Web UI page is a command parameter and the Update button executes the command. A command acts on a configurable parameter referred to as an “object.” Each object has an authority setting of either `Admins` or `Users`, which works with the rights identifier to determine the permissions being granted. See the next section for more detail.

---

**NOTE:** This predefined user management configuration cannot be deleted or renamed.

---

## Rights

Whether you have *read* or *read+write* permissions for each command is determined by the *rights identifier*, which assigns access modes based on a combination of the group and the object authority settings. Your user account determines to which group you belong, and the object authority is set at the factory. [Table 4](#) demonstrates this principle.

**Table 4** User rights permissions

Log in	Identifier	Group	Object	Permissions
admin	admin	admins	Admins	read+write
user	useradv	users	Admins	read
user	userbasic	users	Users	read+write

## Passwords

Passwords are set in the User Account configuration page.

You are advised to change the default passwords during setup of the BSGX4e. The default passwords are:

*admin* user = **admin**

*user* user = **netcat**

Password authentication can be internal (SHA) or external (RADIUS and TACACS+). For external authentication, you must also configure the RADIUS or TACACS+ client ([page 53](#)) after configuring the user account.

You can have a situation where the user account is set for SHA authentication, but the groups the user account belongs to are set for one of the external authentication servers. This does not create a conflict, even if the user account is configured to inherit the authorization properties from the group. The user can log in with either (SHA or external) password.

Users are allowed three log in attempts. After that, the console is locked against all log ins for 15 minutes or until the BSGX4e is power-cycled. All invalid log in attempts are recorded in the audit log.

The *admin* user can change the password on any user account that has internal authentication.

## Configuration

Perform the following steps to create new, or modify existing, user accounts, groups, and rights. You can create up to 20 user accounts and 10 user groups.

**NOTE:** If you are using RADIUS or TACACS authentication, read the section [RADIUS and TACACS+ on page 53](#) before configuring a user account here.

### System > User Accounts > Users tab

You can create up to 20 user accounts.

With the **Users** tab active on the User Accounts page, click **New** to create a profile.

To modify an existing profile, click the profile name, then click **Modify**.

To remove a user account, select the check box next to the account name, then click **Delete**. Note that you cannot remove the predefined *admin* and *user* accounts.

Name	Access	Auth	Group1	Group2	Group3	Group4	Group5	Password	Inherit Enabled
<input type="checkbox"/> admin	ssh + web + cli + telnet*	SHA	admins	admins	admins	admins	admins	*****	yes
<input type="checkbox"/> user	web + cli	SHA	users	users	users	users	users	*****	yes

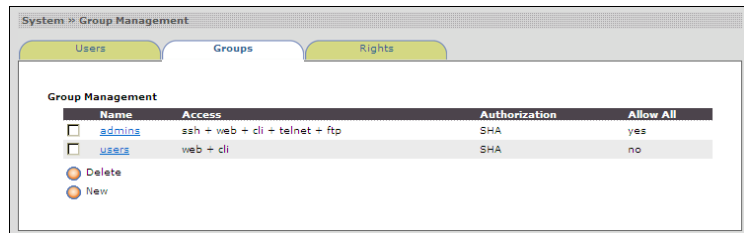
Fill in the fields as follows, click **Update** when finished:

<b>Name</b>	Log in name of new account being added, or modification of existing account.
<b>Access</b>	<p>Access methods allowed to this user:</p> <ul style="list-style-type: none"> <li>ssh – Secure Shell (SSH)</li> <li>Web – Web User Interface (Web UI)</li> <li>cli – Command Line Interface (CLI)</li> <li>telnet – Remote access through a Telnet session</li> <li>ftp – File Transfer Protocol (FTP)</li> </ul> <p>If you do not select any access methods, the access defined for the groups to which this user is assigned is used.</p>
<b>Auth</b>	<p>Internal or external password authorization:</p> <ul style="list-style-type: none"> <li>SHA – Internal authorization (Default)</li> <li>RADIUS – External authorization (<a href="#">page 53</a>)</li> <li>TACACS+ – External authorization (<a href="#">page 53</a>)</li> </ul> <p><b>NOTE:</b> For external authorization, you must also configure an authentication client profile. Follow the RADIUS and TACACS+ page links above.</p>
<b>Group1</b>	<p>Assign the user account to a user group. Group1 is required, all other groups are optional. A user can be assigned to up to five groups.</p> <p>Review the section <a href="#">Rights on page 42</a> to determine the appropriate group.</p>
<b>Group2 - 5</b>	<p>Optional additional user groups to which a user account can be assigned.</p> <p>To remove a user from a group, select <b>none</b> for the group parameter.</p>
<b>Password</b>	<p>The password for the user account.</p> <p>The authorization method (<b>Auth</b> field) determines whether the password is authenticated internally by the BSGX4e, or externally by a RADIUS or TACACS+ server. For external authentication, you must also configure an authentication client profile. See the links in the <b>Auth</b> field above.</p> <p>You can leave this field blank if you are using external authentication. However, you can create a password here that can be used if the external server cannot be reached.</p>
<b>Inherit</b>	<p>Whether or not the user account inherits access and authorization settings from the groups to which it belongs.</p> <p>Default is <b>yes</b>.</p>
<b>Enabled</b>	Whether or not the user account is enabled. Default is <b>yes</b> .

## System > User Accounts > Groups tab

With the **Groups** tab active on the User Accounts page, click **New** to create a profile.

To modify an existing profile, click the profile name, then click **Modify**.



To remove a group profile, select the check box next to the profile name, then click **Delete**.

Fill in the fields as follows, click **Update** when finished:

<b>Name</b>	Name of the new user group to be added or the existing user group to be modified.
<b>Access</b>	<p>Access methods allowed to user accounts in this group.</p> <p>A user account uses these access values only if its own access values are not specified, and the access values of any preceding groups in its group list are also not specified.</p> <ul style="list-style-type: none"> <li>ssh – Secure Shell</li> <li>Web – Web User Interface (Web UI)</li> <li>cli – Command Line Interface</li> <li>telnet – Telnet</li> <li>ftp – File Transfer Protocol</li> </ul>
<b>Authorization</b>	<p>Internal or external password authorization:</p> <p>A user account uses the authentication method specified here only if its own authentication method is not specified, and the authentication method of any groups in its group list are also not specified.</p> <ul style="list-style-type: none"> <li>SHA – Internal authentication (Default)</li> <li>RADIUS – External authentication (<a href="#">page 53</a>)</li> <li>TACACS+ – External authentication (<a href="#">page 53</a>)</li> </ul> <p>For external authentication, you must also configure an authentication client profile. Follow the RADIUS and TACACS+ page links above.</p>
<b>Allow All</b>	<p>Whether or not users associated with this group are allowed all rights, or held to only those defined on the Rights page.</p> <p>Default is <code>no</code>.</p>

## System > User Accounts > Rights

**NOTE:** The two permissions (Access mode) allowed are `read` and `write`. The `execute` permission is not used.

As explained in the section [Rights on page 42](#), the permissions for any given command are defined by the combination of the rights identifier and the object name in the command's authority parameter. Each page in the Web UI is the equivalent of a command.

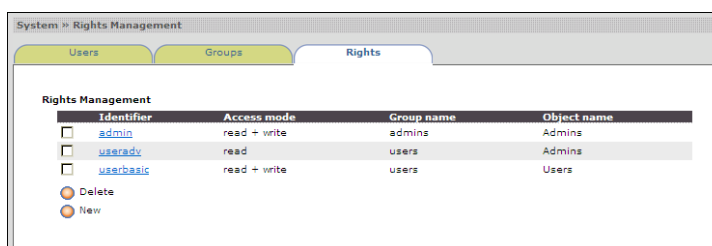
The three predefined identifier profiles and the groups to which a user account is assigned determines the rights that a user has. The default users, groups, and rights cover all usage scenarios. If you create new user accounts, you can copy these default configurations to accomplish the access, authorization, and rights combination you desire.

With the **Rights** tab active on the User Accounts page, click **New** to create a profile.

To modify an existing profile, click the profile name, then click **Modify**.

To remove an identifier, select the check box next to the identifier name, then click **Delete**. Note that you cannot remove the predefined `admin`, `useradv`, or `useradv` identifier.

Fill in the fields as follows, click **Update** when finished:



<b>Identifier</b>	Name for new identifier profile.
-------------------	----------------------------------

<b>Access mode</b>	Permissions granted by this record. Select all that apply. read – View data write – Change parameter values
--------------------	---

**NOTE:** `execute` is not used at this time

<b>Group name</b>	Name of the user group granted rights by this profile.
-------------------	--

<b>Object name</b>	Each object (command) has an authority field that is set to <b>Admins</b> or <b>Users</b> . Select the name that sets the desired permissions in conjunction with the user group that was selected:
--------------------	---

Group	Object	Permissions
admins	Admins	read+write
users	Admins	read
users	Users	read+write

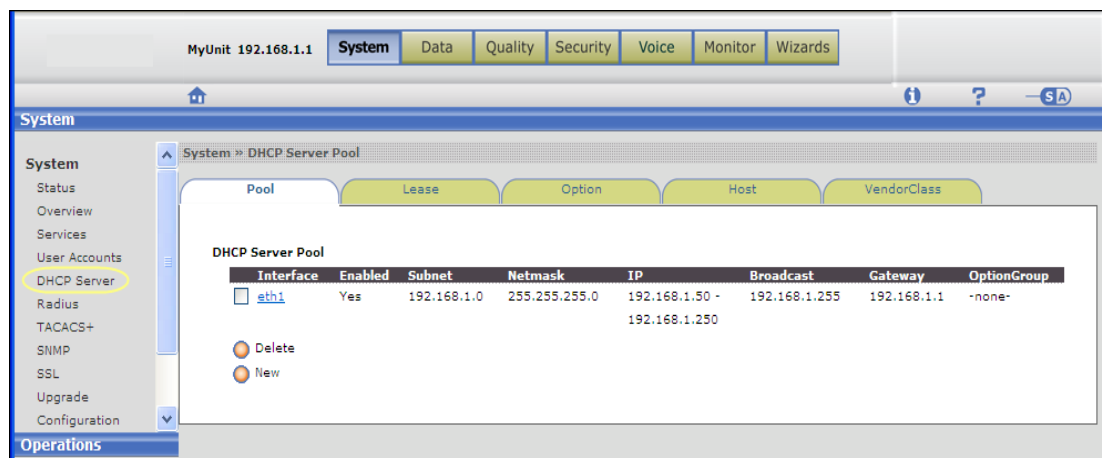
## DHCP server

The DHCP server in the BSGX4e provides dynamic IP addresses to hosts connected to its LAN ports. This service is enabled by default. Optionally, you can assign static addresses to LAN hosts.

For clarification, the BSGX4e also includes two other DHCP features:

- ❑ **DHCP relay** ([page 85](#)) – Rather than having the DHCP server providing addresses to LAN hosts, the relay service receives the host's DHCP request and proxies it to an external server. To the LAN hosts, the BSGX4e appears to be the server. To the external server, the BSGX4e appears to be the requesting host. You must disable the DHCP server to use the DHCP relay. The relay is disabled by default.
- ❑ **DHCP client** ([page 72](#)) – The DHCP client requests a dynamic address from an external server. The DHCP client can be enabled on either the WAN or LAN ports, but not both. It is most common on the WAN with interfaces that do not require a static IP address. The DHCP client can be enabled on the LAN if you have a DHCP server connected to the LAN.

**Figure 6** DHCP Server Pages



## Functional characteristics

The DHCP server, as implemented in the BSGX4e, has the following characteristics:

- ❑ Supports one address range per LAN interface (eth1 or vif*n*). Up to four virtual interfaces (vif) can be configured on the LAN ports, one on each port.
- ❑ Address range must be within the subnet of the interface.
- ❑ Up to four servers can be configured—one on each interface configured on the LAN ports.
- ❑ Up to 500 IP addresses can be configured on each server.
- ❑ Options can be enabled for each interface, vendor class, or MAC address.
- ❑ Lease information is saved in non-volatile memory so it can be retrieved immediately after a restart.
- ❑ The DHCP server relies on DNS for name/address translation. It connects to a DNS server through the DNS client ([page 36](#)), which must be appropriately configured.
- ❑ The DHCP relay ([page 78](#)) and DHCP client ([page 71](#)) must both be disabled on eth1 to implement the DHCP server.

## Configuration

Perform the following tasks to configure the DHCP server.

### System > DHCP Server > Pool tab

The DHCP server pool is where you configure the network parameters and assign an option group.

A DHCP pool is automatically created for the eth1 LAN interface when the BSGX4e is first initialized after bootup. IP addresses are leased from the address pool.

To create a new pool for a virtual (vif*n*) interface, click **New** to open the configuration page and fill in the fields as described below.

To modify an existing pool, click eth1/vif*n* in the display to open the properties page, then click **Modify** to open the configuration page.

You can delete interface profiles by activating the check box next to the profile on the display page, then click **Delete**.

Fill in the fields as follows, click **Update** when finished:



<b>[interface]</b> (1)	The BSGX4e interface for which the server supplies addresses. Default is eth1 (LAN).
<b>Enabled</b> (1)	Enables or disables the DHCP server for the designated interface. Default is enabled.
<b>Subnet</b> (1)	The subnet that is to be served. Must be a subnet of the interface. Default is 192.168.1.0.
<b>Netmask</b> (1)	The netmask for the subnet. Default is 255.255.255.0.
<b>IP</b> (1)	The beginning address for the range of IP addresses that the server can assign to hosts. Must be within the BSGX4e's subnet. Default is 192.168.1.50.
<b>(range to)</b> (1)	The ending address for the range of IP addresses. Default is 192.168.1.250.
<b>Broadcast</b>	The broadcast address for the subnet. Default is 192.168.1.255.
<b>Lease</b>	The length of lease. Range is 1-7 days. Default is 7.
<b>Gateway</b>	The network gateway address. Default is 192.168.1.1.
<b>OptionGroup</b>	The name of an option group to be sent to the host. Default is none.

(1) These fields are required. All remaining fields are populated with intelligent default values if left blank. These fields can be modified after initial creation.

## System > DHCP Server > Lease tab

This is a display-only page that shows the current leases.

The Expired field shows an asterisk (\*) if the current system time is greater than the end time of the lease. This indicates that the lease has expired.

The BSGX4e can accommodate a maximum of 500 leases for all pools.

## System > DHCP Server > Option tab

The Option page is where you create groups, configure options, and assign the options to groups. The option group can then be assigned to a specific interface, host, or vendor class as needed.

A DHCP option contains information that is sent to a LAN client when it is assigned an IP address by the DHCP server. It typically describes a network configuration and various services that are available on the network.

### **Functional characteristics**

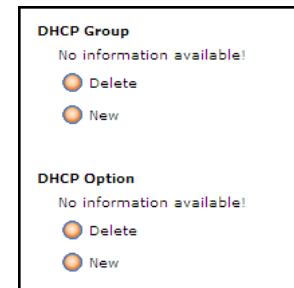
The Group/Option feature has the following characteristics:

- A group cannot be deleted if it is referenced by another configuration entry on the Pool or Host pages.
- A group cannot be renamed if it is referenced by another configuration entry on the Pool or Host pages.
- A group cannot be modified after being created. If you need to change the group option parameters, you must delete the option and create a new one.
- An option code can be assigned to different groups with the same or different value for each group.
- Multiple option codes can be assigned to the same group.
- A maximum of 32 groups can be created.

### Configuration

The Option page is divided into DHCP Group and DHCP Option sections, as shown here.

1. Click **New** under the **DHCP Group** heading and enter a name for the new group.
2. Click **New** under the **DHCP Option** and configure the parameters as follows:



<b>Id</b>	Enter a number. If you enter <b>new</b> , the next sequential number is automatically assigned.
<b>Group</b>	Select the group name to which you are applying an option.
<b>Code</b>	Select the option code to apply to the selected group.

<b>Value</b>	Enter an appropriate value for the selected code:
<b>bootfile-name</b>	Text. Identifies a bootstrap file.
<b>domain-name</b>	Text. The domain name the client must use when resolving host names through a DNS.
<b>domain-name-servers</b>	IP address. A list of DNS servers available to the client. Enter multiple servers separated by a comma (.). List the servers in order of preference. <b>NOTE:</b> Read the DNS entry under the <a href="#">Functional characteristics on page 48</a> for reference.
<b>nntp-servers</b>	IP address or domain name. A list of NTP (time sync) servers available to the client. Enter multiple servers separated by a comma (.). List the servers in order of preference.
<b>option-150</b>	IP address. Proprietary DHCP option. Location of a TFTP server for proprietary terminals (Cisco, for example).
<b>option-151</b>	IP address. Proprietary DHCP option. Location of a SIP server for proprietary terminals (Cisco, for example).
<b>option-160</b>	IP address. Proprietary DHCP option. Location of a TFTP server for proprietary terminals (Polycom, for example).
<b>option-161</b>	IP address. Proprietary DHCP option. Location of an FTP server for proprietary terminals (Polycom, for example).
<b>routers</b>	IP address or domain name. A list of routers on the client's subnet. Enter multiple routers separated by a comma (.). List the servers in order of preference.
<b>tftp-server-name</b>	IP address or text. Identifies a TFTP server. Supported by some DHCP clients, required by others.
<b>time-offset</b>	Time format in hours:minutes (HH:MM) or in seconds (NNNN). The time offset from Coordinated Universal Time (UTC). Specify time East of UTC as positive (+) and West as negative (–).

3. Click **Update** when finished.

## System > DHCP Server > Host tab

The configuration parameters on this page are optional. Use them to reserve a specific IP address for a given MAC address and assign an option group to that address.

Click **New** to open the configuration page.

You can modify existing host profiles by clicking the **Id** number on the display page.

You can delete host profiles by activating the check box next to the profile on the display page, then click **Delete**.

Fill in the fields as follows, click **Update** when finished:

<b>Id</b>	A unique identification number. Use “new” or enter a whole number.
<b>MACAddress</b>	The MAC address of the host.
<b>IPAddress</b>	The IP address to assign to this host. The address must be within the subnet defined for the interface.
<b>OptionGroup</b>	Choose an option group from the drop-down list. If you choose a different group than that assigned to the entire interface (Pool tab page), this setting overrides the interface setting for this specific host.
<b>Description</b>	Optional text to help identify the host.

## System > DHCP Server > VendorClass tab

The configuration parameters on this page are optional. Use them to assign an option group to a specific *vendor class* identifier of a LAN host. You can also specify an interface (physical or virtual) to further define the option group application. The option group can be applied only to the specified vendor class on the specified interface.

Click **New** to open the configuration page.

You can modify existing host profiles by clicking the **Id** number on the display page.

You can delete host profiles by activating the check box next to the profile on the display page, then click **Delete**.

Fill in the fields as follows, click **Update** when finished:

<b>Id</b>	A unique identification number. Use “new” or enter a whole number.
<b>VendorClass</b>	The vendor class of the host device. This data is in the vendor’s documentation or on their Web site.
<b>Interface</b>	The interface (optional). Default is <b>none</b> .
<b>OptionGroup</b>	Choose an option group from the drop-down list. This assignment applies only to this vendor class. This setting overrides the interface setting for this vendor class

---

## RADIUS and TACACS+

The BSGX4e includes both the Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+) clients to establish external authentication security, rather than using the default internal SHA method. To use either service, you must first establish an account on a RADIUS or TACACS+ server. That can be your company's server or a commercial service provider.

These clients provide external password authentication by sending the log in password to an external server for authentication. The default SHA uses authentication internal to the BSGX4e.

### Technical reference

The process to establish RADIUS or TACACS+ authentication is as follows:

1. Establish an account on the RADIUS or TACACS+ server. The account information you receive must include the server address, user name, secret key, and password.
2. Create a new user account or modify an existing account (see [User accounts page on page 41](#)).

On the user account configuration page:

The user name must be the same as for the RADIUS or TACACS+ account.

Select RADIUS or TACACS+ for the authorization field.

The password field is optional, since the external account password is actually used for log in. A password entered here is used as backup if the external server cannot be reached.

3. On the RADIUS or TACACS+ configuration pages:

Select the user for which the RADIUS or TACACS+ account was established.

Enter the RADIUS or TACACS+ server IP address and the secret key.

The authentication clients in the BSGX4e have the following characteristics:

- Any user account that specifies RADIUS or TACACS+ for remote authentication uses the password from the authentication server. If the server cannot be reached, the password defined in the BSGX4e user account is used.
- Authentication records are mapped to users by their user account name. Every user account that specifies external authentication must have its own authentication record. Up to twenty authentication records can be referenced.
- Disabling an authentication record suspends authentication for the corresponding user account. This prevents log ins by the user account until either its authentication record is re-enabled or its authentication method (Auth field) is changed.
- Deleting a user account also deletes its authentication record.
- Clients are compatible with standard RADIUS or TACACS+ servers.
- Normal operation fully encrypts the body of the packet for secure communication. TACACS uses TCP port 49 for transport; RADIUS use UDP ports 1812 and 1813.
- Client activity is reported in the system log ([page 30](#)).

## Configuration

Perform the following steps to create a RADIUS or TACACS+ authentication record.

**NOTE:** A user account ([page 43](#)) must be configured for external authentication before the corresponding authentication record is created.

### System > Radius

The Radius page displays existing authentication records and contains the buttons for adding a new record or deleting an existing record.

Every authentication record that accesses the same RADIUS server must specify the same field values, except for the **User** and **Secret** fields.

To configure a RADIUS authentication record, click **New** to open the configuration page.

You can modify an existing profile by clicking the **User** name on the display page.

You can delete a profile by activating the check box next to the profile on the display page, then click **Delete**.

Fill in the fields as described here, click **Update** when finished:

<b>User</b>	The user account to which the authentication record applies. The user account must specify <b>Radius</b> authentication.
<b>Enabled</b>	Enable /disable the Radius client. The default is <b>no</b> (disabled).
<b>Automatic</b>	Automatically binds the client to the interface specified in the <b>Interface</b> field. Select <b>yes</b> if DHCP is in use. The default is <b>no</b> (no binding).
<b>Auth</b>	FQDN or IP address of the Radius authorization server that the client uses.
<b>Secret</b>	Shared secret the client uses for security.
<b>Bind</b>	Binding IP address for the client. The IP address of the interface that the server references. Typically, this is the IP address of the WAN interface. Specify this value only if DHCP is <i>not</i> in use.
<b>Interface</b>	Physical interface through which RADIUS communicates if the <b>Automatic</b> field is <b>yes</b> . eth0 = WAN To clear the parameter, specify <b>none</b> .

## System >TACACS+

The TACACS+ page displays existing authentication records and contains the buttons for adding a new record or deleting an existing record.

Configure a TACACS+ authentication record, click **New** to open the configuration page.

You can modify an existing record by clicking the **User** name on the display page.

You can delete a record by activating the check box next to the profile on the display page, then click **Delete**.

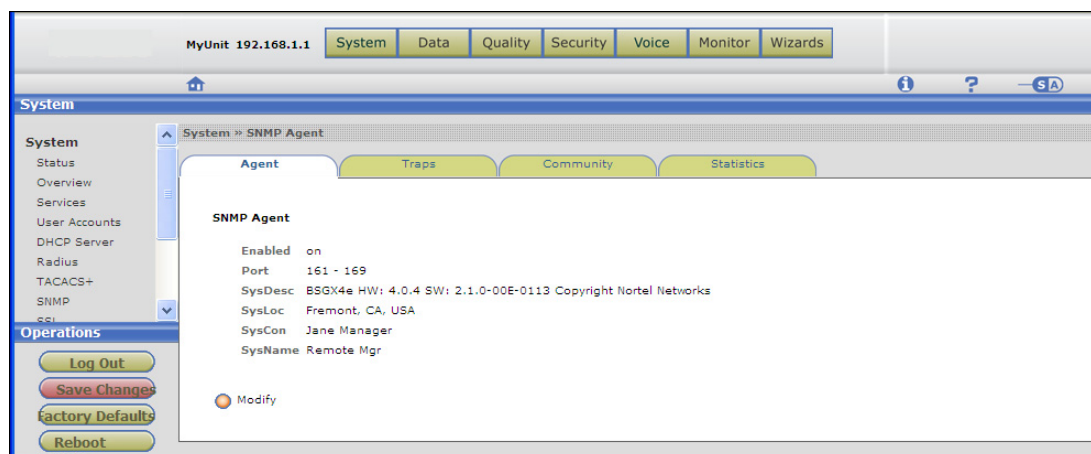
Fill in the fields as described here, click **Update** when finished:

<b>User</b>	The user account to which the authentication record applies. The user account must specify TACACS+ authentication.
<b>Enabled</b>	Enable /disable the TACACS+ client. The default is <b>no</b> (disabled).
<b>Server</b>	IP address or FQDN of the TACACS+ server that the client uses.
<b>Key</b>	Shared key for the client as determined by the server. If the key includes a space character, enclose the entire value in double-quotes (" ").

## SNMP

The BSGX4e contains an SNMP agent that allows for remote monitoring. The BSGX4e cannot be configured through SNMP in the current version.

**Figure 7** SNMP agent configuration



SNMP uses a Management Information Base (MIB) database. The MIBs are described in IETF RFC 1213. SNMP traps are supported.

The SNMP agent replies only to SNMP version 2c requests. Apart from the system group, which can be configured with write permissions, all MIBs are in read-only mode in this version.

The SNMP agent sends the following traps:

<b>ColdStart</b>	The BSGX4e has restarted
<b>WarmStart</b>	SNMP agent has restarted
<b>LinkUp</b>	An interface has become active
<b>LinkDown</b>	An interface has become inactive
<b>Authentication Fail</b>	SNMP authentication has failed (such as when the wrong community name is used)

SNMP traps are sent on port 162; this cannot be changed. Port 161, used by the SNMP agent, must be open in the firewall to allow access for SNMP clients to reach the agent. See [SNMP security policy on page 127](#).



## Configuration

The SNMP agent is enabled by default but not configured. Traps are disabled by default, and no community is configured.

### System > SNMP > Agent tab

Click **Modify** to configure the SNMP agent:

<b>Enabled</b>	Enables the agent (boolean). The agent is initially enabled.
<b>Port</b>	Port on which the agent listens. The default is port <b>161</b> .
<b>(range to)</b>	DO NOT USE. This field is removed in the next release.
<b>SysLoc</b>	SNMP system location (sysLocation MIB); physical location of the hardware.
<b>SysCon</b>	SNMP system contact (sysContact MIB); contact person for this hardware.
<b>SysName</b>	SNMP system name (sysName MIB); administrator assigned to this hardware.

The display page contains a **SysDesc** field that is read-only. It reports basic hardware and software versions of the host that is running the BSGX4e.

### System > SNMP > Traps tab

Click **Modify** to configure SNMP traps:

<b>Enabled</b>	Enable/disable transmission of traps. Default is <b>no</b> (disabled).
<b>Comm</b>	The community string to authenticate access.
<b>IP</b>	IP address of the management station that receives traps.
<b>(range to)</b>	DO NOT USE. This field is removed in the next release.

### System > SNMP > Community tab

Click **New** to add an SNMP community:

<b>Community</b>	The community string. Used to authenticate access permission.
<b>IP</b>	IP address of the management station that sends SNMP requests.
<b>Access</b>	Select <b>read</b> or <b>read-write</b> .

## System > SNMP > Statistics tab

The statistic page is a read-only display of the SNMP agent performance. You can update the display with the **Refresh** button, and delete accumulated statistics with the **Clear** button.

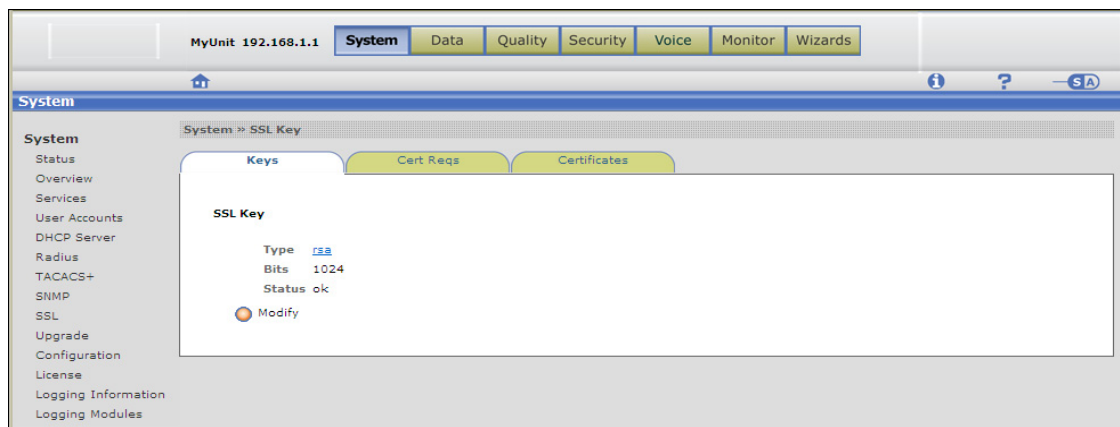
Field definitions are as follows:

Out Pkts	Total number of Out SNMP messages.
In Pkts	Total number of In SNMP messages.
In BadCommunityNames	Total number of In messages with an unknown community name.
In BadVersions	Total number of In messages with an unsupported SNMP version.
In ASNParseErrs	Total number of In messages with ASN.1/BER errors.
In BadCommunityUses	Total number of In messages with a disallowed operation.
In NoSuchNames	Total number of In messages with “noSuchName” in error-status field.
In Toobigs	Total number of In messages with “tooBig” in error-status field.
In GenErrs	Total number of In messages with “genErr” in error-status field.
In ReadOnlys	Total number of In messages with “readOnly” in error-status field.
In TotalSetVars	Total number of Set-Request PDUs processed successfully.
In TotalReqVars	Total number of Get-Request and Get-Next PDUs.
In GetNexts	Total number of Get-Next PDUs.
In GetRequests	Total number of Get-Request PDUs.
In GetResponses	Total number of Get-Response PDUs.
In SetRequests	Total number of Set-Request PDUs.
Out TooBigs	Total number of Out Messages with “tooBig” in error-status field.
In Traps	Total number of SNMP Trap PDUs accepted and processed.
Out GenErrs	Total number of Out Messages with “genErr” in error-status field.
Out NoSuchNames	Total number of Out Messages with “noSuchName” in error-status field.
Out GetNexts	Total SNMP Get-Next PDUs generated.
Out GetRequests	Total SNMP Get-Request PDUs generated.
Out GetResponses	Total SNMP Get-Response PDUs generated.
Out SetRequests	Total SNMP Set-Request PDUs generated.
Enable AuthenTraps	Permission to generate authentication-failure traps, enabled (1), disabled (2).
Out Traps	Total SNMP Traps generated.
Silent Drops	Total number of In PDUs silently dropped.

## SSL

This section describes configuring the Secure Socket Layer (SSL). SSL provides a secure connection to any device contacting the BSGX4e on well-known port 443 with TCP protocol. This applies primarily to the WAN interface, but is also applicable to the LAN interface. Traffic over an SSL connection is encrypted and authenticated to prevent eavesdropping, tampering, or forgery.

**Figure 8** SSL configuration



The BSGX4e has a private SSL key, a certificate signing request (CSR), and a certificate by default. You can normally create a new key (and accompanying certificate) only if the existing key's security has been compromised.

## Application notes

The Web UI accommodates one key and certificate. You cannot delete these in the Web UI. However, you can cause a new key or certificate to be generated by modifying the key or CSR profile.

- If you modify the key profile, a new key is generated, and a new CSR is generated.
- If you modify the CSR profile, a new request is generated.

You can also delete the key, certificate request, and certificate with the Command Line Interface (CLI) console:

```
del ssl key rsa
del ssl csr x509
del ssl cert x509
```

Then, the steps for a new SSL configuration are:

- a.** Generate a new SSL key with the default values.  
On the **Keys** tab, click **Modify** then **Update**.
- b.** Generate a new SSL CSR.  
On the **Cert Req** tab, click **Modify** then **Update**.
- c.** Generate or import the SSL certificate.  
On the **Certificates** tab, click **Modify** then **Update**.

During the time that a profile is being regenerated, a new SSL connections cannot be established. The **Status** field on the **Keys** page displays **generating** during the generation process, and displays **OK** when the process completes. The **Cert Reqs** and **Certificates** tabs also have a status field.

## Configuration

As explained above, the default SSL configuration is applicable in most situations. This section explains the configuration parameters in those situations where you need to regenerate a key or a certificate, or a key and a certificate.

Any modification to the Keys or Cert Reqs profile causes regeneration.

### System > SSL > Key tab

The BSGX4e has a private SSL key by default, which is randomly-seeded, 1024-bit, and RSA encrypted. Normally, a new private key does not need to be generated unless the security of the existing key had been compromised.

The process for generating a new key can take several minutes depending on the size of the key. When key generation starts, the key used by the SSL server is deleted and a new SSL connection cannot be created until a new key is available. When key generation completes, the key used by the SSL server is set to the newly generated key. New SSL connections can then be created.

To generate a new key, click the **Modify** button on the **Keys** tab page and change the **Bits** parameter (the only parameter you can modify). Modifying this profile causes a new key to be generated. Alternately, use the CLI command **del ssl key rsa**.

<b>Type</b>	Type of encryption. The BSGX4e uses only RSA.
<b>Bits</b>	Number of bits in key ( <b>512</b>   <b>768</b>   <b>1024</b>   <b>2048</b> ). Default is 1024

## System > SSL > Cert Reqs tab

This page is where you can create a new Certificate Signing Request (CSR), if needed. A valid key must first be configured.

A CSR exists by default. It is an X509 certificate and is self-signed by the SSL module.

To generate a new CSR, modify any of the parameters on this page. Alternately, you can delete the CSR with the CLI command **del ssl csr x509**. Then, come back to the **Cert Req** tab and click the **Modify** and **Update** buttons to regenerate the default profile.

The fields on the CSR configuration page are self-explanatory.

The **Status** field on the tab page displays the following:

<b>no key</b>	There is no SSL key.
<b>waiting for key generator...</b>	The certificate request is being generated.
<b>ok</b>	Generation is complete; an SSL key is available. The <b>PEMData</b> field shows the actual CSR in the standard PEM format.

The **PEMData** field on the tab page displays the certificate request. This can be the self-signed certificate generated by the SSL module, or it can be a certificate signed by an external certificate authority.

## System > SSL > Certificates tab

This page is where you designate the certificate as self-signed, or you import an external certificate. You must have generated a key and a CSR before enacting this page.

If a new key and CSR has been generated, click the **Modify** then **Update** buttons to set this page to its defaults, which is a self-signed certificate generated by the SSL module.

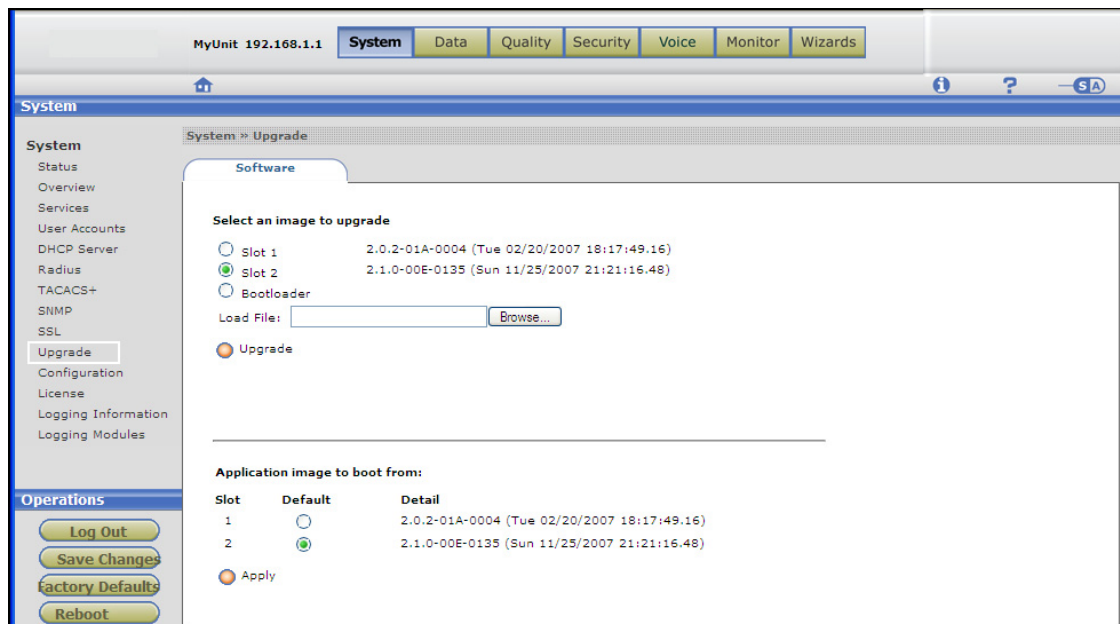
The only parameter you can set on the configuration page (**Modify** button) is the **Signed** field. Your choice are **self** and **NULL**.

- ❑ The default is **self** for a self-signed certificate.
- ❑ Select **NULL** if you have a certificate from an external certificate authority.

The certificate must be in PEM format with no header before the “----- BEGIN CERTIFICATE -----” phrase. Copy the certificate text and paste it into the **Certificate** text box. The certificate is checked to ensure it is in the correct PEM format. If the format is incorrect, the certificate is rejected, an error message displays, and the **Status** field on the tab page shows *invalid certificate*.

# Upgrade

**Figure 9** Upgrade system image



Use the Upgrade page to import new system software image files and bootloader files. You can store two image files and define which to use for booting the system.

The manual configuration and user settings you made persist through an image upgrade.

You acquire system update files at Nortel's support Web site.

## System > Upgrade

Perform the following steps to import a new software image:

1. Acquire the new image file and store it on the PC connected to the BSGX4e.
2. In the upper panel, select the slot in which to load the new image. Normally, this is the slot that is not currently in use. In the lower panel, the slot to boot from is automatically detected as the slot to which the new image was loaded.
3. Use the **Browse** button to navigate to the file stored in [Step 1](#).
4. Click the **Upgrade** button. The importing process takes a few minutes. You are notified when it is finished, and prompted to reboot the system.

Perform these steps to import a new bootloader file:

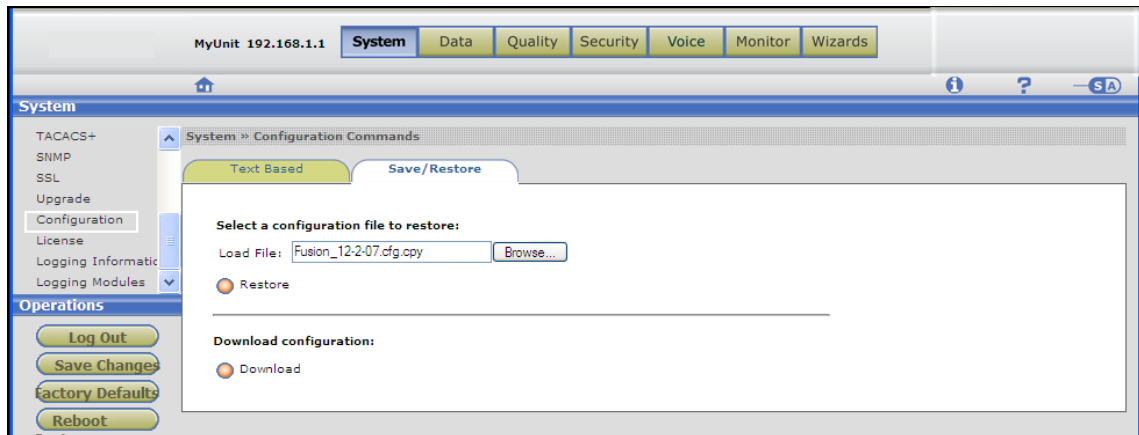
1. Acquire the bootloader file and store it on the PC connected to the BSGX4e.
2. Use the **Browse** button to navigate to the file stored in [Step 1](#).
3. Click the **Upgrade** button. You are notified when it is finished.

## Configuration

The Configuration page has two tabs:

- ❑ **Text Based** shows a display of the current user configurations. These are listed as CLI commands.
- ❑ **Save/Restore** is where you import and export a configuration file.

**Figure 10** Configuration file Save/Restore



**Best practises:** After performing any manual configurations, save the changes, export a configuration file and store it outside of the BSGX4e so that you can re-import the configuration in the event of an emergency recovery.

## System > Configuration > Save/Restore

### Save

To save a file with the current configuration settings, click the **Download** button. You are prompted to select the storage location on the PC connected to the BSGX4e.

### Restore

Perform the following to restore a configuration using a saved configuration file:

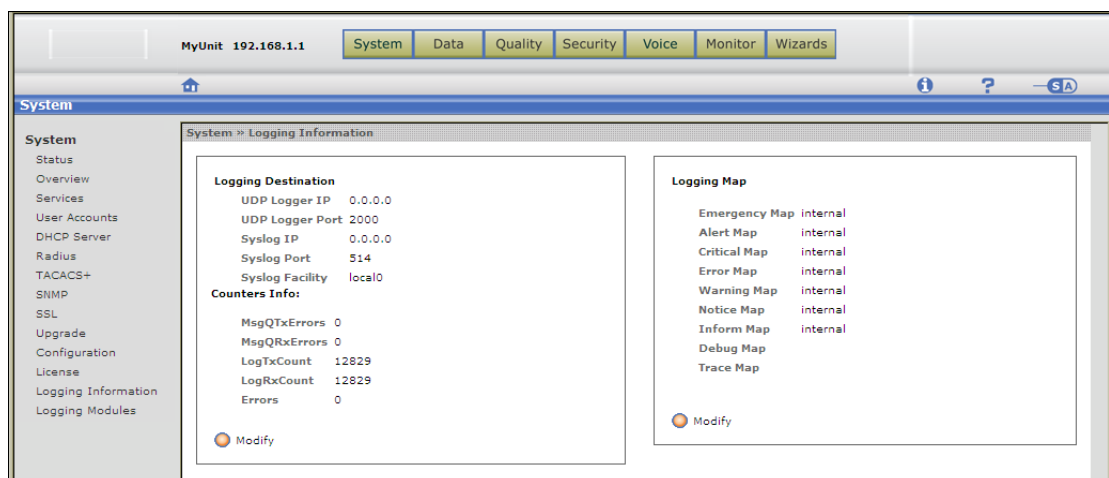
1. Ensure the target configuration file is on the PC connected to the BSGX4e.
2. Click **Browse** and navigate to the configuration file.
3. Click the **Restore** button to import the configuration.
4. **Reboot** the system to implement the configuration. Changes are saved automatically in this process.

## License

This is a display page that lists the copyrights of other companies' products used in the BSGX4e.

## Logging information

**Figure 11** Logging information



The BSGX4e logs event and error messages to various internal and external destinations. Most of these logs are intended to assist in troubleshooting during a technical support session and do not provide useful information for normal operations. If you need to contact technical support, it is important to provide both system information and hardware information about the unit. This information is displayed at [System > Overview > System Information panel on page 32](#).

However, the system (internal) log displays its most recent entries at [System > Status > System Log panel on page 30](#).

The Logging Information page allows you to configure the destination of each message type (based on severity level) and the network configuration for external destinations. It also displays logging statistics (Counters Info).



## System > Logging Info > Logging Destination panel

This panel is where you configure the external server to receive UDP and/or syslog messages. Log messages are compliant with the syslog protocol. The UDP section can also be configured to send raw UDP messages to a PC that is reachable from the BSGX4e.

External logging is not configured by default. Click the **Modify** button to open the configuration page:

<b>UDP Logger IP</b>	For messages with <b>UDP</b> destination. <b>NOTE:</b> This is for customer support and factory use. The destination must be running a UDP logger.
<b>UDP Logger Port</b>	For messages with <b>UDP</b> destination. Port of the receiving UDP logger. Default is 2000.
<b>Sys log IP</b>	For messages with <b>syslog</b> destination. IP address of a receiving Syslog logger.
<b>Syslog Port</b>	For messages with <b>syslog</b> destination. Port of a receiving Syslog logger. Default is 514.
<b>Syslog Facility</b>	For messages with <b>syslog</b> destination. Syslog facility to use: <b>local<math>n</math></b> , where $n$ is 0-7.

## System > Logging Info > Counters Info panel

These are read-only fields that display the following information:

<b>MsgQTxErrors</b>	Number of errors when sending to a message queue.
<b>MsgQRxErrors</b>	Number of errors when receiving from a message queue.
<b>LogTxCount</b>	Number of messages sent.
<b>LogRxCount</b>	Number of messages received.
<b>Errors</b>	Number of generic errors from the logging system.

## System > Logging Info > Logging Map panel

This page is where you configure each message type for one or more destinations, or no destination. As described in the next section, each functional module in the BSGX4e can be configured for which message types it sends. Message types are defined by severity level.

Click the **Modify** button to open the configuration page. Each message type can be configured for the following destinations:

<b>Console</b>	<p>Messages are displayed on the RS-232 console. This applies whether or not you are logged in to the CLI.</p> <p><b>NOTE:</b> Excessive messages to the console can prevent you from entering CLI commands.</p>
<b>UDP</b>	<p>Messages are sent in raw UDP format to the UDP logger specified in the <a href="#">System &gt; Logging Info &gt; Logging Destination panel</a> of this page.</p> <p><b>NOTE:</b> This is for customer support and factory use. The destination server must have a UDP logger.</p>
<b>Syslog</b>	<p>Messages are sent in syslog format to the syslog logger specified in the <a href="#">System &gt; Logging Info &gt; Logging Destination panel</a> on this page.</p>
<b>Internal</b>	<p>Messages are stored in an internal buffer of limited size, filled in FIFO order, but irretrievable after the unit restarts. The messages are displayed in the <a href="#">System &gt; Status &gt; System Log panel</a>.</p>
<b>File</b>	<p>Messages are stored in an internal file of limited size, filled in FIFO order, and retrievable after the unit reboots. The contents are the same as the System Log display on the Status page.</p> <p>These logs are also saved in the compact flash in the /cf0usr/log directory. A directory is created for each day and includes one or several log files. Files can be exported to an external device using SFTP. Files can be viewed using the following Unix commands through a CLI terminal:</p> <pre>BSGX4e&gt; cd log BSGX4e&gt; ls .. 2008-01-09 2008-01-10 BSGX4e&gt; cd 2008-01-09 BSGX4e&gt; ls .. 0 1 BSGX4e&gt; cat 1 15:21:27: No need to upgrade ids-hw for s/w version 2.1 15:21:30: DHCPSP: no vendor fixing 15:21:30: Using system DNS <i>display continues</i></pre>

[Table 5](#) describes the message severity levels and shows the default destinations.

**Table 5** System message severity

Severity Level	Message Level	Description	Default Destination
0	Emergency	Emergency operation error	Internal buffer.
1	Alert	Alert level operation error	Internal buffer.
2	Critical	Critical operation error	Internal buffer.
3	Error	Low-level operation error	Internal buffer.
4	Warning	Warnings, such as a system attack.	Internal buffer.
5	Notice	Notices	Internal buffer.
6	Inform	Informative messages	Internal buffer.
7	Debug	Debug messages, such as receipt of a SIP signaling packet.	Not logged.
8	Trace	Trace messages	Not logged.

## Logging modules

This page lists the functional modules in the BSGX4e and shows which message types are mapped to that function.

This page is intended to be used only for troubleshooting during a technical support session. You may be directed by the support technician to change the severity mapping, or to change the destination mapping (previous section).



**CAUTION:** Do not change the severity mapping unless so directed by technical support personnel. Enabling the `debug` and `trace` messages degrades system performance.

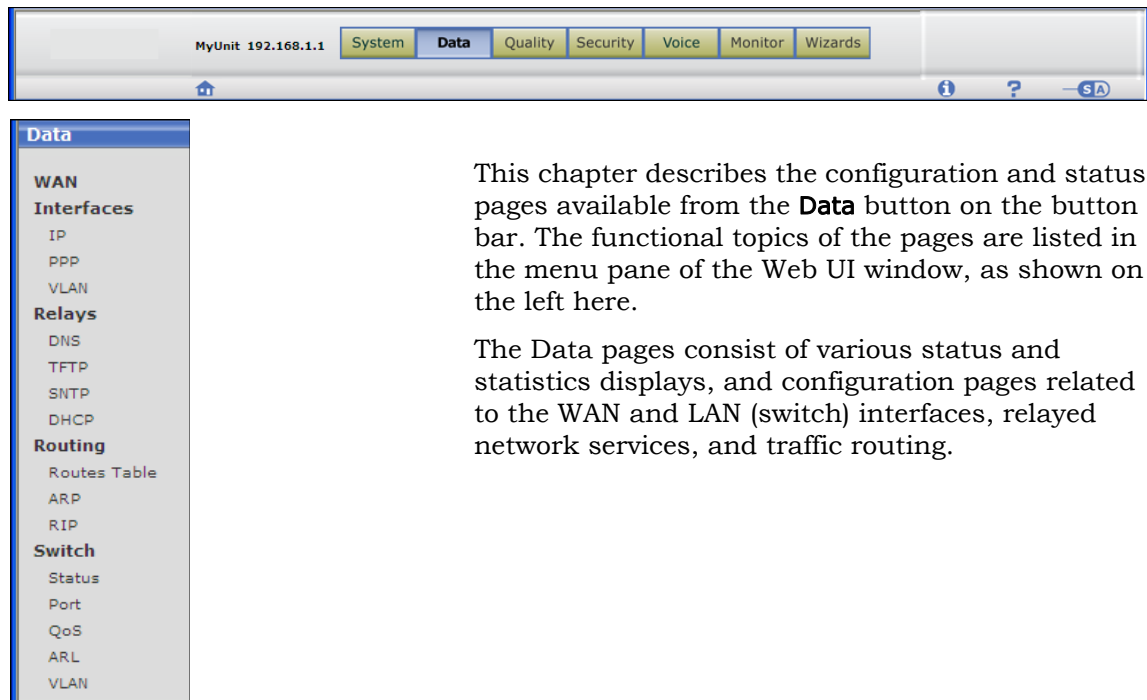
To change the message mapping of any function:

1. Click the module name in the display panel to open the properties page.
2. Click the **Modify** button to open the configuration page.
3. Enable or disable the desired message types and click **Update** when finished.

**NOTE:** Changes are not persistent. Any changes you make are reverted to the default settings with the next reboot.



## 3 DATA PAGES



The Data menu provides the following functions:

- **WAN** ([page 70](#))  
Configure the physical parameters of the WAN interface.
- **Interfaces** ([page 70](#))  
Configure the various interfaces that can be associated with the WAN and LAN ports.
- **Relays** ([page 78](#))  
Configure DNS, TFTP, SNTP, and DHCP relays for LAN devices.
- **Routing** ([page 86](#))  
Display ARP table; add static routes; configure proxy ARP; enable RIP daemon.
- **Switch** ([page 95](#))  
Display LAN switch status; configure LAN ports; set up layer 2 QoS; map MAC addresses to ports; configure VLAN on the LAN switch.

## WAN

This section is where you configure the BSGX4e network (WAN) interface. Your choices are:

- ☐ Ethernet (eth0) [default]
- ☐ PPP (pppn)
- ☐ VLAN (vifn)

The BSGX4e has an eth0 interface configured by default. To modify this interface or to add the other interface types, see the next section, [Interfaces](#).

## Interfaces

The Interfaces section is where you configure the WAN and LAN interface protocols. You can configure the following interfaces on the BSGX4e:

**Table 6** WAN interfaces

BSGX4e
IP over Ethernet (ethn)
PPP over Ethernet (pppn)
VLAN (vifn)
IP over VPN (vpnn)

## Data > Interfaces > IP page

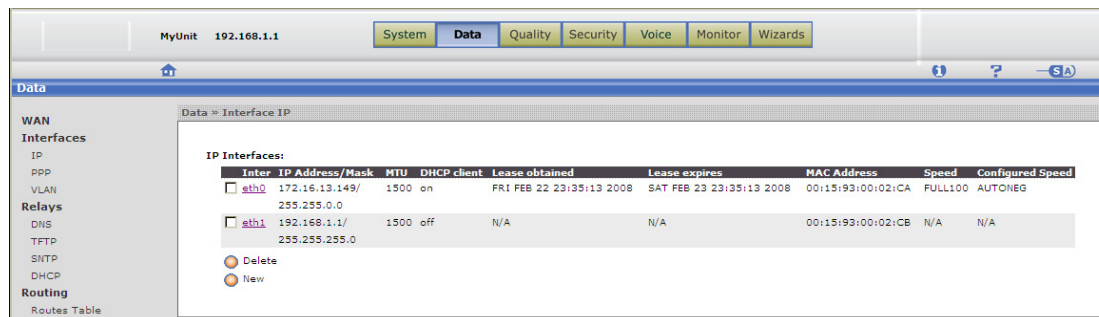
BSGX4e proprietary interface terminology:

eth0 – WAN

eth1 – LAN

This page is where you configure a WAN or LAN IP interface and view configuration data. The BSGX4e has an eth0 and eth1 interface by default.

**Figure 12** IP Interface display pages



## IP display pane

The display pane ([Figure 12](#) above) shows the parameters of each WAN or LAN interface. This is also where you configure new interfaces and delete existing entries.

Most of the fields are self-explanatory. Below are a few fields that need some explanation:

- The **Lease obtained** and **Lease expires** columns display **N/A** if DHCP is off or DHCP has not assigned an IP address to eth0. Otherwise, the columns describe the DHCP lease for the IP address assigned.
- The **Speed** column reports the current negotiated speed for eth0:
  - ❑ **FULL100** – 100 Mbps, full duplex mode
  - ❑ **HALF100** – 100 Mbps, half duplex mode
  - ❑ **FULL10** – 10 Mbps, full duplex mode
  - ❑ **HALF10** – 10 Mbps, half duplex mode
- The **Configured Speed** column reports the speed setting in the eth0 configuration: either **AUTONEG** (auto-negotiation enabled) or a specific speed and duplex mode (**FULL100**, **HALF100**, **FULL10**, or **HALF10**).

## IP configuration

To configure a new interface, click **New** to open the configuration page. Fill in the fields as shown below. Click **Update** when finished.

To modify an existing interface, click the **Inter** designator in the display to open the Properties page, then **Modify** to open the configuration page.

To delete an entry, enable the check box next to the **Inter** designator on the display page, then click **Delete**.



**CAUTION:** Do not configure a PPP interface as an IP interface. The PPP profile ([page 73](#)) creates the ppp0 interface.

<b>Interface value</b>	Select the interface to be configured. This is applicable to eth(n), vif(n), and vpn(n) interfaces.
<b>IP Addr/mask</b>	You can specify a static address/mask using dotted-decimal or CIDR notation (for example, 192.168.15.33/255.255.255.0 or 192.168.15.33/24). You must disable the DHCP client if you specify a static address on an interface. Virtual interfaces (vifn and vpn) require a static address.
<b>MTU</b>	Maximum Transmission Unit (MTU) of the interface (in bytes). This sets the maximum packet size. Default is <b>1500</b> bytes.
<b>DHCP client</b>	Enable/disable the DHCP client ( <b>on</b>   <b>off</b> ). Default for eth0 is <b>on</b> . Default for eth1 is <b>off</b> . The DHCP client is off by default when creating a new interface. (See the <a href="#">DHCP client</a> section below for more discussion.) See the notes for the <b>IP Addr/Mask</b> field above.
<b>Status</b>	Whether the interface is enabled or disabled ( <b>up</b>   <b>down</b> ). Default is <b>up</b> .

---

<b>Speed</b>	<p>Applicable only to the eth0 interface on the BSGX4e.</p> <p>Whether the speed and duplex mode for the interface is auto-negotiated or explicitly specified.</p> <p>For auto-negotiation, choose <b>Auto</b> (default).</p> <p>To specify speed and duplex mode, select:</p> <p><b>10Half</b> – 10 Mbps, half duplex</p> <p><b>10Full</b> – 10 Mbps, full duplex</p> <p><b>100Half</b> – 100 Mbps, half duplex</p> <p><b>100Full</b> – 100 Mbps, full duplex</p>
--------------	--

---

### **DHCP client**

The DHCP client obtains a dynamic address from an external server for the interface on which the client is enabled. The client can be enabled on either the WAN or LAN interface, but not both.

Enable the DHCP client on the LAN if you have a DHCP server on the LAN.

The DHCP client is enabled on the WAN by default for the Ethernet interface of the BSGX4e, and it is disabled for all other interfaces. This information is summarized in [Table 7](#).

**Table 7** DHCP client status by interface

DHCP disabled	DHCP enabled
	Ethernet (ethn)
PPP(pppn)	
VLAN (vifn)	
VPN (vpnn)	

In addition to the DHCP client, the BSGX4e also has a DHCP server for the LAN ([page 47](#)) and a DHCP relay that proxies requests from the LAN to an external server ([page 85](#)). You can apply only one of these three services to any given interface, the other two must be disabled.

### **IP statistic**

Each configured IP interface has a tabbed page that displays performance statistics. Access this page by clicking the **Inter** designator in the display pane, then click the **Statistics** tab.



## VLAN configuration

As part of the VLAN configuration process, the Data > Interfaces > IP page is where you configure the virtual interface (vifn) as an IP interface.

**NOTE:** You must have created the virtual interface before performing this task. See [Data > Interfaces > VLAN on page 75](#) for VLAN process details.

### Procedure:

Follow the instructions under the [IP configuration](#) heading above.

- ❑ Select vifn from the Interface drop-down list on the configuration page.
- ❑ Assign an IP address.
- ❑ Create firewall security policies for the vifn interface. See [VLAN security policies on page 127](#).

## Data > Interfaces > PPP page

You can configure the BSGX4e to use a PPP link as its primary WAN interface. It is designated as PPPoE on the BSGX4e. After the PPP profile is created you can view it as the pppn interface in the Data > Interfaces > IP display.

**Figure 13** PPP interface page

**Data > PPP**

PPP Profiles:

Profile	Interface	L2Interface	Active	SelfIP	AuthProto	MRU	MTU	RestartTime	ServiceName	Username	Password	LinkStatus
<input type="checkbox"/> 0	ppp0	eth0	yes	0.0.0.0/ 255.255.255.255	PAP	1492	1492	3000	PPP Serv	uname	*****	Activating

☐ Delete  
☐ Refresh

**Data > Interface IP**

IP Interfaces:

Inter	IP Address/Mask	MTU	DHCP client	Lease obtained	Lease expires	MAC Address	Speed	Configured Speed
<input type="checkbox"/> eth0	10.10.10.10/ 255.255.255.0	1500	off	N/A	N/A	00:15:93:00:02:CA	HALF10	AUTONEG
<input type="checkbox"/> eth1	192.168.1.1/ 255.255.255.0	1500	off	N/A	N/A	00:15:93:00:02:CB	N/A	N/A
<input type="checkbox"/> ppp0	0.0.0.0/ 0.0.0.0	1500	off	N/A	N/A	00:15:93:00:02:CA	N/A	N/A

☐ Delete  
☐ New

PPP establishes the session between the BSGX4e and your service provider using its own Link Control Protocol.

The BSGX4e's PPP client discovers and authenticates a PPP access concentrator and negotiates parameters, including an IP address, to establish the PPP link. The client supports a single PPP session and is compliant with RFC 1661 (PPP), RFC 2516 (PPPoE), and RFC 1662 (PPPoHDLCL).



**CAUTION:** The PPP protocol uses a control signal to establish and maintain a connection over the WAN link. This signal is critical to sustaining traffic through the link and should be protected using QoS. See the section [ARP/PPP page on page 121](#).

## PPP configuration summary

You must perform the following process to establish a functioning PPP link as the WAN interface:

1. Disable the DHCP client on the eth0 (WAN) interface. [\[page 71\]](#)
2. Create a PPP profile. This displays as the ppp0 IP interface. [\[this section\]](#)
3. Create security policies for the ppp0 interface. [\[page 127\]](#)
4. Enable NAT for the ppp0 interface. [\[page 134\]](#)
5. Create a QoS group to protect the PPP control signal. [\[ARP / PPP page on page 121\]](#)

---

**NOTE:** The Initial Setup Wizard performs all of these steps after completing the WAN, QoS, and VoIP pages of the wizard.

---

To remove a PPP link, perform the above tasks in reverse order. However, do not delete the QoS group if it is also being used by ARP.

Perform the following steps to delete the PPP profile created in [Step 2](#).

1. De-activate the PPP profile.
  - a. Open the PPP profile page by clicking the **Profile** number in the **Interface > PPP** display page.
  - b. Click **Modify** to open the configuration page.
  - c. Set the **Active** field to **no** and click **Update**. You return to the profile page.
2. Delete the profile.
  - a. enable the check box next to the profile number on the display page.
  - b. Click **Delete**.

## Configuring a PPP profile

Note that only one PPP profile can be configured.

In the Data > Interfaces > PPP display pane, click **New** to open the configuration page. Fill in the fields as shown below. Click **Update** when finished.

If a profile has already been defined, click the **0** in the **Profile** column in the display to open the Properties page, then **Modify** to open the configuration page.

<b>Profile</b>	Default is 0 and cannot be changed.
<b>L2 Interface</b>	Layer 2 interface name. Only one interface ( <b>eth0</b> ) is supported at this time.
<b>Active</b>	Specify <b>yes</b> to activate the profile. Specify <b>no</b> to de-activate the profile. (A profile must be activated to enable PPP link negotiation; the profile must be de-activated before it can be modified.) The default is <b>no</b> .
<b>AuthProto</b>	Authentication protocol [ <b>PAP</b>   <b>CHAP</b> ]. The default is <b>PAP</b> . On the BSGX4e, a PPPoE interface also has MSCHAPV1 and MSCHAPV2 protocol options.

<b>SelfIP/Mask</b>	Optional static IP address and subnet mask (1.2.3.4/8) for the pppn interface. Enter <b>any</b> if none is provided. Default is <b>any</b> .
<b>MTU</b>	Maximum Transmission Unit (MTU) of the interface (296-1492 bytes). The default is <b>1492</b> bytes.
<b>MRU</b>	Maximum Receive Unit (MRU) of the interface (296-1492 bytes). The default is <b>1492</b> bytes.
<b>RestartTime</b>	Time interval before a request is re-sent (in milliseconds). The default is <b>3000</b> (3 seconds).
<b>ServiceName</b>	Optional service name (up to 30 characters) to identify the profile.
<b>Username</b>	Account user name (up to 64 characters) for logging in to the PPP access concentrator.
<b>Password</b>	Account log in password (up to 32 characters).

## Data > Interfaces > VLAN

This section is where you assign the VLAN to an interface, thereby creating the virtual interface (**VIF**). This section also includes an overview of the entire **VLAN** (virtual LAN) configuration process.

A VLAN is an independent network formed as a logical subcomponent of a physical network. Since a VLAN functions as a separate network, its traffic is isolated from traffic on other VLANs and traffic on the rest of the physical network.

**Figure 14** VLAN interface page

**VLAN Interfaces:**

VID	Interface	Status	VIF	Comment
<input type="checkbox"/> 1	eth1	on	vif0	

**Data > Interface IP:**

Inter	IP Address/Mask	MTU	DHCP client	Lease obtained	Lease expires	MAC Address	Speed	Configured Speed
<input type="checkbox"/> eth0	172.16.13.149/ 255.255.0.0	1500	on	SAT FEB 23 10:54:12 2008	SUN FEB 24 10:54:12 2008	00:15:93:00:02:CA	FULL100	AUTONEG
<input type="checkbox"/> eth1	192.168.1.1/ 255.255.255.0	1500	off	N/A	N/A	00:15:93:00:02:CB	N/A	N/A
<input type="checkbox"/> vif0	1.1.1.1/ 255.255.255.0	1500	off	N/A	N/A	00:15:93:00:02:CB	N/A	N/A

## Technical reference

The VLAN function in the BSGX4e has the following characteristics:

- The BSGX4e supports IEEE 801.Q, which allows up to 64 VLANs across the four LAN switch ports. Up to 16 virtual interfaces (vif0 - vif15) can be created on the Interface > IP configuration page. VLANs are integrated into the host IP stack as separate layer 2 Ethernet interfaces.
- A VLAN is most commonly created on the LAN (eth1) interface. A VLAN can also be created on the Ethernet WAN interface (eth0) of the BSGX4e.
- A VLAN cannot be configured on a PPP (ppp*n*) WAN interface.
- By default, no VLANs or virtual interfaces are configured.
- A LAN port is configured as tagged or untagged when it is assigned to a VLAN. See [Data > Switch > VLAN on page 103](#) for more details.
- A VLAN on any interface restricts access by allowing only the subnet addresses defined by the VLAN. Thus, when a VLAN is activated on a LAN port, the LAN switch can no longer be accessed through that port. A VLAN can be created on the Ethernet WAN of the BSGX4e to establish trunking to a switch. In this configuration, the WAN is accessible only by the trunk.
- A VLAN requires firewall security policies to define which traffic to accept or reject.

## Configuration overview

The complete VLAN configuration process requires the following steps:

1. Assign one or more LAN switch ports to the VLAN. Skip this step if you are creating a VLAN for the WAN of a BSGX4e. [\[Data > Switch > VLAN on page 103\]](#)
2. Create the virtual interface (vif*n*) profile for the VLAN and associate it to the physical interface.
3. Configure the virtual interface and assign an IP address to it. [\[VLAN configuration on page 73\]](#)
4. Create one or more firewall security policies so that the firewall allows traffic through the virtual interface. [\[VLAN security policies on page 127\]](#)

To delete a VLAN, delete the above configurations in the opposite order as listed.

## Configuration procedure – Virtual interface

Perform the following procedure on the Data > Interfaces > VLAN page to create a virtual interface profile for a VLAN.

Virtual interfaces are displayed as vif(*n*), where *n* is 0 through 15. A VLAN cannot be configured on a PPP (ppp*n*) WAN interface.

1. Click **New** to open the configuration page.
2. Fill in the fields:

<b>VID</b>	Specify the VID that was created on the Switch > VLAN page (See the NOTE above).
<b>interface</b>	<p>This parameter is required. Physical Ethernet interface on which the virtual interface is configured:</p> <ul style="list-style-type: none"> <li>• <b>eth1</b> for the LAN interface (default)</li> <li>• <b>eth0</b> for the WAN interface. If <b>eth0</b> is specified, the WAN port is automatically assigned to the VLAN.</li> </ul>
<b>Status</b>	Enables the virtual interface ( <b>on</b>   <b>off</b> ). Default is on.
<b>Comment</b>	Optional comment. The comment can be up to 256 characters; if it contains spaces, enclose the string in quotation marks. Special CLI characters (such as ? and <tab>) are not allowed.

3. Proceed to [Data > Interfaces > IP page on page 70](#) to assign an IP address to the VIF.

To modify an existing profile, click the profile's **VID** number to open the properties page, then **Modify** to open the configuration page.

To delete a profile:

- a. Go to [Data > Interfaces > IP page on page 70](#) and delete the virtual interface (vif) that is associated with the VID to be deleted. VID/VIF association is shown on the page in the next step.
- b. Go to [Data > Interfaces > VLAN on page 75](#) and delete the VLAN profile associated with the VID.
- c. Go to [Data > Switch > VLAN](#) and enable the check box next to the **VID** number, then click **Delete**.

## Relays

This section describes using the BSGX4e as a relay for devices on its LAN that request DNS, TFTP, SNTP, or DHCP services. The BSGX4e acts as a proxy and forwards any such requests to the servers on the WAN specified by the services' configurations. To a LAN device, the BSGX4e appears to be a server; to the WAN server, the BSGX4e appears to be a client.

All relays are disabled by default.

The DNS relay is enabled by default. All other relays are disabled.

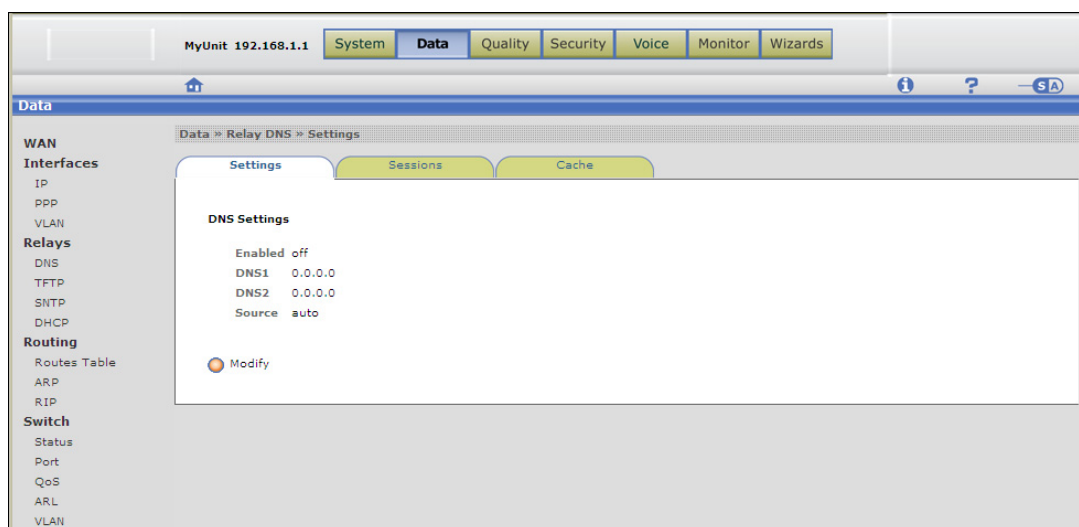
Under the **System** button on the button bar, the BSGX4e can also be configured with a client for DNS and SNTP services, and as a DHCP server. BSGX4e clients get their DNS and SNTP data from servers on the WAN and then provides it for internal functions. The DHCP server is enabled by default to provide IP addresses to your LAN devices. See the sections [Services page on page 33](#) and [DHCP server on page 47](#) for more information.

For clarification, the BSGX4e also has a DHCP client on its WAN interface that obtains an IP address for the unit from a DHCP server. This client is enabled by default. See [Data > Interfaces > IP page on page 70](#) to access this parameter.

### Data > Relays > DNS page

The DNS relay proxies requests (such as those required for Web browsing and email) from devices located on the BSGX4e LAN to a server located on the WAN. To a LAN device, the BSGX4e appears to be a server; to the WAN server, the BSGX4e appears to be a client.

**Figure 15** Relay – DNS page



The BSGX4e maintains a cache of successful DNS exchanges. If a DNS request is already in the cache, the BSGX4e can reply to the request without referencing a DNS server.

As described below, if the DNS relay configuration source is set to **auto**, the actual configuration used depends on the settings of the DNS client. See [System > Services > DNS Configuration panel on page 36](#) for DNS client configuration.

**NOTE:** To use DNS relay, devices on the LAN must be configured—either through DHCP server options (see [page 49](#)) or manually—with the IP address of the BSGX4e LAN as their DNS server.

## Settings tab

To configure the DNS relay, click **Modify** on the Settings tab page, fill in the fields as follows, and click **Update** when finished:

<b>Enabled</b>	Yes to enable. Default is <b>no yes</b> .
<b>DNS1</b>	IP address of a DNS server. This value is stored and is then applied as the “user settings” shown in <a href="#">Table 8</a> .
<b>DNS2</b>	IP address of a DNS server to use if DNS1 is not available. This value is stored and is then applied as the “user settings” shown in <a href="#">Table 8</a> .
<b>Source</b>	The source of the DNS relay’s configuration. Your choices here are: <ul style="list-style-type: none"><li>• <b>user</b> – The last server or servers specified for the <b>DNS1</b> and <b>DNS2</b> parameters.</li><li>• <b>auto</b> – The actual source depends on the choice made here combined with the <b>Source</b> field of the DNS client (<a href="#">page 36</a>). The next table shows how the DNS client and DNS relay interact to determine the relay’s configuration source.</li></ul>

**Table 8** Sources for DNS relay configuration

Source Parameter Setting		Can DHCP/PPP provide DNS configuration?	Did user provide DNS Client configuration?	Source of DNS Relay configuration
DNS Relay	DNS Client			
user	any or null	--	--	User settings in DNS Relay
auto	DHCP or PPP	yes	--	DHCP or PPP
auto	DHCP or PPP	no	--	User settings in DNS Relay
auto	user	--	yes	User settings in DNS Client
auto	user	--	no	User settings in DNS Relay
auto	auto	yes	--	DHCP or PPP
auto	auto	no	yes	User settings in DNS Client
auto	auto	no	no	User settings in DNS Relay

### Sessions and cache tabs

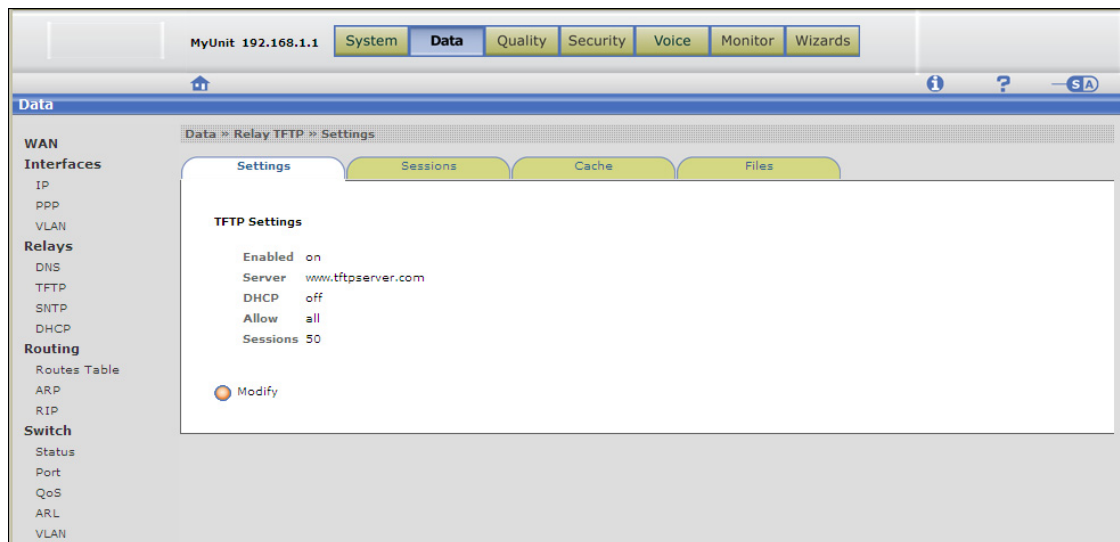
The Sessions tab shows current DNS sessions that are active in the BSGX4e.

The Cache tab shows the history of DNS exchanges.

### Data > Relays > TFTP page

TFTP relay function proxies file requests between devices located on the BSGX4e LAN and a single server located on the WAN. To the devices on the LAN, the BSGX4e appears as a server; to the server on the WAN, the BSGX4e appears as a client.



**Figure 16** Relay – TFTP page

You can cache frequently requested files. If the requested file is in the cache, the BSGX4e can reply to the request without contacting the server.

File caching provides the following benefits:

- Avoiding unnecessary WAN bandwidth usage for frequently requested files, especially if there are several user devices, such as VoIP phones.
- Improved scalability of VoIP service from a service provider, by reducing load on the central file servers that are used for provisioning user devices.

**NOTE:** To use TFTP relay, devices on the LAN must be configured—either through DHCP server options (see [page 49](#)) or manually—to use the BSGX4e as their TFTP server.

## Settings tab

To configure the TFTP relay, click **Modify** on the Settings tab page, fill in the fields as follows, and click **Update** when finished:

<b>Enabled</b>	Enables the TFTP relay. Default is <b>off</b> .
<b>Server</b>	IP address or FQDN of the external TFTP server. If using the <b>DHCP</b> client option, leave this field blank.
<b>DHCP</b>	Enable to have the TFTP server address provided by the DHCP client on the WAN interface of the BSGX4e { <b>on</b>   <b>off</b> }. Do not enable if you specified a server address for the <b>Server</b> parameter. Default is <b>off</b> .
<b>Allow</b>	Types of TFTP messages to relay { <b>get</b>   <b>all</b> }. Default is <b>get</b> .
<b>Sessions</b>	Maximum number of concurrent TFTP sessions. This ensures that the CPU is not monopolized by TFTP packet relays. Default is <b>50</b> .

## Sessions tab

This page shows the current TFTP sessions active in the BSGX4e.

## Cache tab

This page is where you enable and configure the caching feature. You must also specify which files to cache on the Files tab page.

To configure caching, click **Modify** on the Cache tab page, fill in the fields as follows, and click **Update** when finished:

<b>Enabled</b>	Enables TFTP file caching. Default is <b>off</b> .
<b>Size</b>	Size of the file cache in MB ( <b>1-16</b> ). Default is <b>6</b> MB.
<b>Refresh</b>	Cache refresh interval (in minutes). Default is <b>240</b> minutes (4 hours).
<b>Download</b>	Method for downloading files into the cache: <ul style="list-style-type: none"> <li>• <b>auto</b> – Files are saved to the cache while being downloaded by the TFTP relay function.</li> <li>• <b>tftp</b> – Files are downloaded into the cache using an internal TFTP client.</li> <li>• <b>ftp</b> – Files are downloaded into the cache using an internal FTP client.</li> </ul> Default is <b>auto</b> .
<b>Server</b>	IP address or FQDN of the TFTP or FTP server.
<b>User</b>	User name if downloading files by FTP.
<b>Password</b>	Password if downloading files by FTP.

## Files tab

All files that you want to cache have to be named specifically. This page is where you specify the files, and where you view all existing cached files. The cache can list up to 50 files.

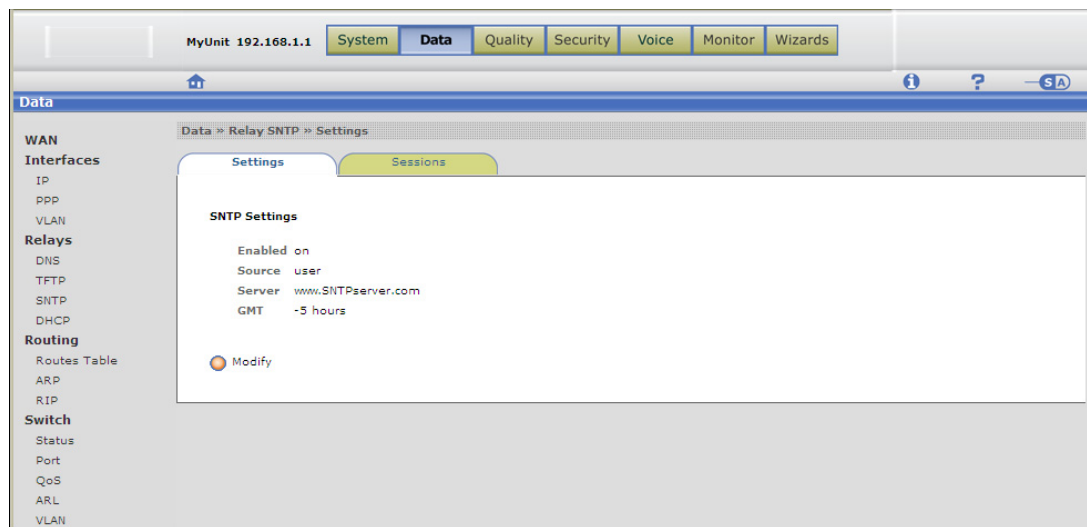
To specify files for caching, click **New** on the Files tab page, fill in the fields as follows, and click **Update** when finished.

To delete an entry, enable the check box next to the **Index** number on the display page, then click **Delete**.

<b>Index</b>	Enter any number from 1 to 50 that is not already in use.
<b>Name</b>	The exact name of the file to be cached.

## Data > Relays > SNTP page

**Figure 17** Relay – SNTP page



The SNTP relay proxies requests from devices on the BSGX4e LAN to a server located on the WAN. To the devices on the LAN, the BSGX4e appears as a server; to the server on the WAN, the BSGX4e appears as a client.

**NOTE:** To use SNTP relay, devices on the LAN must be configured—either through DHCP server options (see [page 49](#)) or manually—to use the BSGX4e as their SNTP server.

## Settings tab

To configure the DNS relay, click **Modify** on the Settings tab page, fill in the fields as follows, and click **Update** when finished:

<b>Enabled</b>	Yes to enable. Default is <b>no</b> .
<b>Source</b>	The source of the SNTP relay's configuration. Your choices here are: <ul style="list-style-type: none"> <li>• <b>user</b> – The last server specified for the <b>Server</b> parameter.</li> <li>• <b>auto</b> – The actual source depends on the choice made here combined with the <b>Source</b> field of the SNTP client (<a href="#">page 35</a>), even if it is disabled. <a href="#">Table 9</a> below shows how the SNTP client and SNTP relay interact to determine the relay's configuration source.</li> </ul>
<b>Server</b>	IP address or FQDN of an external SNTP server. This value is stored, but is used only when the source parameter is <b>user</b> .
<b>GMT</b>	Local time offset from Greenwich Mean Time in +/- hours. Default is 0. Specify this offset only if the LAN devices cannot provide their own offset. If the devices can provide an appropriate offset, set this parameter to 0.

**Table 9** Sources for SNTP relay configuration

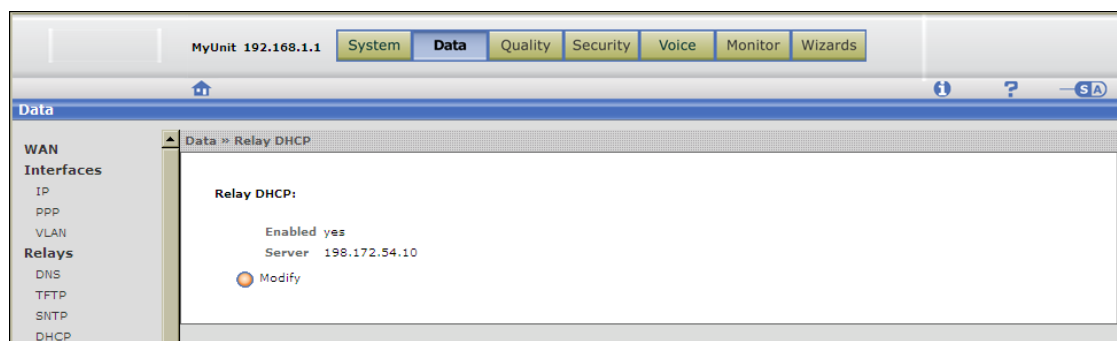
Source Parameter Setting		Can DHCP provide SNTP configuration?	Did user provide SNTP Client configuration?	Source of SNTP Relay configuration
SNTP Relay	SNTP Client			
user	any or null	--	--	User settings in SNTP Relay
auto	DHCP	yes	--	DHCP
auto	DHCP	no	--	User settings in SNTP Relay
auto	user	--	yes	User settings in SNTP Client
auto	user	--	no	User settings in SNTP Relay
auto	auto	yes	--	DHCP
auto	auto	no	yes	User settings in SNTP Client
auto	auto	no	no	User settings in SNTP Relay

## Sessions tab

This page shows the current SNTP sessions active in the BSGX4e.

## Data > Relays > DHCP page

**Figure 18** Relay – DHCP page



The DHCP relay proxies requests from devices on the BSGX4e LAN to a server located on the WAN. To the devices on the LAN, the BSGX4e appears as a server; to the server on the WAN, the BSGX4e appears as a client.

For clarification:

- The BSGX4e has a DHCP client that obtains an IP addresses for the unit from an external DHCP server. This client is normally enabled on the WAN interface. Optionally, it can also be enabled on the LAN interface.
- The BSGX4e has a DHCP server to provide IP addresses to devices on the LAN. This server is enabled by default.

You must perform these tasks to make the DHCP relay functional:

1. Disable the DHCP server on the LAN interface. [\[DHCP server on page 47\]](#)
2. Ensure DHCP client is not enabled on the LAN interface. [\[Data > Interfaces > IP page on page 70\]](#)
3. Disable NAT on the WAN interface. [\[Security > NAT > Interfaces tab on page 134\]](#)
4. Create a security policy to allow traffic from the external DHCP server to the DHCP relay. [\[DHCP relay security policy on page 128\]](#)
5. Configure the DHCP relay:

<b>Enabled</b>	Enable ( <b>yes</b> ) or disable ( <b>no</b> ) the DHCP relay. Default is <b>no</b> .
<b>Server</b>	IP address or FQDN of the external DHCP server.

---

## Routing

This section describes the routing configuration options in the BSGX4e, which consists of a routing protocol table and an Address Resolution Protocol ([ARP](#)) table.

When a network node sends data to an IP address on its subnet segment, it broadcasts an ARP request to resolve the IP address to an Ethernet MAC address.

### Technical reference

The configuration topics in this section refer to three separate protocols that each maintain their own data structure. Each protocol is used for a separate purpose:

- ❑ ARP runs over Ethernet. It translates an IP addresses to a MAC addresses on Ethernet networks.
- ❑ Internet Protocol ([IP](#)) operates at a higher level to route IP packets to addresses on the Internet. It automatically records dynamic entries in a routing table to define routes to destination IP addresses. Static routes can also be configured.
- ❑ The Routing Information Protocol ([RIP](#)) uses a routing daemon. RIP is used in the BSGX4e only if the daemon is manually started. The daemon then listens for RIP messages on the WAN interface from other routers on the network. It uses the RIP message information to maintain the routes in the RIP table.

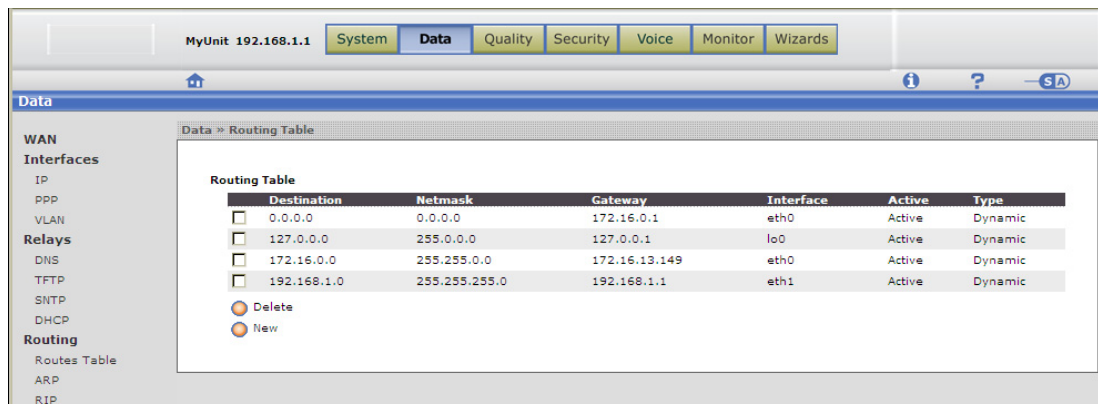
Functional characteristics include:

- Routing table entries can be *dynamic* (automatic) or *static* (manual).  
A dynamic ARP entry is automatically configured when an IP interface is created or enabled. It is deleted when the IP interface is removed or disabled.  
A static ARP entry is manually configured and must be manually deleted. Static routes cannot be modified after creation. You must delete the route and re-create it.
- The ARP table only maps IP addresses within the IP sub-network assigned to the device.
- ARP runs over Ethernet only. It does not run on non-Ethernet interfaces such as PPP, frame relay or VPN interfaces.
- Each packet contains a destination IP address. If the destination address is within the address range specified for a route, the route is applied to the packet. A *default route* does not specify a destination address range; instead, it applies to any packet to which no other route applies. The destination address is entered as 0.0.0.0.

## Data > Routing > Routes Table

View dynamic routes and configure static routes in the routing table on this page.

**Figure 19** Routing Table page



Dynamic routes are automatically created when IP interface are created or enabled. It is possible to delete dynamic routes, but this is not recommended.

Use the following procedure to create a static route:

1. Click **New** to open the configuration page.
2. Fill in the fields as follows:

<b>Destination</b>	Destination IP addresses and mask for which the route applies. To add a <i>default</i> route to the table, specify the destination as 0.0.0.0, or enter the word <b>default</b> .
<b>Gateway</b>	IP address of the gateway. The gateway must be reachable from the BSGX4e. Do not use this field if you specified an interface address.
<b>Interface</b>	Output interface for the route. Do not use this field if you specified a gateway address.

## Data > Routing > ARP

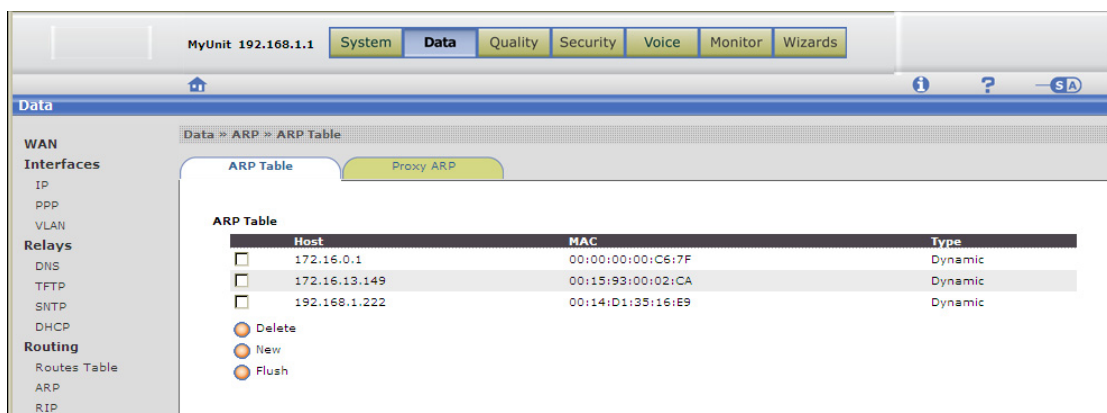
Address Resolution Protocol ([ARP](#)) is a network layer protocol that automatically maps IP addresses to hardware Media Access Control ([MAC](#)) addresses.

Use the ARP page to manually create an ARP table entry, to delete an entry, to flush the table of all entries, and to configure an ARP proxy.

**NOTE:** ARP traffic is essential for the maintenance of the ARP table. Therefore, the manufacturer recommends this traffic be protected from packet loss by placing it in a QoS quality group. See the section [ARP/PPP page on page 121](#) for configuration instructions.

### ARP Table tab

Figure 20 ARP Table page



This tab page is where you create a static ARP entry for a known host by associating the hosts's IP address with its MAC address.

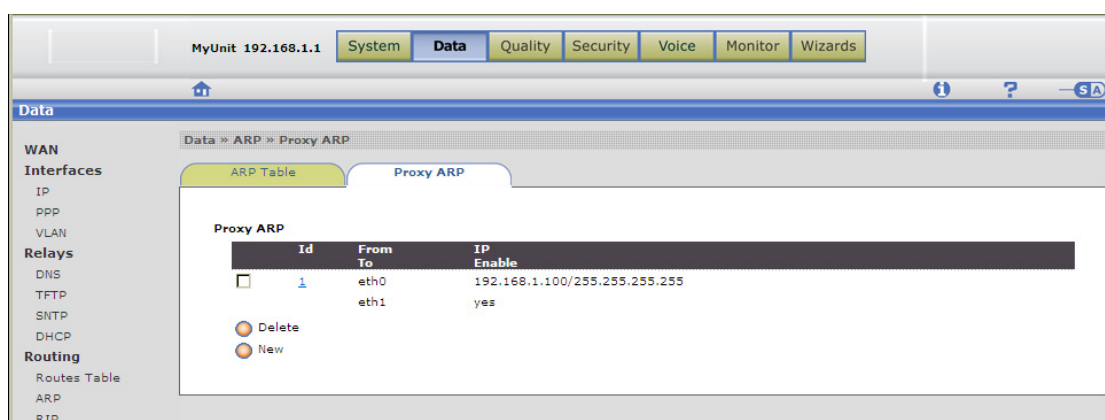
Click **New** to open the configuration page. The fields are self-explanatory.

Click **Flush** to delete all dynamic entries from the ARP table.



## Proxy ARP tab

**Figure 21** Proxy ARP page



Proxy ARP enables the BSGX4e to transparently connect hosts that belong to different networks without having to configure default gateways, routes, or other network parameters.

This section describes the general proxy ARP configuration process. It also includes an application scenario where a BSGX4e is inserted into an existing network that used a firewall/router/NAT appliance as its WAN interface. In this scenario, the firewall becomes a device on a BSGX4e VLAN, thus creating a sub-network that is proxied to the Internet through BSGX4e's WAN interface.

When a host on a network accessible to the BSGX4e's WAN port sends an ARP request through the BSGX4e to a device on its LAN, the BSGX4e responds to the request by supplying its own MAC address (WAN port's MAC) as proxy for the LAN device. The sending host caches the BSGX4e's MAC address with the proxy device's IP address. All subsequent traffic between the hosts, sent as normal (as if on the same subnet), is then routed by the BSGX4e.

A similar process occurs in the reverse direction. When a host on the BSGX4e's LAN sends an ARP request to a host on a remote network, the BSGX4e responds with the LAN's MAC address. The process then repeats as described in the preceding paragraph.

### Technical reference

- Proxy ARP is applicable to both WAN and LAN interfaces. Can be enabled or disabled on each interface and works with VLANs on WAN or LAN interfaces.

**NOTE:** If you use a VLAN with proxy ARP, the VLAN must be created before the proxy is configured. See [Data > Interfaces > VLAN on page 75](#).

- Can be establish only from interfaces that use ARP, which are eth0, eth1, and vifn. A proxy ARP is not supported on PPP, VPN, or FR interfaces.

- ❑ Works with static or dynamic WAN IP address assignments, depending on the configuration. The more standard configurations—like that in [Configuration example 1](#)—can use a dynamic address. More specialized configurations—like that in [Configuration example 2](#)—require a static address.
- ❑ Automatically creates dynamic ARP route table entries and firewall security policies as needed. Deleting or disabling a proxy ARP removes the corresponding ARP route table entries and security policy.
- ❑ Serves as a proxy for a LAN device in the outbound direction. For the reverse traffic direction, the LAN device must be configured with the BSGX4e as its default gateway. A separate proxy must be configured for inbound and outbound traffic.
- ❑ User can create static firewall security policies for existing proxy ARP configuration profiles.
- ❑ A proxy can be established for a specific IP address.
- ❑ Maximum of 32 proxies can be configured.

### Configuration

Terminology:

eth0 – WAN interface

eth1 – LAN interface

vif*n* – Virtual interface

In the display pane, click **New** to open the configuration page. Fill in the fields as shown below. Click **Update** when finished.

To modify an existing entry, click its **Id** number in the display pane.

To delete an existing entry, activate the check box next to the profile on the display page, then click **Delete**.

To configure a new proxy ARP:

1. Navigate to the **Data > Routing > ARP** page, **Proxy ARP** tab.
2. Click **New** to open the configuration page.
3. Fill in the fields:

<b>Id</b>	Enter <b>new</b> to create a new entry.
<b>From/To</b>	Select the interfaces that correspond to the direction of the traffic. If a VLAN has been configured, its virtual interface is in the drop-down list.
<b>IP</b>	The destination address and mask for which this proxy is being created. <address/mask>
<b>Enable</b>	To enable or disable this proxy function.

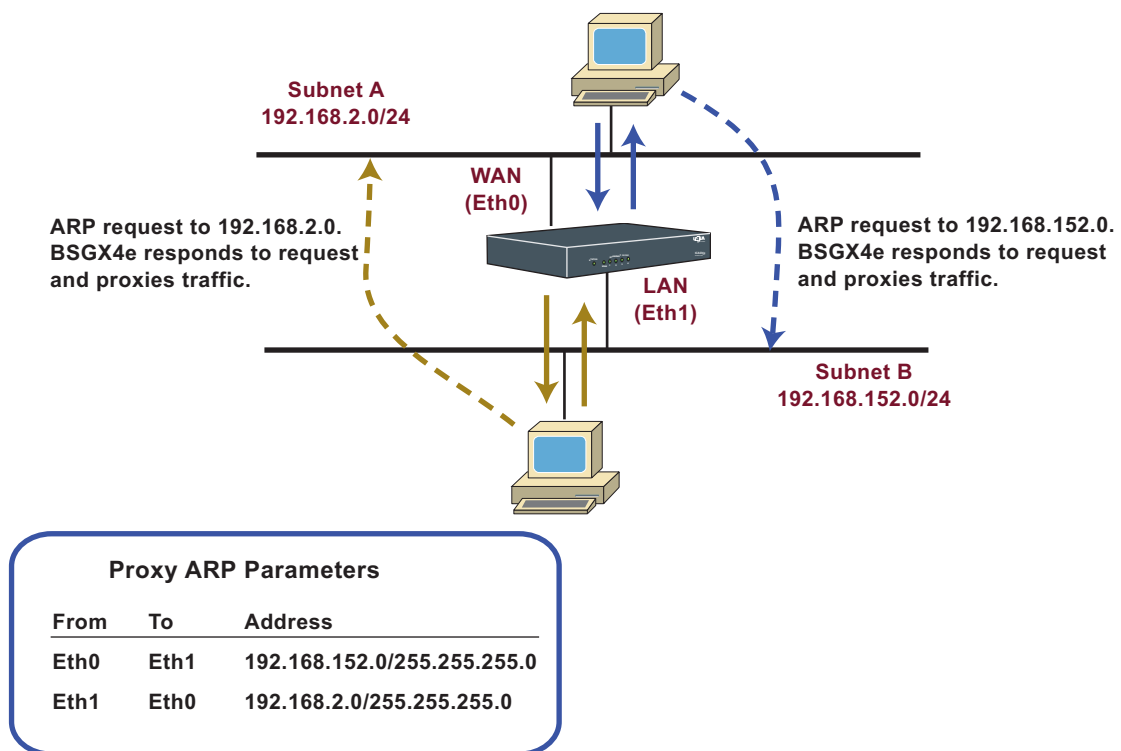
4. Click **Update** when finished.

**Configuration example 1**

The diagram in [Figure 22](#) shows two proxies established (one in each direction) between a subnet on the WAN and a subnet on the BSGX4e LAN. The two proxies would be configured as follows:

Field	Value (Proxy 1)	Value (Proxy 2)
<b>Id</b>	<ID 1>	<ID 2>
<b>From</b>	eth0	eth1
<b>To</b>	eth1	eth0
<b>IP</b>	192.168.152.0/24	192.168.2.0/24
<b>Enable</b>	yes	yes

**Figure 22** Proxy ARP – General configuration example



### Configuration example 2

The diagram in [Figure 23](#) shows the scenario where a BSGX4e has been inserted into an existing network that was using a firewall appliance for WAN interface. The result of this configuration is that the firewall still functions as if connected directly to the Internet.

In this configuration, you cannot have VoIP devices connected to the LAN side of the firewall in the data VLAN (Vif1). VoIP devices must be connected directly to the BSGX4e LAN.

### Proxies

The two proxy routes needed for this scenarios are as follows:

Field	Value (Proxy 1)	Value (Proxy 2)
<b>Id</b>	<ID 3>	<ID 4>
<b>From</b>	eth0	vif1
<b>To</b>	vif1	eth0
<b>IP</b>	1.1.1.2/32	1.1.1.0/24
<b>Enable</b>	yes	yes

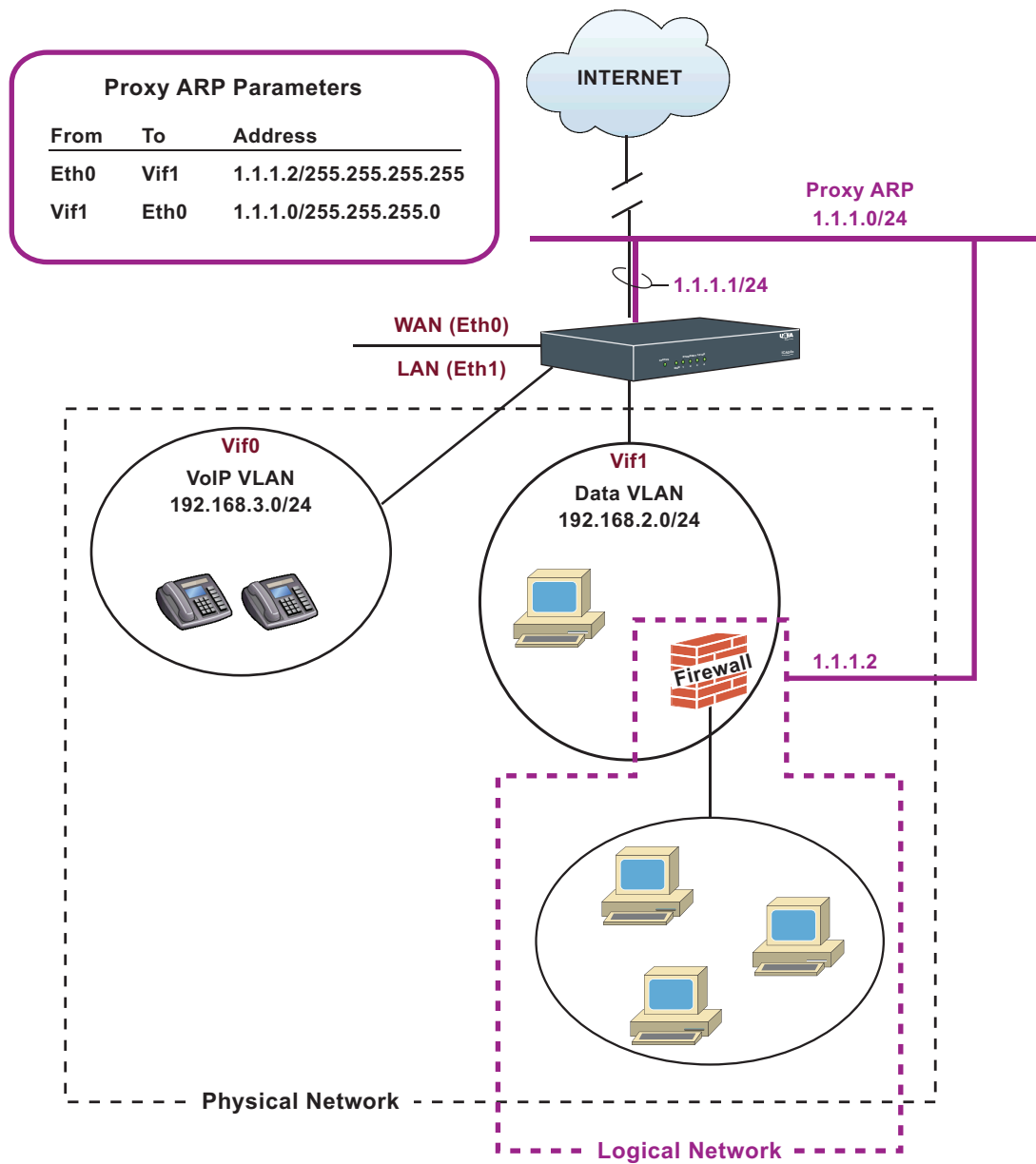
### Firewall security policy and QoS group

This configuration requires a firewall security policy for the incoming (eth0 → vif1) traffic, which you must add manually.

This example uses the default QoS quality group “control” to perform the downstream QoS functions. You must create this quality group, if it was not already created by the Initial Setup Wizard. See [Quality > Group > Group tab on page 112](#) for a detailed discussion.

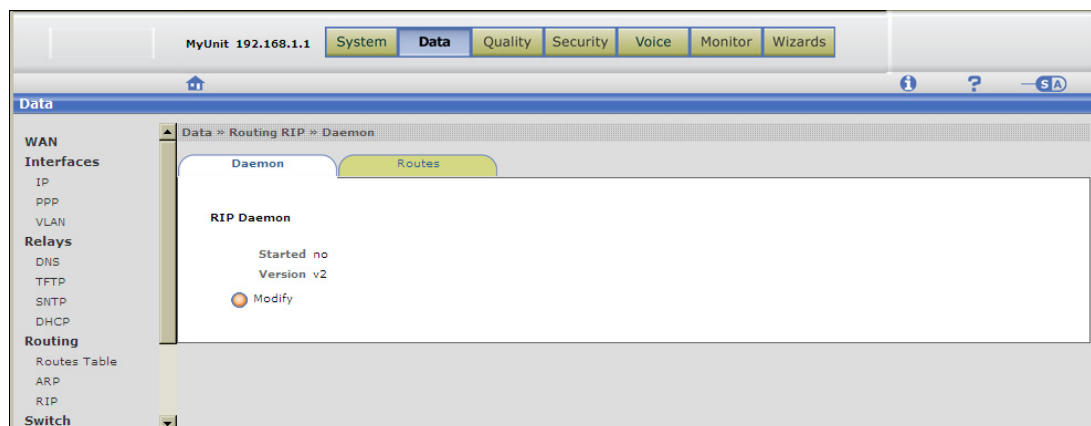
On the **Security > Policy** page, create a new policy with the following parameter values, and leave all other parameters at default values. See the section [Policy on page 125](#) for general instructions on security policies.

<b>From</b>	eth0
<b>To</b>	vif1
<b>Dest IP</b>	1.1.1.2
<b>QoS</b>	control

**Figure 23** Proxy ARP – Subnet with firewall

## Data > Routing > RIP

**Figure 24** RIP page



The BSGX4e executes dynamic routing by enabling [RIP](#) (Routing Information Protocol). RIP is a simple routing protocol that is part of the TCP/IP protocol suite. The BSGX4e supports RIP versions 1 and 2.

The RIP daemon is disabled by default and must be started manually. When started, it listens for RIP messages on the WAN interface and uses that information to store routes in a table.

### Functional characteristics

- For RIP to be effective, all routers in the network must support RIP version 1 or version 2. Version 2 is recommended. RIP v2 supports RIP v1 capabilities and also provides:
  - Variable-Length Subnet Masks (VLSMs) – Support for next-hop addresses, which allows route optimization in certain environments.
  - Multicasting – Multicasting, instead of broadcasting, reduces the load on hosts that do not support routing protocols.
- The BSGX4e is installed at the edge of the network and is intended to run NAT. Thus, it only listens to RIP messages on its WAN interface or interfaces; it does not support RIP on its LAN interface.
- RIP requires a firewall security policy for incoming messages on port 520.



**CAUTION:** An open port on the WAN interface can be a security risk.

- RIP broadcasts routing information to its neighboring routers. Therefore, it consumes some of the bandwidth.

### Configuration

The only parameters you can change are starting RIP and selecting the version.

On the Daemon tab of the RIP page, click **Modify** to open the configuration page and change the settings as needed.

The Routes tab displays the routes that the RIP daemon has stored.

NOTE: You must create a firewall policy to allow RIP responses into the BSGX4e. See [RIP security policy on page 129](#).

## Switch

The LAN switch in the BSGX4e implements a non-blocking switch fabric, enabling packet switching at wire speed over all ports.

- The switch provides four LAN ports, displayed as 0-1 through 0-4.  
The switch also has an uplink port displayed as 0-0. This port is not configurable and is made visible only for diagnostic purposes. Port 0 connects the LAN switch to the processing functions of the BSGX4e.
- Within the BSGX4e, the switch passes traffic from LAN hosts to the LAN switch interface (eth1). Traffic destined for the Internet is then routed to the WAN interface. The switch also routes traffic from a host on one LAN port to a host another LAN port.
- A functional LAN switch requires configuration of both the LAN ports (this section) and the eth1 LAN interface. The eth1 interface is configured by default. See [Data > Interfaces > IP page on page 70](#) for the interface display.

### Data > Switch > Status page

This page is a status display of the LAN port configurations.

**Figure 25** LAN status page

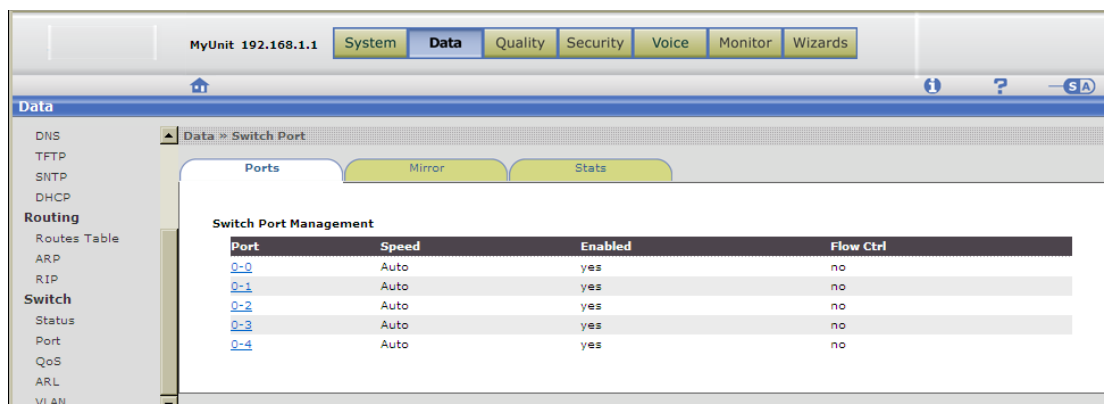
Port	Link	Speed/Duplex	FlowCtl
0-0	UP	100Full	None
0-1	DOWN	10Half	None
0-2	UP	100Full	None
0-3	DOWN	10Half	None
0-4	DOWN	10Half	None

Clicking on the port number takes you to the same configuration page as the [Data > Switch > Port tab](#).

## Port page

This page is where you configure the BSGX4e LAN ports and view port related statistics.

**Figure 26** LAN ports page



This page has three tabs:

- ❑ **Port** tab is where you configure the LAN switch ports.
- ❑ **Mirror** tab is a diagnostic tool where you can mirror one port to another.
- ❑ **Stats** tab displays port statistics.

### Data > Switch > Ports tab

All ports are configured by default for auto negotiation of speed and duplex mode; flow control is disabled; and the port is enabled.

You can modify each port's default configuration. The port can be manually configured for:

- speed of 10Base T or 100Base T
- duplex mode of half or full duplex, and
- flow control to provide back pressure (forced collision) for half duplex mode and pause frames for full duplex mode

**NOTE:** Flow control must not be enabled if layer 2 QoS is enabled. See [QoS page on page 98](#).

To modify a port's configuration, click the port number in the display to open the properties page, then click **Modify** to open the configuration page:



<b>Port</b>	Display only. The port being configured.
<b>Speed</b>	The speed and duplex mode: <ul style="list-style-type: none"> <li>• <b>Auto</b> – Auto-negotiate speed and duplex mode</li> <li>• <b>10Half</b> – 10Base T speed; half duplex</li> <li>• <b>10Full</b> – 10Base T; full duplex</li> <li>• <b>100Half</b> – 100Base T speed; half duplex</li> <li>• <b>100Full</b> – 100Base T; full duplex</li> </ul> Default is <b>auto</b> .
<b>Enabled</b>	Port is enabled or disabled. Default is <b>yes</b> (enabled).
<b>Flow Ctrl</b>	When enabled, provides back pressure (forced collision) for half duplex mode and pause frames for full duplex mode. Default is <b>no</b> (disabled).

### Data > Switch > Mirror tab

This tab page configures port mirroring, which duplicates traffic from one port to another.



**CAUTION:** Port mirroring is intended for troubleshooting only. When finished, remove the mirroring configuration so that unit performance is not degraded.

#### Technical reference

- Mirroring can be configured either for outbound traffic or for both inbound/outbound traffic.
- Port mirroring applies to LAN ports only.
- The mirroring port and the port being mirrored should have the same speed.
- To stop mirroring, set the **Direction** parameter to **none**.

#### Configuration

In the display pane, click **New** to open the configuration page. Fill in the fields as shown below. Click **Update** when finished.

To delete an entry, enable the check box next to the port number on the display page, then click **Delete**.

<b>Port</b>	Port whose traffic is mirrored. {0   1   2   3   4}
<b>To</b>	Destination port where the mirrored traffic goes {1   2   3   4}. If mirroring is in progress, the default is the current destination port.
<b>Direction</b>	Direction of traffic to mirror ( <b>both</b>   <b>out</b>   <b>none</b> ). Default is both. Specify <b>none</b> to suspend mirroring.

### Data > Switch > Stats tab

This tab page displays traffic statistics for each port.

## QoS page

The LAN switch in the BSGX4e unit provides a layer 2 Quality of Service (QoS) feature. This feature enables prioritization of network traffic coming into the BSGX4e through its LAN ports. See the relevant sections in the chapter [4 Quality pages on page 105](#) for layer 3 QoS.

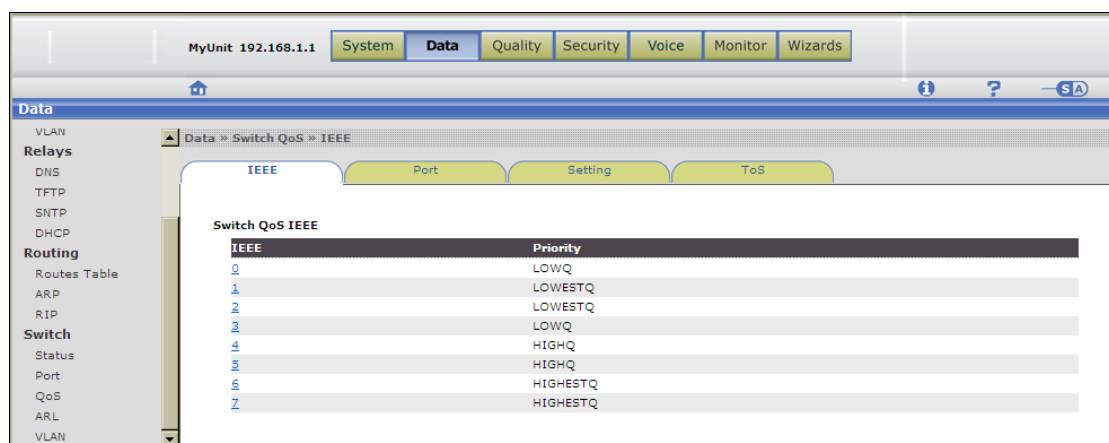
This page has four tabs:

- ❑ **IEEE** tab maps IEEE 802.1p (CoS) bit values to priority queues.
- ❑ **Port** tab sets a priority level applied to all traffic through the port.
- ❑ **Setting** tab sets the prioritizing type and the scheduling method.
- ❑ **ToS** tab maps the ToS/DiffServ values to priority queues.

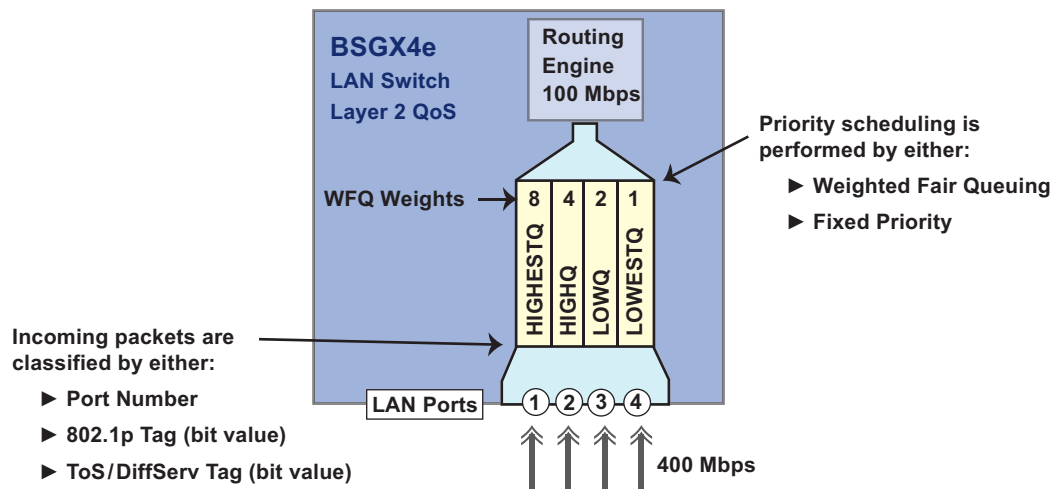


Creating static Address Resolution Logic (ARL) maps with specified priorities overrides the priority settings in this section. See [Data > Switch > ARL on page 101](#).

**Figure 27** LAN Port QoS Page



Since the BSGX4e has four LAN ports to send traffic to one WAN interface, the unit must prioritize the incoming LAN traffic to resolve contention. Layer 2 QoS ensures that higher priority traffic is routed while lower priority traffic could be delayed or discarded. This is accomplished by classifying traffic and routing it to one of four priority queues, as shown in [Figure 28](#) below. See [QoS overview on page 190](#) for a detailed discussion of QoS and diagrams showing specific application scenarios.

**Figure 28** Layer 2 QoS functionality

The configuration process consists of configuring a priority classification type (IEEE, port, or ToS) and a priority scheduling method (WFQ or fixed). See the section [Quality of service – Layer 2 on page 191](#) for a technical reference on these items.

Layer 2 QoS is always operating with the following default settings:

- ❑ Classification type – Port
  - See [Table 10](#) below for the default settings of each type.
- ❑ Scheduling method – WFQ

These settings treat all LAN traffic the same, effectively disabling layer 2 QoS. You must modify these settings to accomplish prioritizing of traffic.

**Table 10** Default priority classification settings

Priority queue	Priority classification types		
	Port	IEEE (bit value)	ToS (bit value)
LOWESTQ	All ports	1, 2	0 – 15
LOWQ		0, 3	16 – 31
HIGHQ		4, 5	32 – 47
HIGHESTQ		6, 7	48 – 63



Layer 2 QoS cannot operate if flow control is enabled on any LAN port. See [Data > Switch > Ports tab on page 96](#) for flow control status. Flow control is disabled by default.

## Data > Switch > IEEE tab

This classification type is used with VLANs and relies on priority bits in the VLAN header to indicate the priority. The priority bits need to be set in the LAN device that is part of the VLAN. Use [Table 10](#), above, to determine the value to set. See the network configuration examples in [Figure 44](#) on [page 193](#).

This *IEEE 802.1p* priority notation is commonly called CoS (class of service). It is three bits in the User field of the ISL frame header.

If you need to change the BSGX4e priority queue associated with a bit value, perform these steps:

1. Click the bit value in the **IEEE** column to open the properties page.
2. Click **Modify** to open the configuration page.
3. Select the appropriate priority level from the **Priority** drop-down list and click **Update**.

## Data > Switch > Port tab

This classification type assigns a priority queue to each LAN port thereby classifying all traffic flowing through that port.

Note in [Table 10](#) that all ports are associated with the LOWESTQ queue by default. To change the association of a port, perform these steps:

1. Click the bit value in the **Switch QoS Port** column to open the properties page.
2. Click **Modify** to open the configuration page.
3. Select the appropriate priority level from the **Priority** drop-down list and click **Update**.

## Data > Switch > ToS tab

This classification type uses the eight bits in the Type of Service (ToS) field of the IP header to indicate priority. The priority bits value needs to be set in the LAN device. Use [Table 10](#), above, to determine the value to set.

If you need to change the BSGX4e priority queue associated with a bit value, perform these steps:

1. Click the bit value in the **Switch QoS ToS** column to open the properties page.
2. Click **Modify** to open the configuration page.
3. Select the appropriate priority level from the **Priority** drop-down list and click **Update**.

## Data > Switch > Settings tab

This tab is where you specify which classification type and scheduling method to use. The defaults are **Port** classification type and **WFQ** scheduling method.

Classification types were described in the preceding sections. The scheduling methods are:

- WFQ (weighted fair queuing) – All queues are serviced depending on the weight assigned to the queue.
- Fixed – All packets are serviced from the highest priority queue first, then the next lower-priority queue is serviced, and so on.

See the section [Priority scheduling on page 192](#) for more discussion.

**NOTE:** To guarantee uninterrupted service for a critical application, such as VoIP, use fixed scheduling and assign that service to the HIGHESTQ queue.

To change the classification type or scheduling method, perform these steps:

1. Click **Modify** to open the configuration page.
2. Select the desired classification type from the **Type** drop-down list.
3. Select the desired scheduling method from the **Scheduling** drop-down list.
4. Click **Update** when finished.

## Data > Switch > ARL

Address Resolution Logic (ARL) maps MAC addresses to specific LAN ports. This enables packets to be switched between ports based on the destination MAC address in the packet.

**Figure 29** ARL page

The screenshot shows the 'Data > Switch > ARL Management' page. The left sidebar contains a tree view with categories: Interfaces (ADSL, ATM, IP, PPP, VLAN), Relays (DNS, TFTP, SNTP, DHCP), Routing (Routes Table, ARP, RIP), Switch (Status, Port, QoS, ARL, VLAN), and Operations (Log Out). The 'ARL' item is highlighted.

The main content area is titled 'Data > Switch ARL Management'. It contains a 'Switch ARL Age' configuration section with the following fields:

- State: Static (dropdown)
- Mac: 00:14:D1:35:23:B7
- Priority: highq
- Ports: 2

Below these fields is an 'Update' button. To the right of the fields is a 'Description of entry' section with the following text:

- MAC Address
- Priority associated with this entry, LOWESTQ:LOWQ:HIGHQ:HIGHESTQ
- Port(s) associated with this MAC address (0(MII) to 4)

Below the configuration section is a 'Switch ARL Table' section containing a table with the following data:

Index	State	Mac	Priority	Port
1	Static	00:00:00:00:A5:6B	LOWQ	4
2	Dynamic	00:14:D1:35:16:E9	N/A	3
3	Dynamic	00:15:93:00:30:C7	N/A	MII

Below the table are 'Clear' and 'New' buttons.

## Technical reference

- Dynamic Entries

A MAC address learning process automatically builds the ARL table as a forwarding database. It creates are dynamic entries that are regularly flushed from the table at a given interval.

- Static Entries

You can add entries to the ARL table. The entries created are static entries; static entries are not aged out of the table. Static entries remain in the table until the table is manually flushed with the **Clear** button.

- Prioritizing Traffic by MAC Address

You can prioritize specific LAN traffic with static ARL entries (but not with dynamic entries). Four priority queues are available: LOWESTQ, LOWQ, HIGHQ, and HIGHESTQ. (See [QoS page on page 98](#) for more discussion of priority queues.)

By specifying a priority queue when you map a destination MAC address to a port, all packets with that address/port combination are routed to the specified priority queue regardless of the LAN QoS settings on the [QoS page on page 98](#).

- Aging Interval for Dynamic Entries

The aging interval determines when dynamic entries are flushed. The default is 304 seconds. This parameter can be changed with the CLI command:

```
config switch arl age xxxx
```

Where **xxxx** = seconds. Range is 16 to 4080 seconds in multiples of 16. Any number entered is rounded to the next multiple of 16.



Received packets that match a static ARL table entry use the priority setting of that entry. This setting overrides all other layer 2 QoS settings ([page 98](#)) for the port (including port, ToS and 802.1p). This feature cannot be disabled.

## Configuration procedure

Perform the following steps to configure a static ARL table entry:

1. Click **New** in the ARL display page to open the configuration page.
2. Fill in the fields as follows:

<b>State</b>	You must select Static. The Dynamic entry is not valid.
<b>MAC</b>	The destination MAC address, in format xx.xx.xx.xx.xx.xx.
<b>Priority</b>	The priority queue to route all traffic for the destination address.
<b>Ports</b>	<p>The LAN port or ports associated with this MAC address.</p> <p>Ports 1-4 are the LAN ports to which you connect your LAN devices.</p> <p><b>NOTE:</b> Do not map port 0 to an address. Port 0 is an internal port in the LAN switch and is made visible only for diagnostic purposes.</p>

3. Click **Update** when finished.

## Clearing the table

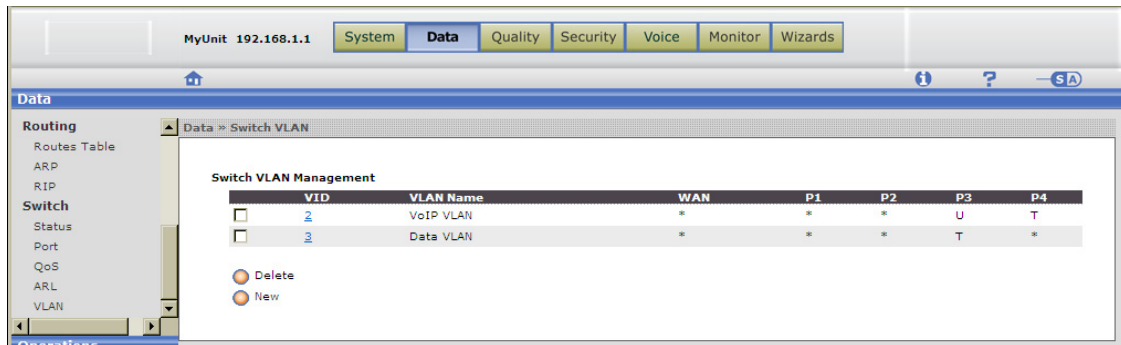
The **Clear** button flushes all entries—dynamic and static—from the table. The table rebuilds immediately after clearing so new dynamic entries appear instantly.

## Data > Switch > VLAN

This section describes the procedure for assigning the BSGX4e LAN ports to VLANs.

This is the first part of the entire VLAN configuration process, which is detailed under [Data > Interfaces > VLAN on page 75](#).

**Figure 30** VLAN – LAN switch



### Technical reference

- A port is configured as tagged or untagged when it is assigned to the VLAN. VLANs handle packets as follows:
  - Untagged ports transmit untagged packets, and tagged ports transmit tagged packets.
  - Untagged packets delivered to an untagged port are internally tagged with the VLAN ID to which the port belongs; this enables those packets to be switched.
  - Untagged packets arriving at a tagged port are discarded; it is undetermined to which port to assign untagged packets.
  - Tagged packets arriving at a port, other than the VLAN port identified by the VLAN ID in the packets, are dropped.
  - IEEE 802.1p packets are considered untagged packets.
  - A port can be assigned to more than one VLAN. However, only one of those ports can be configured as untagged, the others have to be tagged.
- You can create 64 VLANs on the LAN switch.
- A VLAN on any interface restricts access to only the subnet addresses defined by the VLAN. When a VLAN is activated on a LAN port, the LAN switch can no longer be accessed through that port.

## Configuration procedure

The following procedure creates a VLAN ID, assigns a port to that VLAN, and configures the tagging characteristics of the port.

1. Click **New** to open the configuration page.
2. Fill in the fields as follows:

<b>VID</b>	VLAN identification number ( <b>1 - 4094</b> ).
<b>VLAN name</b>	Name or description of the VLAN. It can be up to 32 alphanumeric characters.
<b>P1, P2, P3, or P4</b>	VLAN state of the LAN port * = not member of the VLAN (default) U = untagged port T = tagged port If the VLAN is for the WAN, leave all ports with the default *.

3. Proceed to [Data > Interfaces > VLAN on page 75](#) to create the corresponding virtual interface. The VID associates the virtual interface with the VLAN.

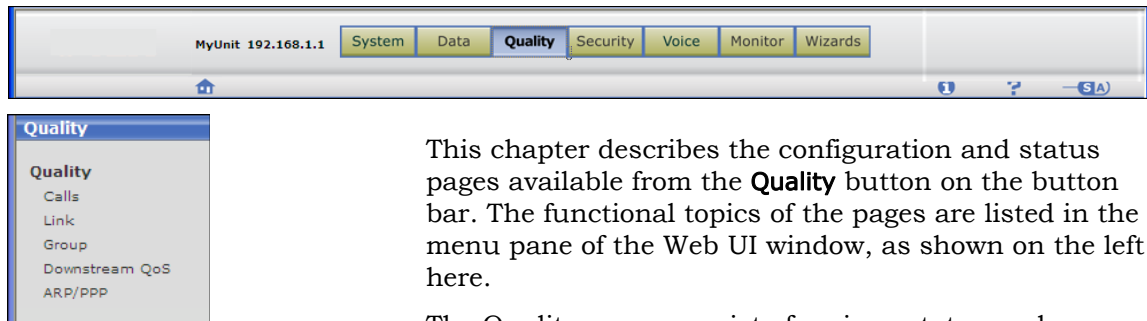
To modify an existing profile, click the profile's **VID** number to open the properties page, then **Modify** to open the configuration page.

To delete a profile:

- a. Go to [Data > Interfaces > IP page on page 70](#) and delete the virtual interface (vif) that is associated with the VID to be deleted. VID/VIF association is shown on the page in the next step.
- b. Go to [Data > Interfaces > VLAN on page 75](#) and delete the VLAN profile associated with the VID.
- c. On the [Data > Switch > VLAN](#) page, enable the check box next to the **VID** number, then click **Delete**.



# 4 QUALITY PAGES



This chapter describes the configuration and status pages available from the **Quality** button on the button bar. The functional topics of the pages are listed in the menu pane of the Web UI window, as shown on the left here.

The Quality pages consist of various status and statistics displays, and configuration pages related to QoS and Downstream QoS.

## Introduction

The following list summarizes the configuration and status functions on the Quality menu:

- **Calls** ([page 106](#))  
Displays various data relating to call quality, call alarms, and other performance data.
- **Link** ([page 110](#))  
Configures the QoS WAN link. Displays link performance data.
- **Group** ([page 112](#))  
Configures quality groups, which guarantee bandwidth and manage priority for each flow under QoS (upstream). Displays performance data. Identifies which group is used for downstream QoS prioritizing.
- **Downstream QoS** ([page 118](#))  
Activates a downstream QoS on the WAN link. Displays operational status and performance data.
- **ARP/PPP** ([page 121](#))  
Assigns ARP and PPP control traffic to a quality group.

## Calls page

The Quality > Calls page has three tabs:

- ❑ **Quality** – Displays various quality statistics, including MoS scores, by endpoint ID number.
- ❑ **Alarms** – Displays statistics on quality, burst and delay alarms.
- ❑ **Analyser** – Configures voice quality monitoring including alarms and thresholds.

**Figure 31** Quality calls page

MyUnit 192.168.1.1   System   Data   **Quality**   Security   Voice   Monitor   Wizards

**Quality**

Quality » Call Quality

Quality   Alarms   Analyser

**Calls Quality**

EP-ID	EP-Name	MOS-LQ	MOS-CQ	R Fact	RTP Rx	Loss	Codec
5101231081	5101231081	4.20	4.18	92	1210	0.00	PCMU
5101231083	5101231083	4.20	4.16	91	1156	0.08	PCMU
5101231065	5101231065	4.20	4.18	92	1441	0.00	PCMU
5101231084	5101231084	4.20	4.16	91	1190	0.08	PCMU
5101231079	5101231079	4.20	4.18	92	1215	0.00	PCMU
5101231032	5101231032	4.20	4.18	92	1485	0.00	PCMU
5101231085	5101231085	4.20	4.18	92	1148	0.00	PCMU
5101231063	5101231063	4.20	4.18	92	1446	0.00	PCMU
5101231066	5101231066	4.20	4.18	92	1477	0.00	PCMU
5101231069	5101231069	4.20	4.18	92	1412	0.00	PCMU
5101231075	5101231075	4.20	4.18	92	1349	0.00	PCMU
5101231090	5101231090	4.18	4.14	90	1070	0.19	PCMU
5101231094	5101231094	4.20	4.18	92	1063	0.00	PCMU
5101231038	5101231038	4.20	4.18	92	1452	0.00	PCMU

Operations

Log Out   Save Changes   Defaults   Reload System

Internet

## Quality > Calls > Quality tab

The Quality tab page is display only and appears as shown above in [Figure 31](#) when calls are active in the BSGX4e.

### Terminology

**EP-ID/EP-Name** – Endpoint (LAN phone) identification number or name.

**MOS-LQ/MOS-CQ/R Fact** – Mean Opinion Score - Listening Quality; Mean Opinion Score - Conversation Quality; and R-Factor. These values depend on the codec used and the level of traffic disruption, for example packet loss, delay, and jitter. MOS is measured on a scale of 1 to 5. R-Factor is measured on a scale of 0 to 93.

**RTP Rx** – Number of RTP packets received from the source.

**Loss** – Packets loss rate. Calculated from  $[\text{number of packet not received}] + [\text{number of packet received but lost in jitter buffer}] \div [\text{theoretical number of packets anticipated}]$

**Codec** – Codec used by the source. If the codec used is not supported by the Calls Analyser, it is not listed and no voice quality measurement is provided.

The following voice codecs are supported by the BSGX4e:

G.711 U-law (PCMU) (64 Kbps)	G.726 ADPCM (16, 24, 32 Kbps)
G.711 A-law (PCMA)	G.729-class (not 729D or 729E) (8 Kbps)
G.723-class (5.3, 6.3 Kbps)	

## Quality > Calls > Alarms tab

The display on the Alarms page shows the quantity of alarms in three categories: low quality, excessive burst, and excessive delay.

## Quality > Calls > Analyser tab

The Analyser page shows the jitter buffer (JB) settings, alarm triggers, and threshold settings. Configure these parameters through the Modify button. Alarms are reported in the system log as INFORM messages. The internal system log is discussed in [System > Status > System Log panel on page 30](#).

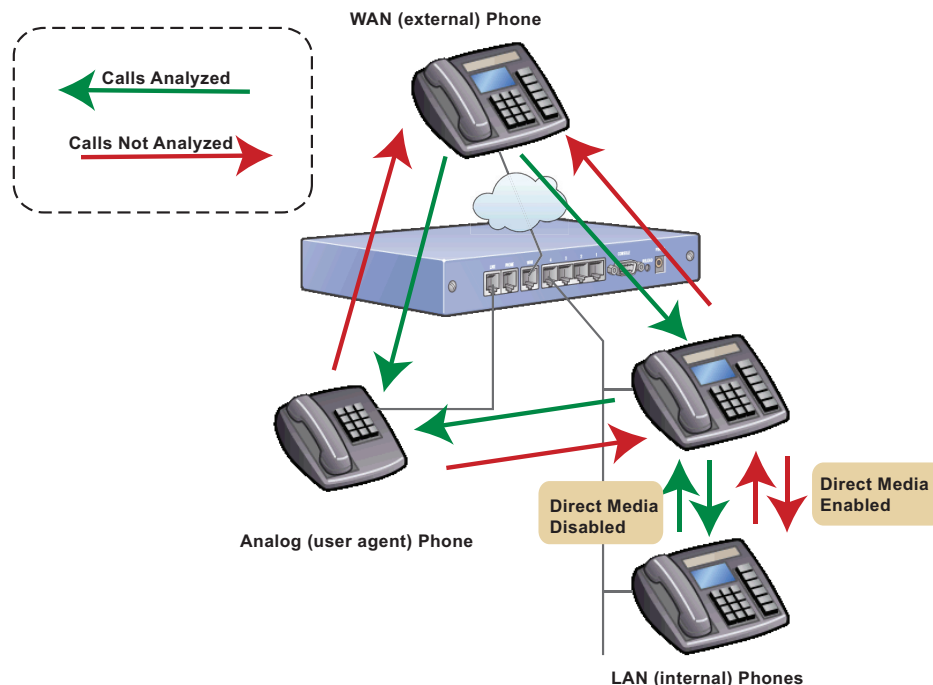
The Calls Analyser simulates a jitter buffer to analyze VoIP media streams and report information such as packet loss, delay and jitter. Based on these parameters, it calculates R-Factors/Mean Opinion Scores updated in real-time over the duration of calls, and displays the outcome on the Quality and Alarms tabs.

The Calls Analyser reports statistics for VoIP media streams that flow through the routing engine in the external→internal, and internal→internal directions. Whether or not Direct Media is enabled also affects which flows are analyzed. As shown below in [Figure 32](#), flows measured by the Calls Analyser are:

- External calls – Inbound flows from WAN to LAN and from WAN to User Agent.
- Local calls – Flows between LAN phones, and flows from LAN to analog phones. Note that flows between LAN phones are analyzed only if Direct Media is disabled.

With Direct Media enabled, the session controller establishes RTP flows directly between two LAN phones. The Call Analyser cannot measure those direct flows. With Direct Media disabled, the routing engine bridges the RTP flows between LAN phones and both flows can be measured by the Call Analyser. See [Voice > Media > Settings on page 161](#) for more discussion on Direct Media.

**Figure 32** Calls analyzer flows



***Calls analyser configuration***

Open the configuration page by clicking the **Modify** button. Change the default values as needed:

<b>JB Type</b>	Whether to emulate a static or adaptive jitter buffer {static   adaptive}. Default is static.
<b>JB Minimum</b>	Minimum size of the simulated jitter buffer. Default is 10.
<b>JB Maximum</b>	Maximum size of the simulated jitter buffer. Default is 60.
<b>JB Nominal</b>	Nominal level of the simulated jitter buffer. Default is 30.
<b>Roundtrip Delay</b>	Estimate of round trip delay if no RTCP records are detected (in milliseconds). Default is 60 milliseconds.
<b>Quality</b>	Enable alarms for low quality R-factor. Default is yes.
<b>Burst</b>	Enable alarms for excessive bursting. Default is yes.
<b>Delay</b>	Enable alarms for excessive delay. Default is yes.
<b>R-Quality</b>	Alarm trigger for low quality R-Factor. Default is 60.
<b>R-Burst</b>	Alarm trigger for excessive bursting. Default is 60.
<b>Burst Min</b>	Minimum alarm trigger for excessive bursting duration (in milliseconds). Default is 500 milliseconds.
<b>Delay Max</b>	Maximum alarm trigger for excessive delay (in milliseconds). Default is 450 milliseconds.
<b>Min Quality Alert Clear</b>	Minimum duration until the low quality alarm is cleared. Default is 3 seconds.
<b>Min Burst Alert Clear</b>	Minimum duration until the excessive bursting alarm is cleared. Default is 3 seconds.
<b>Min Delay Alert Clear</b>	Minimum duration until the excessive delay alarm is cleared. Default is 3 seconds.

## Link page

The Quality > Link page is where you specify the upstream bandwidth for the QoS link. This relates to the quality groups you configure for QoS in the section, [Group page on page 112](#), which is next. The total bandwidth of all quality groups cannot exceed 90% of the link rate.

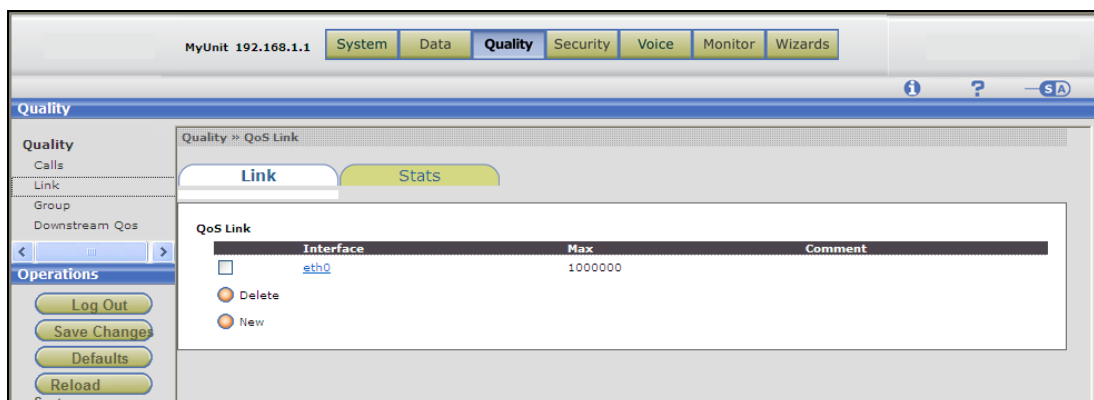
See also [Appendix 12–Quality of service](#) for a technical description of QoS implementation in the BSGX4e.

This section relates to layer 3 QoS functions. See [QoS page on page 98](#) for layer 2 QoS functions.

The Quality > Link page has two tabs:

- ❑ **Link** – Specify the bandwidth for the QoS network (WAN) link.
- ❑ **Stats** – Displays performance statistic for Best Effort traffic on the WAN link.

**Figure 33** Quality link page



### Quality > Link > Link tab

The QoS link is the upstream bandwidth of the BSGX4e. This value affects the quality groups that reserve bandwidth for your protected applications. The total reserved bandwidth of all quality groups cannot exceed 90% of the QoS link rate.



**CAUTION:** Do not enter a link rate that is higher than your actual bandwidth. If quality group bandwidth is configured based on this excessive rate, you can experience interrupted service from the applications under QoS management.

The BSGX4e supports just one QoS link, which is the WAN interface. This is designated as **eth0** for the BSGX4e model. You cannot configure the QoS link on a virtual interface, such as VPN or VLAN, or on PPP.

Configure the QoS link as follows:

1. Click **New** to open the configuration page.
2. The appropriate **Interface** normally displays by default. Select it from the drop-down list if necessary.
3. Enter the network connection rate in bits per second (bps) into the **Max** field.

This is normally the uplink rate indicated by your network service provider. However, if your actual rate is significantly different than the indicated rate, use the actual.

The **eth0** link on the BSGX4e is limited at 100,000,000 bps.

4. Add a comment as desired.
5. Click **Update** when finished.

QoS Link:  
Configure the bandwidth of the specified interface

Interface	eth0	The interface
Max	1000000	The maximum speed of the link. (64000-100000000 bps)
Comment		An optional comment for this link

## Quality > Link > Stats tab

This tab page provides performance data on packet and byte traffic. The displayed data is self-explanatory.

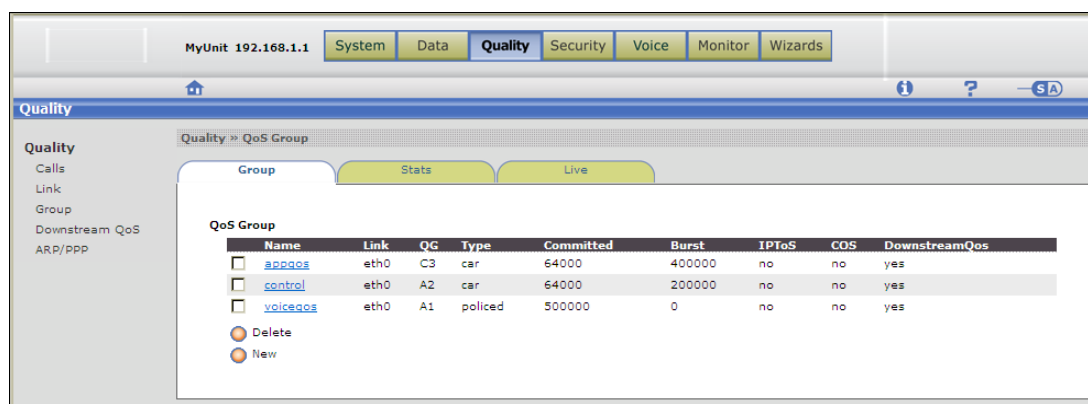
The display shows cumulative statistics for all Best Effort traffic on the WAN (eth0/t1e1) link. Statistics for quality groups are on the Quality > Group page, discussed in the next section.

## Group page

The Quality > Group page has three tabs:

- ❑ **Group** – Create and configure the quality groups used in QoS.
- ❑ **Stats** – Cumulative performance statistics for quality groups.
- ❑ **Live** – Instantaneous performance statistics for quality groups.

**Figure 34** Quality group page



## Quality > Group > Group tab

The Group page is where you create and configure the *quality groups* used in QoS. A quality group guarantees bandwidth for the media assigned to it, and it designates a *quality class*, which assigns priority. The quality group also enables Downstream QoS, which is discussed on [page 118](#).

See also [Appendix 12–Quality of service](#) for a summary of the over-all QoS configuration procedure, and for a technical description of QoS implementation in the BSGX4e.

Common or recommended quality groups are:

- VoIP

This is the most common use of QoS. You must create a quality group for the two traffic flows that comprise VoIP: media and control signal. You must then associate this group with the session controller. The session controller detects the VoIP flows and assigns them to this quality group. Configure the session controller association on the following pages:

The VoIP media is associated on the Web UI page, [Voice > Media > Settings on page 161](#).

The VoIP control signal is associated on the Web UI page, [Voice > Session Control > SIP Control on page 167](#).

Note that the Initial Setup Wizard creates a “voiceqos” quality group for this purpose and configures the needed associations.



- SIP video

Protecting SIP video stream under QoS requires special considerations due to the characteristics of the stream. Video has a moderate average rate but experiences high peaks that can reach 3 Mbps.

- Use only with high-bandwidth installations of at least 1.5 Mbps.
- SIP video is detected by the session controller and assigned to a quality group named “video.” This is a special name that the session controller recognizes. You must create this quality group as described in this section.
- Configure the video quality group with CAR policing to allow the peaks to burst into best-effort space. Note that this can cause discarded packets.
- This configuration must be performed by technical personnel experienced with VoIP and QoS processing. This personnel can experiment with various settings to determine the optimal configuration.

- SIP data

Multimedia applications using SIP—such as whiteboards and data transfer clients—are placed into the appqos quality group. This is a special name that the session controller recognizes. You must manually create this group.

Multimedia applications register with the session controller. The session controller detects the multimedia data streams and assigns them to the appqos quality group. This assignment is automatic so a separate action is not needed to associate this quality group with the session controller.

- ARP/PPP

You are advised to place these control signals under QoS management.

You must first create a control group, then assign the ARP/PPP signals to it. That assignment is performed on [ARP / PPP page on page 121](#).

Note that the Initial Setup Wizard creates a “control” quality group for this purpose and performs the needed assignment.

The recommended configurations for the SIP data and ARP/PPP quality groups are:

Parameter	Value
<b>QG</b>	C3 (SIP Data Group) A2 (ARP/PPP Group)
<b>Type</b>	CAR
<b>Committed</b>	64000
<b>Burst</b>	200000
<b>Downstream QoS</b>	Yes

Parameters not shown here can be left at their default values.

If you need to create a quality group for traffic that is not detected by the session controller or does not have configuration page in the Web UI, you must create a firewall policy to identify the data stream and assign it to the quality group. See [Security > Policy > Static tab on page 130](#).

## Configuring a new quality group

If you need to create a new quality group, click **New** in the Group tab page and fill in the fields as described below. Click **Update** when finished.

To modify an existing group, click the **Name** in the display to open the properties page, then **Modify** to open the configuration page.

To delete an entry, enable the check box next to the group name on the display page, then click **Delete**.

QoS Group:

Configure the quality group to prioritize traffic

Name	<input type="text" value="apppos"/>	The name of the quality group
Link	<input type="text" value="eth0"/>	The interface of the link
QG	<input type="text" value="C3"/>	The GoS 2.0 class
Type	<input type="text" value="car"/>	The type of the policer
Committed	<input type="text" value="64000"/>	The committed rate for a Quality Group
Burst	<input type="text" value="100000"/>	The burst rate (ignored when Type = police)
IPToS	<input type="text" value="no"/>	decimal IPToS value to write into packets in this quality group ("no" to disable)
COS	<input type="text" value="no"/>	802.1p COS value to write into packets in this quality group if VLAN ("no" to disable)
DownstreamQos	<input type="text" value="yes"/>	Enabling Downstream GoS for this group (yes/no)

<b>Name</b>	Name of the quality group to be created.
<b>Link</b>	QoS link, which is the WAN link over which QoS transmits. This setting must be <b>eth0</b> .
<b>QG</b>	QoS quality class for setting priority ( <b>A1</b>   <b>A2</b>   <b>A3</b>   <b>B1</b>   <b>B2</b>   <b>B3</b>   <b>C1</b>   <b>C2</b>   <b>C3</b>   <b>BE</b> ). Default is <b>A1</b> . <b>BE</b> (best effort) specifies no QoS prioritizing. Up to 10 quality groups can be assigned to the same GoS class.
<b>Type</b>	Policing method ( <b>car</b>   <b>policed</b>   <b>besteffort</b> ). The default is <b>policed</b> . <ul style="list-style-type: none"> <li>• <b>policed</b> – Strict policing at an absolute bandwidth rate. Traffic that exceeds the rate is discarded.</li> <li>• <b>car</b> (committed access rate) – A committed (absolute) rate, plus the ability to burst into available BE bandwidth, up to the designated burst limit. Traffic that exceeds the committed rate is either burst into BE space or is discarded. Traffic that exceeds the burst rate is discarded.</li> <li>• <b>besteffort</b> – Best effort indicates no QoS processing. In this case, traffic that exceeds the link rate is discarded.</li> </ul>
<b>Committed</b>	Committed upstream bandwidth rate for this quality group (in bps). Do not specify a value if the <b>QG</b> field is <b>BE</b> . The minimum rate is 64000. <p><b>NOTE:</b> The sum total of committed rates for all quality groups must not exceed 90% of the specified QoS link rate.</p>
<b>Burst</b>	If <b>Type</b> is <b>car</b> , enter a bandwidth value (in bps) to allow this group to burst data above the committed rate. Typically, the rate is set equal to the QoS link. Do not specify a value if the <b>QG</b> field is <b>BE</b> .
<b>IPToS</b>	IP ToS value to be written into each packet assigned to this quality group (decimal, 0-255). Enter <b>no</b> if no ToS value is to be written. If supported by the upstream router, the ToS value can notify the router to minimize delay/cost or maximize throughput/routing.

---

<b>COS</b>	CoS value to be written into each packet assigned to this quality group (decimal, 0-7). Enter <b>no</b> if no CoS value is to be written. If supported by the upstream router, the CoS value can notify the router if VLAN traffic is to be prioritized (as defined by the IEEE 802.1p standard).
<b>DownstreamQoS</b>	Reserves incoming bandwidth for non-TCP traffic. Intended primarily for the voice and control quality groups. See <a href="#">page 118</a> .

---

## Using wizards

The Initial Setup wizard can configure the QoS with common default settings. There is also a QoS wizard where you must enter all data manually.

The Initial Setup wizard provides non-technical users with a simplified interface to configure the basic parameters in the BSGX4e that leave the unit in a functional state. For technical users, the wizard provides a convenient way to quickly configure basic features during installation, and provides a general example of parameter settings.

### Quality groups

On the QoS page of the Initial Setup wizard, the user can create the two quality groups deemed necessary for uninterrupted service of the BSGX4e's critical functions: one for VoIP devices (**voiceqos**), and one for ARP/PPP control signals (**control**). The user can click the Defaults button or manually enter the required data. The only inputs required by the wizard are:

- ❑ Upstream QoS link rate
- ❑ Downstream QoS link rate
- ❑ WAN encapsulation type
- ❑ Committed bandwidth for voice and control quality groups

All other QoS parameters are pre-configured by the wizard.

The **voiceqos** quality group processes both the VoIP media stream and the control signal stream. The wizard automatically associates both streams with the **voiceqos** quality group. In the Web UI, these associations can be viewed at:

- ❑ VoIP media stream – [Voice > Media > Settings on page 161](#)
- ❑ VoIP control signal stream – [Voice > Session Control > SIP Control on page 167](#)

The **control** quality group processes the control signals, when needed, for the ARP and PPP functions when they contact their external devices. This quality group is associated with these functions on the ARP/PPP configuration page. In the Web UI, this association can be viewed at:

- ❑ ARP/PPP control signal stream – Quality > [ARP/PPP page on page 121](#)

### QoS defaults

If the wizard was used with the Default button, the various pages under the Quality button in the Web UI displays the settings in the following tables. These pages are where you can modify the default settings.

**Table 11** Qos link rate defaults

BSGX4e	Upstream Rate	Downstream Rate
BSGX4e (Ethernet)	800000	1500000

**Table 12** QoS groups defaults – BSGX4e

Name	Link	Quality Class	Policer Type	Committed Rate	Burst Rate	IPToS	COS	Downstream QoS
voiceqos	eth0	A1	strict	500000	0	no	no	yes
control	eth0	A2	CAR	64000	200000	no	no	yes

## Quality > Group > Stats

You can view cumulative performance statistics for quality groups on the Stats tab of the Group page. The displayed statistics are as follows:

<b>Packets in</b>	Total number of packets offered to and received by the quality group.
<b>Packets out</b>	Total number of packets forwarded on the primary output. These packets were protected because they arrived within the committed rate.
<b>Downgraded packets</b>	Total number of packets downgraded and forwarded to the Best Effort quality group. This applies only to CAR policing and represents packets that arrived above the committed rate, but below the burst rate.
<b>Packets dropped</b>	Total number of packets dropped: <ul style="list-style-type: none"> <li>• Strict Policing: Packets dropped if traffic exceeds the committed rate.</li> <li>• CAR Policing: Packets dropped if traffic exceeds the burst rate.</li> </ul>
<b>Bytes in</b>	Byte count for the <b>Packets in</b> counter.
<b>Bytes out</b>	Byte count for the <b>Packets out</b> counter.
<b>Bytes dropped</b>	Byte count for the <b>Packets dropped</b> counter.
<b>Bytes downgraded</b>	Byte count for the <b>Downgraded packets</b> counter.

## Quality > Group > Live

You can view instantaneous performance statistics (one-second interval) for quality groups on the Live tab of the Group page. The displayed statistics are as follows:

<b>Input rate</b>	Offered rate to the quality group.
<b>Output rate</b>	Overall output rate of the quality group, including protected and downgraded traffic.
<b>Primary output rate</b>	Output rate of the protected traffic.
<b>Downgrade output rate</b>	Output rate of downgraded (non-protected) traffic. This rate applies only to quality groups that use CAR.
<b>Packet loss rate</b>	Rate of packets dropped by the quality group: <ul style="list-style-type: none"><li>– Strict Policing: Packets dropped if traffic exceeds the committed rate.</li><li>– CAR Policing: Packets dropped if traffic exceeds the burst rate.</li></ul>
<b>Data loss rate</b>	Packet loss rate translated to bytes per second.
<b>Packet loss ratio</b>	Ratio comparing total packets out to total packets in.
<b>Data loss ratio</b>	Ratio comparing total bytes out to total bytes in.
<b>Average packet size</b>	Average packet size in bytes.

## Downstream QoS page

**Attention:**

**Downstream QoS is not yet supported.**

Downstream QoS manages WAN link inbound bandwidth to provide quality protection for specified incoming data streams. This is intended primarily to ensure adequate bandwidth for incoming VoIP and ARP/PPP control streams. It is applied by enabling the Downstream QoS field in a quality group.

Downstream QoS functions differently than the upstream QoS described in the preceding sections. Downstream processing is based on differentiating non-quality TCP traffic from quality non-TCP traffic.

Incoming traffic is processed by the Routing Engine, with the Classifier as the first process. A quality group that has its Downstream QoS parameter set creates a policy in the Classifier. All traffic that does *not* match the quality group criteria is routed to a delaying queue.

In practice, IP voice and control streams use non-TCP protocols. With these streams under Downstream QoS protection, the remaining traffic (mostly TCP) is queued. The delay resulting from queuing causes TCP traffic to limit itself, which leaves most of the bandwidth available for non-TCP traffic.

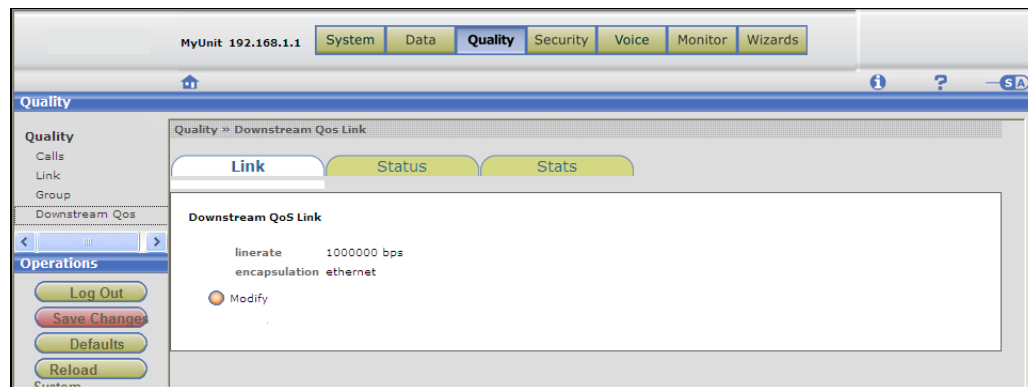
By limiting required bandwidth for non-quality (TCP) traffic, which is normally Web pages and email, quality traffic (non-TCP) experiences only minimal packet loss and delay.

When you designate a QoS quality group as the downstream carrier, it does not apply the upstream QoS parameters to the downstream traffic. The function of the quality group in the downstream direction is to identify quality traffic, create the Classifier policy, and process the stream through the downstream QoS queuing mechanism.



**CAUTION:** Enabling Downstream QoS in too many quality groups can result in excessive restriction of TCP traffic causing unacceptable delays in affected applications.

Downstream QoS is recommended for VoIP applications and the ARP/PPP control signals. If you have other non-TCP applications for which you have created a quality group, they can also utilize Downstream QoS. However, depending on your bandwidth and level of Internet usage, having too many Downstream QoS quality groups can cause a noticeable reduction in the responsiveness of TCP-based application.

**Figure 35** Downstream QoS page

## Quality > Downstream QoS > Link tab

The link tab is where you specify the downstream link rate and encapsulation type. The BSGX4e uses the encapsulation type to add overhead bandwidth to the downstream link calculation.

**NOTE:** The network device directly upstream from BSGX4e can affect overhead, as described in the next paragraph. Select an encapsulation type that accommodates this device.

The actual downstream bandwidth can be significantly affected by the router (or other device) that is immediately upstream from the BSGX4e. This device can add or remove encapsulation. For BSGX4e to make the most accurate calculation, it needs to consider the affect on overhead of this device. Therefore, the encapsulation field on this page offers an extended list for protocols to choose from. [Table 13](#) below shows which encapsulation types are from BSGX4e and which are to accommodate an upstream device.

Perform the following steps to configure downstream QoS:

1. On the **Link** tab page, click **New** to modify the link parameters.
2. Enter the WAN data rate in bps into the **linerate** field. Normally, this is the downstream bandwidth indicated by your service provider.
3. Select a WAN link encapsulation method from the drop-down list. Normally, this is the same encapsulation as was configured for the WAN (Data > WAN). However, if you are connecting to a device upstream that encapsulates (a frame relay modem, for example), then select that encapsulation type.

 This is a screenshot of a configuration dialog box titled 'Downstream QoS Link:'. Below the title is a subtitle 'Configure the profile of the downstream link'. The dialog contains two input fields: 'linerate' with the value '80000' and 'encapsulation' with a dropdown menu showing 'ethernet'. To the right of these fields, there is explanatory text: 'WAN interface line rate' and 'Physical encapsulation of the WAN interface'. At the bottom of the dialog are two buttons: 'Update' and 'Cancel'.

**Table 13** WAN encapsulation options

BSGX4e WAN encapsulation	Network device encapsulation
• Ethernet	pppoa_vc
• VLAN	pppoa_llc
• PPPoE	pppohdlc
	fr

Terminology:

LLC = Logical Link Control

VC(MUX) = Virtual Circuit Multiplexing

## Quality > Downstream QoS > Status tab

The status tab indicates whether or not Downstream QoS is enabled in a quality group.

Note that you must configure the Downstream QoS link before you can enable this feature in a quality group.

## Quality > Downstream QoS > Stats tab

The statistics tab page displays three categories of WAN link performance data:

- **Protected group**  
Statistics for the quality traffic through the protected downstream bandwidth.
- **Non-Protected group passed**  
Statistics for non-quality traffic that has passed through the unprotected downstream bandwidth.
- **Non-Protected group dropped**  
Statistics for non-quality traffic that has been dropped in the unprotected downstream bandwidth.

The displayed statistics are self-explanatory.



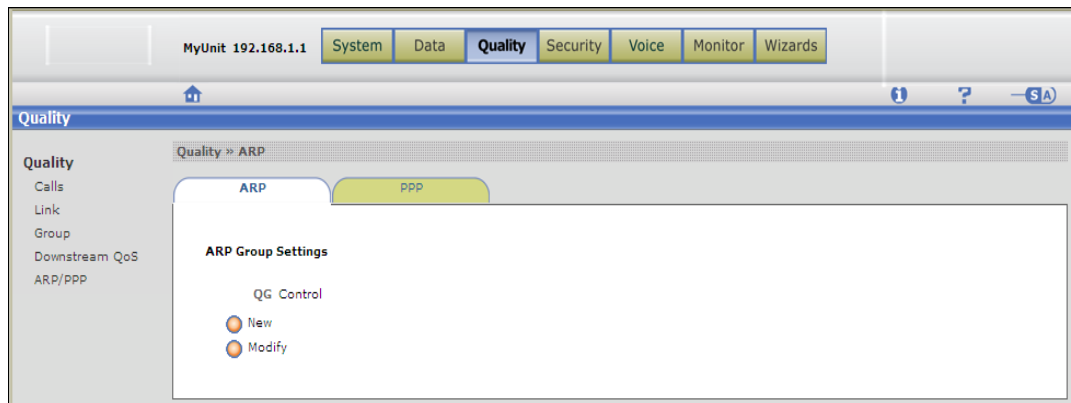
## ARP/PPP page

Both ARP (address resolution protocol) and PPP (point-to-point protocol) use a control signal to establish and maintain their traffic flow through the WAN port.

If you are using either or both of these protocols, you can experience traffic stoppage if the control signal is interrupted at times of heavy traffic load through the WAN. Therefore, these control signals must be protected from packet loss. This is accomplished by protecting them with a QoS quality group.

You create a quality group for this feature (see [Group page on page 112](#)). The ARP/PPP page is where you assign these functions' to that quality group.

**Figure 36** ARP/PPP QoS page



For more discussion on control protocols under QoS, see the section [Media and control signals on page 196](#).

**NOTE:** As an alternative to manual process described in this section, you can use the Initial Setup Wizard to create a “control” quality group with the appropriate values and associations. This is described under [Using wizards on page 115](#).

## Configuration

This page is where you assign the ARP/PPP control signals to a quality group. However, you must have first created that quality group.

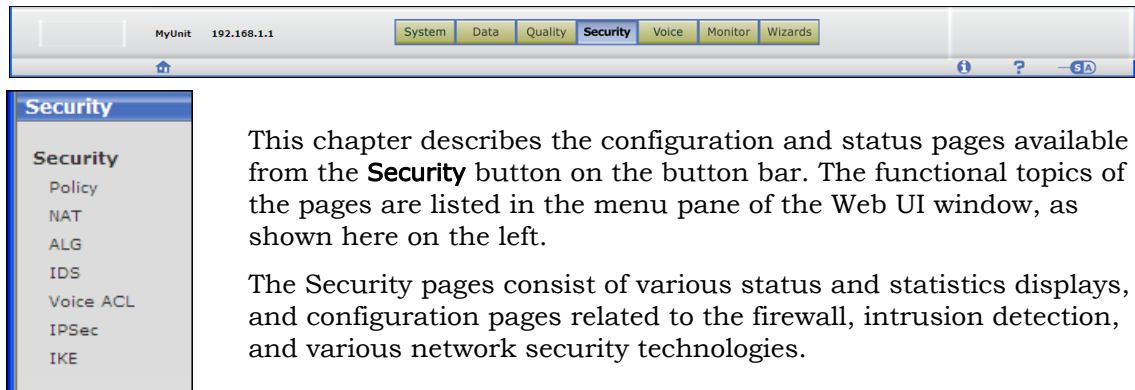
The complete process to put control signals under QoS requires the following two steps:

1. Create a quality group as described under [Quality > Group > Group tab on page 112](#). Use the following values:

<b>Name</b>	<as desired>
<b>Link</b>	eth0
<b>QG</b>	A2
<b>Type</b>	CAR
<b>Committed</b>	64000
<b>Burst</b>	200000
<b>IPToS</b>	no
<b>COS</b>	no
<b>DownstreamQoS</b>	yes

2. On either the ARP tab or PPP tab, click **New** to open the configuration page. Select the quality group name from [Step 1](#). and click **Update**.

## 5 SECURITY PAGES



The following list summarizes the configuration and status functions on the Security menu:

- **Policy** ([page 125](#))  
Create static firewall security policies. View static and dynamic policies.
- **NAT** ([page 132](#))  
Configure Network Address Translation policies on the WAN interface for LAN address translation. Enabled by default on BSGX4e.
- **ALG** ([page 139](#))  
Enable/disable the Application Layer Gateway for FTP, TFTP, and PPTP traffic. Enabled by default.
- **IDS** ([page 140](#))  
Enable/disable the Intrusion Detection System for protection against anomaly, flood, scan, and spoof attacks. Enabled by default.
- **Voice ACL** ([page 145](#))  
Maintain the Access Control List to control which LAN endpoints are allowed to place and receive calls. A default policy exists to allow all endpoints.
- **IPSec/IKE/VPN** ([page 147](#))  
Create VPNs, which include configuring IPSec and IKE to establish the security functions.

## Security overview

The BSGX4e security features enabled: firewall, IDS, and NAT/ALG. These security features process each incoming packet as follows:

1. Incoming packets are sorted by the information in the packet. The information used from layer 2, layer 3, and layer 4 is listed in [Table 14](#).

**Table 14** Packet security processing

Layer 2 Data link	Layer 3 Network	Layer 4 Transport
From interface	Source IP address	Protocol (ICMP, UDP, TCP, GRE, or ESP)
To interface	Destination IP address	Source port
	IP ToS tag (for GoS quality treatment only)	Destination port

2. The packets are then compared to the firewall security policies for its interface. If the packet matches a policy, the policy action determines if the packet is accepted or discarded.
3. If the firewall accepts a packet, then the IDS checks if the packet format is normal (known as a *sanity check*). Abnormally formatted packets are discarded. IDS also checks whether the packet can be considered an attack and, if so, discards it. If the packet is valid, it is delivered to the destination interface.
4. If the packet is identified as valid, information in its header is modified by NAT/ALG to guard private IP information from public entities.

---

## Policy

This page is where you configure new firewall security policies and view existing policies.

As described below, the BSGX4e factory configuration has a basic set of firewall policies defined. Additionally, you are required or advised to create new policies for some of the features that you enable. The section, [Additional security policies](#), provides those instructions.

### Technical reference

The BSGX4e firewall is initially set to block all traffic by default. However, the BSGX4e model has a set of basic firewall policies configured by default for common applications that are normally allowed access from the Internet (see [Table 15](#)). These policies are defined as follows:

- ❑ Traffic from WAN to LAN is rejected.
- ❑ Traffic from LAN to WAN is allowed.
- ❑ Traffic from LAN to the BSGX4e is allowed.
- ❑ Web (HTTP, HTTPS), Telnet, FTP, SFTP, and SSH traffic from the WAN terminating at the BSGX4e is allowed; all other WAN traffic to the unit is rejected.

If the Initial Setup Wizard is used to configure either BSGX4e model, it also creates a number of policies for PPP or frame relay WAN interfaces (see [Table 16](#)).

Observe these constraints when working with security policies:

- ❑ The firewall is always active. It cannot be disabled.
- ❑ Security policies cannot be edited. To change a policy, delete the policy and then re-create it with the desired changes.
- ❑ Up to 128 security policies can be created.

An incoming packet can match more than one security policy. The packet is compared to the policies in order of the sequence value (**Seq** on the display page), starting with sequence 1. Its treatment (acceptance or rejection) is determined by the first policy that the packet matches. Therefore, the sequential order of firewall policies is important.

You can specify the sequential position of a policy. To do so, use the Sequence parameter on the configuration page to specify the beginning or end of the sequence or a position within the sequence.

Policy sequence numbers are always evenly spaced. Thus, when a new policy is inserted within the sequence, policy sequence numbers might be reassigned. The following example demonstrates the process:

- a. Assume that policies with sequence numbers 3 and 5 exist and a new policy is to be inserted between them.
- b. The command specifies 4 as the sequence number of the new policy.
- c. However, the new policy is actually created as policy 5 and the existing policies are re-numbered as 3 and 7. The new policy sequence (3, 5, 7) allows future policies to be inserted into the sequence.

## Default security policies

This section describes the basic set of firewall security policies needed for the WAN interface.

The following notes apply to the tables in this section:

- Parameters not shown in the table are populated with “**any**” or a null value.
- The “**From - To**” fields in the security policies use this terminology:  
eth0/ppp0 = WAN  
eth1/vif(n) = LAN  
self = BSGX4e

[Table 15](#) shows a summary of the default policies for the BSGX4e.

**Table 15** Default firewall policies – BSGX4e

Destination port	From – To	Protocols	Usage
22	eth0 – self	TCP, UDP	SSH, SFTP
23	eth0 – self	TCP	Telnet
80	eth0 – self	TCP	HTTP
443	eth0 – self	TCP	HTTPS, TLS/SSL
any	eth1 – self	any	--
any	eth1 – eth0	any	--

## Additional security policies

This section describes additional policies that you must add for various features in the BSGX4e.

### QoS quality groups

The BSG4Xe applies QoS by assigning selected traffic streams to a quality group. VoIP traffic is assigned in the Media and Session Control sections; certain system control signals are assigned in the Quality section. For all other traffic that you want under QoS management you must create a security policy. The configuration of that policy specifies how the traffic stream is detected (for example, by address or port) and the quality group to which it is assigned.

As an example scenario, a commercial store has a point-of-sale credit card reader that must not experience significant delay. The card reader is known to the BSG4Xe by address:port 10.10.10.120:7750. A quality group named “credit” was created for the card reader traffic. The security policy has the following configuration:

<b>From</b>	<LAN interface>
<b>To</b>	<WAN interface>

<b>Source IP</b>	10.10.10.120
<b>Source (port)</b>	7750
<b>QoS</b>	credit

Other elements that can be used to identify a data stream are destination IP, destination port, protocol, and type of service (ToS) value.

Also, consider whether or not the protected traffic should have downstream QoS enabled, which provides bandwidth for incoming non-TCP traffic.

### **PPP interfaces**

If you configure a PPP WAN interface, it needs security policies similar to the eth0 default policies shown above. If you use the Initial Setup Wizard for the PPP or frame relay interfaces, it creates these policies automatically. For any interface you configure manually, you must also create the needed firewall policies.

[Table 16](#) shows the policies created by the Initial Setup Wizard for a PPP interface. If you are performing a manual configuration, these are the policies you must create.

**Table 16** Firewall policies for PPP

From	To	DPort	Protocol	Action
eth1	ppp0	any	any	allow
ppp0	self	161	UDP	allow
ppp0	self	22	TCP	allow
ppp0	self	80	TCP	allow
ppp0	self	443	TCP	allow

### **VLAN security policies**

VLANs are normally created on the eth1 LAN interface. To emulate the default security policies, you must create the policies shown in [Table 17](#).

See [Data > Interfaces > VLAN on page 75](#) for reference.

**Table 17** Firewall policies for VLAN

From	To	IP Address	S/DPort	Protocol
vif(n)	self	any	any	any
vif(n)	eth0 ppp0	any	any	any

### **SNMP security policy**

As described in the section [SNMP on page 56](#), BSGX4e's SNMP agent requires a firewall policy to allow SNMP client to reach the agent. Create the policy shown in [Table 18](#).

**Table 18** Firewall Policies for SNMP

From	To	IP Address	DPort	Protocol
eth0 ppp0	self	any	161	UDP

***DHCP relay security policy***

If you are using the DHCP relay rather than the default DHCP server for LAN devices, you must create the firewall policy defined in [Table 19](#).

See [Data > Relays > DHCP page on page 85](#) for reference.

**Table 19** Firewall policies for DHCP relay

From	To	Source IP	SPort	DPort	Protocol
eth0 ppp0	eth1 vif(n)	<DHCP server on WAN>	67	67	UDP

***VPN security policies***

If you created a VPN, it needs firewall policies for certain protocols, plus a policy for all traffic from the LAN to the VPN WAN interface.

The vpn-to-self policy is specifically for a VPN to your ISP. The other policies are for two private networks to connect.

See [VPN on page 152](#) for reference.

**Table 20** Firewall policies for VPN

From	To	Source IP	DPort	Protocol
eth1	vpn0	any	any	any
eth0	self	<remote gateway>	500	UDP
eth0	self	<remote gateway>	any	ESP
vpn(n)	self	any	any	ICMP



## Relay security policies

If you want to protect relay traffic (see [Relays on page 78](#)) with QoS, you must create a security policy (see [Table 21](#)) to identify the relay traffic and assign it to the designated quality group:

**Table 21** Security policies for relay

From	To	Destination IP	QoS
BSGX4e	eth0/ppp0/frn/vpn/ hdlc/atm	<IP address>	<quality group created for relays>

## RIP security policy

The RIP routing daemon (see [Data > Routing > RIP on page 94](#)) listens for messages on port 520. Configure the security policy shown in [Table 22](#) if you enabled RIP:

**Table 22** Security policy for RIP

From	To	DPort	Protocol
eth0 ppp0	BSGX4e	520	UDP

## Security > Policy page

This page is where you view existing policies and configure new ones. The page has two tabs: Static and Dynamic. Dynamic policies are those created automatically by applications running on the BSGX4e. Static policies are created manually or by the Initial Setup Wizard.

### Security > Policy > Static tab

This page is where you create new security policies. As discussed above, some default policies exist, and the Initial Setup Wizard creates policies if PPP or frame relay encapsulation is selected. You must create policies manually for VPN and VLAN. Some specialized applications can require a unique security policy.

Perform the following process to create a new security policy:

In the display pane, click **New** to open the configuration page. Fill in the fields as shown below. Click **Update** when finished.

A security policy cannot be modified. You must delete the policy and create a new one with the modified parameters.

To delete an entry, enable the check box next to the port number on the display page, then click **Delete**.

Fill in the configuration page fields as follows:

<b>Index</b>	Specify <b>new</b> if the new policy is to be at the beginning or end of the policy sequence; otherwise, specify a number to indicate where the policy is to be inserted in the sequence (see <a href="#">Technical reference</a> above).
<b>From</b>	Interface from which the packet originated ( <b>self</b>   <b>eth0</b>   <b>eth1</b>   <b>ppp(n)</b>   <b>vif(n)</b>   <b>vpn(n)</b> ). Specify <b>self</b> for packets originating from the BSGX4e. See <a href="#">Additional security policies</a> above for reference.
<b>To</b>	Interface to which the packet is destined ( <b>self</b>   <b>eth0</b>   <b>eth1</b>   <b>ppp0</b>   <b>vif(n)</b>   <b>vpn(n)</b> ). Specify <b>self</b> for packets destined for the BSGX4e. See <a href="#">Additional security policies</a> above for reference.
<b>Source IP (range to)</b>	Source IP address. Default is <b>any</b> . Beginning address of a range.
<b>Dest IP (range to)</b>	Destination IP address. Default is <b>any</b> . Ending address of a range.
<b>Source (range to)</b>	Source port number. Default is <b>any</b> . Beginning port number of a range.
<b>Dest (range to)</b>	Destination port number. Default is <b>any</b> . Ending port number of a range.
<b>Proto</b>	Protocol specified in the packet ( <b>udp</b>   <b>tcp</b>   <b>icmp</b>   <b>esp</b>   <b>gre</b>   <b>any</b> ). Default is <b>any</b> .
<b>NAT</b>	ID number of the NAT profile to be referenced. Change this field only if this security policy is used with a NAT profile. See <a href="#">NAT on page 132</a> . Default is <b>0</b> .

<b>QoS</b>	Name of a QoS quality group. Change this field only if this security policy is used to identify a traffic stream for QoS management. See <a href="#">Quality &gt; Group &gt; Group tab on page 112</a> .
<b>ToS</b>	IP ToS tag value (decimal byte). This field is ignored if ToS is specified in firewall and NAT policies. This is used only if the preceding QoS parameter is configured.
<b>Sequence</b>	Position of the new policy within the policy sequence ( <b>Begin   End   Position</b> ). If <b>Position</b> is specified, the <b>index</b> number specifies where the policy is inserted in the sequence. (See <a href="#">Technical reference on page 125</a> .)
<b>action</b>	Indicates whether a packet matching the policy is accepted or rejected ( <b>allow   deny</b> ).

## Dynamic tab

The firewall dynamically opens and closes ports for some data traffic. This page displays these dynamic policies.

TCP-based applications such as Telnet and FTP, and HTTP applications open connections to external servers, which can be left idle for extended periods. Leaving a port open and idle creates a security risk.

The BSGX4e has a firewall timer to terminate idle TCP and HTTP connections. The default settings are:

TCP timer = 7200 sec.

HTTP timer = 300 sec.

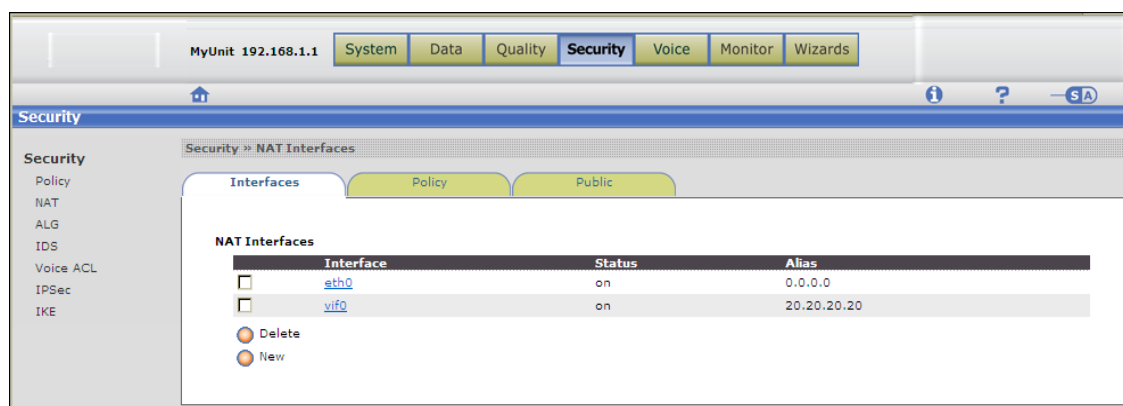
You must use the CLI to change these settings. Use the command `conf firewall tcp`.

## NAT

Network Address Translation ([NAT](#)) provides security by hiding the internal addresses of the LAN private network from the public Internet and it provides economy by mapping multiple private addresses or ports to one public address.

The basic purpose of NAT as applied in the BSGX4e is to multiplex traffic from the internal network and present it to the Internet as if it was coming from a single IP address.

**Figure 37** NAT page



## Technical reference

NAT is designed to provide security and utility to WAN interfaces. Applying NAT to a LAN interface is not contemplated in this document.

NAPT (network address port translation) or PAT (port address translation) are common terms associated with NAT. The technical difference between NAPT/PAT and NAT is whether or not the port number in the IP header is translated. This document uses the term “NAT” to generically refer to all translation

- In general, NAT is accomplished by configuring NAT policies and corresponding security policies. The BSGX4e provides three NAT policy types:
  - Static – A direct (1-to-1) translation of a private LAN address to a public address. Normally configured for sessions initiated on the LAN.
  - Redirect address – Translates addresses of incoming (WAN-to-LAN) traffic based on IP address.
  - Redirect port – Translates addresses of incoming (WAN-to-LAN) traffic based on address/port combination.

- Default configurations:

The WAN port is pre-configured with an Ethernet (eth0) interface. NAT is enabled and provides global address translation for outbound sessions initiated from the LAN. The private LAN addresses are translated to the public address of the WAN port. A default firewall policy allows all traffic from LAN (eth1) to WAN (eth0).

If you need a VLAN, PPP, or VPN, for the interface, you must manually configure it and apply NAT.

- Up to 16 NAT public IP addresses can be configured.
- NAT can create a public address that is outside the subnet of the WAN interface.
- The BSGX4e also supports an Application Layer Gateway (ALG), which enables FTP, TFTP, or PPTP traffic through the firewall and NAT. See the section [ALG on page 139](#).

## Configuration

Configure a NAT profile if you need address and port translation more specific than the default configurations described above. Any such translation requires both a NAT profile and a firewall policy.

### Configuration overview

Here are the three basic NAT configurations that you can implement, depending on the **Type** field on the NAT policy page:

- Inbound Address Translation

The NAT profile maps the private LAN address of the target device to the public address created in the profile. The firewall policy detects inbound traffic destined for the public address and applies the NAT policy to it. This translates the public address to the private address.

- Inbound Port Translation

The NAT profile contains the private LAN address and port number of the target device. The firewall policy detects inbound traffic destined for a specific public address and port number, and applies the NAT policy to it. This translates the public address and port number to the private address and port number.

- Outbound Address Translation

The NAT profile contains the public (static) WAN address. The firewall policy detects outbound traffic from a private LAN address and applies the NAT policy to it. This translates the private address to the public address.

The NAT page contains three tabs, as detailed below. On all tab pages:

- ❑ Click **New** to open the configuration page. Fill in the fields and click **Update** when finished.
- ❑ To delete an entry, enable the check box next to the entry on the display page, then click **Delete**.
- ❑ On the Interfaces tab, if an interface has already been defined, click the **Interface** name in the display to open the properties page, then **Modify** to open the configuration page.

## Security > NAT > Interfaces tab

This tab page is where you enable NAT on the selected WAN interface. This page also displays any interfaces on which NAT has been configured.

Click **New** to open the configuration page. Fill in the fields as follows:

<b>Interface</b>	<p>Select the interface. All configured interfaces are available from the drop-down list:</p> <ul style="list-style-type: none"> <li>• eth0 (BSGX4e; NAT on by default)</li> <li>• ppp(n)</li> <li>• vif(n)</li> <li>• vpn(n)</li> </ul> <p><b>NOTE:</b> Do not select <b>eth1</b> (LAN). This option is to be removed in future releases.</p>
<b>Status</b>	Enable or disable NAT. {on   off}

## Security > NAT > Policy tab

This tab page defines the NAT policy type and the applicable address and/or port to be translated.

If NAT is enabled on an interface but no policy is defined, outbound LAN traffic has its address translated to the defined WAN address.

Fill in the fields as follows (ignore the **range to** fields as they are to be removed in the next release):

<b>Id</b>	The policy ID number. Enter a number, or use <b>new</b> to let the Web UI assign a number.
<b>Type</b>	<p>Select the type of policy to implement:</p> <ul style="list-style-type: none"> <li>• <b>static</b> – Maps one public (WAN) address to one private (LAN) address.</li> <li>• <b>rport</b> – Redirect port. Maps the specified address/port of a private (LAN) address to a public (WAN) address.</li> <li>• <b>raddr</b> – Redirect address. Maps the specified private (LAN) address to a public (WAN) address/port.</li> </ul>
<b>Address</b>	<p>The address entered here depends upon the policy type selected in the <b>Type</b> field. See <a href="#">Application scenarios on page 136</a>.</p> <p>For redirect policies this is a private address.</p> <p>For static policies this is a public address.</p>
<b>Port</b>	If policy <b>Type</b> <b>rport</b> has been selected, enter the port number of the address that was entered into the <b>Address</b> field.

## Security > NAT > Public tab

This tab page is where you assign public IP addresses to the WAN interface. Up to 16 addresses can be assigned.

Fill in the fields as follows:

<b>Address</b>	The public address to be assigned to the WAN interface. The beginning address when specifying a range.
<b>(range to)</b>	The ending address when specifying a range.
<b>Interface</b>	Select “none” (default) if the public address you entered is within the subnet range of the WAN. If you are creating a public subnet outside of the existing WAN subnet, select the WAN interface to which it applies. See also the <a href="#">WAN subnet</a> section below. Note that eth1 is not a valid selection. This option is to be removed in future releases.

### WAN subnet

A special application of NAT is where you are creating a public WAN address that is outside of the defined address range for the WAN. In this case you must create:

- ❑ A NAT public address profile
- ❑ An outbound static NAT profile and a related firewall policy
- ❑ An inbound redirect NAT profile and a related firewall policy

[Table 23](#) shows the required configurations for an example where a device on the Internet at 172.100.10.20 must connect with a device on the BSGX4e LAN at 192.168.2.30. The BSGX4e WAN (eth0) has a static address of 172.150.12.100/22.

**Table 23** WAN subnet configuration

	NAT Profile	Firewall Policy
<b>Profile 1</b>	Interfaces tab: Enable NAT on eth0  Public tab: Address – 172.100.10.20 range to – 172.100.10.35	N/A
<b>Profile 2</b>	Policy tab: Type – static Address – 172.100.10.20	From – eth1 To – eth0 Source IP – 192.168.2.30 NAT – 2
<b>Profile 3</b>	Policy tab: Type – raddr Address – 192.168.2.30	From – eth0 To – self Dest IP – 172.100.10.20 NAT – 3

## Application scenarios

The following examples demonstrate how to configure common NAT application scenarios. See the section [Technical reference on page 132](#) for existing defaults.

### 1. Redirect address example

This example maps a private LAN address to a specific public WAN address. This policy allows incoming traffic from a specific public address on the WAN to a private address on the BSGX4e LAN.

- a. On the **Interfaces** tab, click **New** then select the interface and enable NAT. The example uses eth0.
- b. On the **Policy** tab, click **New** to open the configuration page. Configure a policy that defines the policy type and identifies the private address to be translated:

<b>Id</b>	<b>new</b> [For this example, the ID 1 is automatically assigned.]
<b>Type</b>	<b>raddr</b>
<b>Address</b>	10.0.1.120 [private]
<b>Port</b>	<b>any</b>

- c. On the **Public** tab, click **New** to open the configuration page. Enter a WAN IP address as the NAT public address.  
For this example, 172.108.134.210 is used.
- d. Move to the **Security > Policy** page and **Static** tab. Click **New** to open the configuration page. Configure a policy that maps the public address to a NAT policy, which identifies the private addresses:

<b>Index</b>	<b>new</b>	<b>Proto</b>	<b>any</b>
<b>From</b>	<b>eth0</b>	<b>NAT</b>	<b>1</b>
<b>To</b>	<b>self</b>	<b>QoS</b>	
<b>Source IP (range to)</b>	<b>any</b>	<b>ToS</b>	<b>any</b>
<b>Dest IP (range to)</b>	172.108.134.210 [public]	<b>Sequence</b>	<b>begin</b>
<b>Source (port)</b>	<b>any</b>	<b>Action</b>	<b>allow</b>
<b>Dest (port)</b>	<b>any</b>		



## 2. Redirect port example

This example maps a Web server on the LAN to a port on the public WAN. A request sent from any public address on the WAN using port 12999 is forwarded to the Web server on the BSGX4e LAN.

- a. On the **Interfaces** tab, click **New** then select the interface and enable NAT. We use eth0 in this example.
- b. On the **Policy** tab, click **New** to open the configuration page. Configure a policy that defines the policy type and identifies the Web server's private addresses and port to be translated:

<b>Id</b>	<b>new</b> [For this example, we say that ID 2 is automatically assigned.]
<b>Type</b>	<b>rport</b>
<b>Address</b>	<b>10.0.1.101</b> [private address of Web server]
<b>Port</b>	<b>80</b> [web port]

- c. Move to the **Security > Policy** page and **Static** tab. Click **New** to open the configuration page. Configure a policy that maps the public WAN address port to the appropriate NAT policy, which identifies the private addresses:

<b>Index</b>	<b>new</b>	<b>Proto</b>	<b>tcp</b>
<b>From</b>	<b>eth0</b>	<b>NAT</b>	<b>2</b>
<b>To</b>	<b>self</b>	<b>QoS</b>	
<b>Source IP (range to)</b>	<b>any</b>	<b>ToS</b>	<b>any</b>
<b>Dest IP (range to)</b>	<b>any</b>	<b>Sequence</b>	<b>begin</b>
<b>Source (port)</b>	<b>any</b>	<b>Action</b>	<b>allow</b>
<b>Dest (port)</b>	<b>12999</b>		

### 3. Static NAT example

This policy maps an address on the LAN to an address on the WAN for outgoing traffic. This configuration is opposite of the redirect NAT examples above. Here, the public address is in the NAT policy and the private address is in the firewall policy.

- a. On the **Interfaces** tab, click **New** then select the interface and enable NAT. We use eth0 in this example.
- b. On the **Public** tab, click **New** to open the configuration page. Enter a WAN IP address as the NAT public address.

For this example, we use 172.168.134.65.

- c. On the **Policy** tab, click **New** to open the configuration page. Configure a policy that defines the policy type and identifies the public address to be translated:

<b>Id</b>	<b>new</b> [For this example, we say that ID 3 is automatically assigned.]
<b>Type</b>	<b>static</b>
<b>Address</b>	<b>172.168.134.65</b> [public]
<b>Port</b>	<b>any</b>

- d. Move to the **Security > Policy** page and **Static** tab. Click **New** to open the configuration page. Configure a policy that maps the private LAN address to a NAT policy, which identifies the public addresses:

<b>Index</b>	<b>new</b>	<b>Proto</b>	<b>any</b>
<b>From</b>	<b>eth1</b>	<b>NAT</b>	<b>3</b>
<b>To</b>	<b>eth0</b>	<b>QoS</b>	
<b>Source IP (range to)</b>	<b>10.0.1.103</b> [private]	<b>ToS</b>	<b>any</b>
<b>Dest IP (range to)</b>	<b>any</b>	<b>Sequence</b>	<b>begin</b>
<b>Source (port)</b>	<b>any</b>	<b>Action</b>	<b>allow</b>
<b>Dest (port)</b>	<b>any</b>		

## ALG

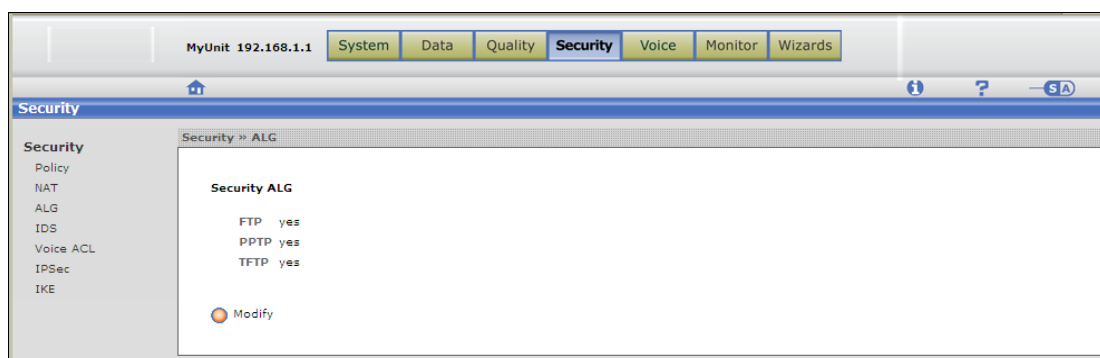
The Application Layer Gateway (ALG) allows FTP, TFTP, and PPTP through the firewall and NAT as trusted traffic. This precludes the need for an administrator to create firewall and NAT policies for the affected protocols. ALG is enabled by default for all three protocols.

ALG works by creating dynamic holes in the firewall and changing IP addresses in application protocol headers.

For reference:

- ❑ FTP (File Transfer Protocol) is commonly used to transfer files over the Internet.
- ❑ TFTP (Trivial File Transfer Protocol) is a simple version of the FTP protocol used to transfer files over the Internet.
- ❑ PPTP (Point-to-Point-Tunneling Protocol) is a networking technology that supports multi-protocol virtual private networks (VPN), enabling remote users to access corporate networks securely across Microsoft computer networks and other point-to-point protocol (PPP)-enabled networks.

**Figure 38** Security ALG page



**NOTE:** NAT must be enabled on the WAN interface to apply ALG. NAT is enabled by default on the eth0 interface of the BSGX4e model. See [NAT on page 132](#).

### Security > ALG page

The ALG page is where you enable/disable ALG on the specified protocols. ALG is enabled by default for the three protocols.

Click **Modify** to open the configuration page. Select **no** from the drop-down list to disable ALG for any of the protocols.

## QoS and PPTP

If you are planning to put the PPTP service under QoS management to give priority to VPN traffic, you must create a quality group and a new outbound firewall policy that associates that quality group. See the section [Policy on page 125](#) for creating firewall policies.

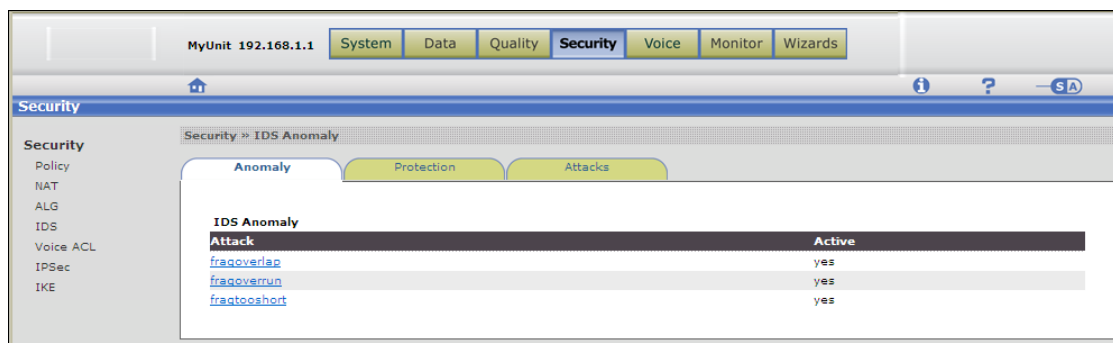
If you define the firewall policy to capture all PPTP traffic on its well known port 1723, you capture both the signal and control traffic and route it to the quality group.

If you want to prioritize only the control traffic, configure the firewall policy to capture GRE protocol from any port.

## IDS

The Intrusion Detection System (IDS) is designed for protection against attacks that are destined for the BSGX4e or its LAN network. The IDS is enabled by default, and it must remain enabled to sustain protection for your local network.

**Figure 39** IDS page



IDS inspects all inbound and outbound network traffic and identifies patterns that can indicate system attacks. IDS identifies the following types of attacks:

- **Packet anomaly** – Protects the unit from abnormal packets that intend to crash the destination. Packet anomalies are configured using the fragoverlap, fragoverrun and fragtooshort commands. See [Security > IDS > Anomaly tab on page 141](#).
- **Scan** – Protects the unit from useless packets that intend to locate “holes” in the firewall. Protection is configured using the IDS scan commands udpportscan, tcpsynscan, and pingsweep.
- **Flood** – Protects the unit from excess incoming packets that can overload the unit. Flood detection is configured using the udpflood, icmpflood, arpflood, synflood, espflood, unknowipprotoflood, stpflood, cdpflood, and unknowntypeflood commands. The protection threshold can be changed for these protocols and services: DHCP, DNS, ESP, IKE, MGCP, RADIUS1, RADIUS2, RIP, SIP, SNMP, SNTP, TFTP, as well as unknown protocols or unknown ports. See [IDS flood activity on page 142](#).

- **Spoof** – Protects the LAN network and the unit from intrusion. IDS spoof protection is applicable for all configured untrusted interfaces.

[Table 24](#) lists the protocols that are inspected.

**Table 24** Protocols for which IDS attack protection applies

Attack type	Ethernet protocols (ARP, STP, CDP, others)	Unknown IP protocols	IP	UDP	TCP	ESP	ICMP	RTP
Anomaly			X		X		X	X
Flood	X	X		X	X	X	X	
Scan				X	X		X	

## Security > IDS > Anomaly tab

This page enables/disables protection against packet fragment anomaly attacks.

All anomaly attack types are enabled by default. To disable an attack type, click the anomaly name on the Anomaly tab page. When the properties page opens, click the **Modify** button.

The following attacks are detected:

- `fragoverlap` — The offset of one fragment overlaps the offset of another fragment. For example, if the offset of the first fragment is 0 and its length is 800, the offset of the second fragment must be 800. If it is less than 800, the second fragment overlaps the first fragment.

This condition might indicate an attack.

- `fragoverrun` — Triggers when a reassembled fragmented datagram exceeds the declared IP data length or the maximum datagram length.

By definition, no IP datagram can be larger than 65,535 bytes; systems that try to process these large datagrams can crash. This type of fragmented traffic can indicate a denial of service attempt.

- `fragtooshort` — Triggers when any IP fragment other than the final fragment is less than 400 bytes, indicating that the fragment is likely to be intentionally crafted. Small fragments can be used in DOS attacks or in an attempt to bypass security measures or detections.

Protection against all other anomalies is enabled by default and cannot be disabled.

[Table 25](#) lists the other anomalies.

**Table 25** Packet anomaly attacks

IP	ICMP	TCP	RTP
Version	Length	Header fragmentation	SSRC ID
TTL (Time to Live)		Flags	
Checksum			
Length			
Options			

## Security > IDS > Protection tab

This page enables/disables protection against flood attacks, scans, and spoofing. These threats can be used in denial of service attacks.

All protection types are enabled by default.

This tab page is divided into four sections:

- [IDS flood activity](#) – Use this section to enable/disable the different types of flood activity. All activities are enabled by default.
- [IDS flood settings](#) – Use this section to change the default threshold for certain protocols.
- [IDS scan](#) – Use this section to enable/disable certain protocols and to change their default timeout value.
- [IDS spoof](#) – Use this section to change the default trusted/untrusted classification of each interface.

### IDS flood activity

The IDS detects floods targeted at protocols and services by using a threshold value to detect a flood attack.

All protocol protection is enabled by default. You can disable a protocol flood detection by clicking the protocol flood name in the display pane. When the properties pages opens, click **Modify**.

The following protocol-based attacks are detected by BSGX4e:

- `udpflood` — In a UDP flood, UDP packets are sent to inactive services (ports); the receiver then replies with an ICMP Destination Unreachable packet.

The flood results in Denial-of-Service, due to sending out several ICMP packets.

- `icmpflood` — An ICMP flood sends over-sized or an excessive number of ICMP packets. This can crash the TCP/IP stack, causing the unit to stop responding to TCP/IP requests.

- **arpflood** — In an ARP flood, 250 ARP request per second are accepted. Over this limit indicates a potential DoS attack.
- **synflood** — SYN (synchronization) packets are repeatedly sent to every port on the server, using fake IP addresses. SYN flooding can result in denial of service.
- **esp flood** — Encapsulated Security Payload (ESP) flood. An ESP flood sends bad IPsec traffic. Packets are discarded after the threshold rate limit is reached.
- **unknowipproto flood** — This flood activity type refers to floods for IP protocols other than those listed specifically.
- **stp flood** — Spanning Tree Protocol (STP) flood. An STP flood sends bad STP packets. Packets are discarded after the threshold rate limit is reached.
- **cdp flood** — Cisco Discovery Protocol (CDP) flood. A CDP flood sends CDP packets at a high rate. Packets are discarded after a threshold rate limit is reached.
- **unknown type flood** — This flood activity type refers to floods targeting Ethernet activities other than ARP, STP and CDP.

## IDS flood settings

IDS uses a threshold value (in packets/second) to detect a flood attack. You can modify the thresholds for the protocols listed in this section. Change the threshold by clicking the name in the **Protocol** column in the display pane. When the properties pages opens, click **Modify**.

The following protocols can be modified:

Protocol	Default threshold (packets/sec)
dhcp	10
dns	20
esp	100
ike	100
mgcp	255
radius_1	100
radius_2	100
rip	20
sip	255
snmp	300
sntp	10
tftp	100
unknown_IP_proto	500
unknown_port	600

## IDS scan

IDS scan protection is activated for ICMP pings, UDP port, and TCP SYN messages. A threshold value determines the number of messages sent that constitute an attack. When IDS detects a scan attack, it bans traffic for that protocol for the timeout interval.

All scan types are enabled by default. You can disable a scan type or changes the timeout value. Click the scan name on the page to open the properties page, then click **Modify**.

The scan attacks monitored by the BSGX4e are:

- **udpportscan** — A port scan is a series of messages sent by a potential system intruder to determine which services the system includes.  
The services are each associated with a well-known port number. Port scanning suggests where the intruder can probe for weaknesses.
- **tcpsynscan** — A TCP SYN scan is a series of messages sent with the TCP Syn flag set.
- **pingsweep** — ICMP requests are sent to multiple hosts. A ping sweep locates network devices that are active and responding, and so, can be targets for an attack.

## IDS spoof

IDS spoof detection can be activated for all IP interfaces, as listed below. It classifies each as a trusted or untrusted interface.

The basic assumptions of spoof detection are:

- IDS assumes that spoof attacks arrive from the WAN and by default assigns untrusted status to WAN interfaces.
- IDS assumes that LAN traffic is safe and the LAN is not a likely source of spoof attacks. Therefore, by default, spoof protection is not needed on LAN interfaces.
- IDS assumes that a VPN secures its traffic from spoof attacks. VPN interfaces are trusted.

The default setting for each interfaces is:

<b>eth1</b>	trusted	<b>vpn</b>	trusted
<b>eth0</b>	untrusted	<b>ppp</b>	untrusted
<b>vif (WAN)</b>	untrusted	<b>fr</b>	untrusted
<b>vif (LAN)</b>	trusted		

---

**NOTE:** Spoof detection for a VPN interface must always be set as trusted.

---

You can change the trusted/untrusted setting of an interface by clicking its name in the **IDS Spoofing > Interface** column of the display pane. When the properties page opens, click **Modify**.

This section displays all interfaces with a valid static or dynamic IP address. If an interface is not displayed, an address problem is indicated.



## Security > IDS > Attacks tab

This is a display-only page that lists a count of the various attacks the IDS has detected. The **Refresh** button updates the statistics. The **Clear** button resets the counters to 0.

**NOTE:** To protect itself from being overwhelmed by a denial of service attack, the IDS counter is limited to reporting 64 packets per second. Thus, the actual packet rate can be greater than the value reported by the IDS counter.

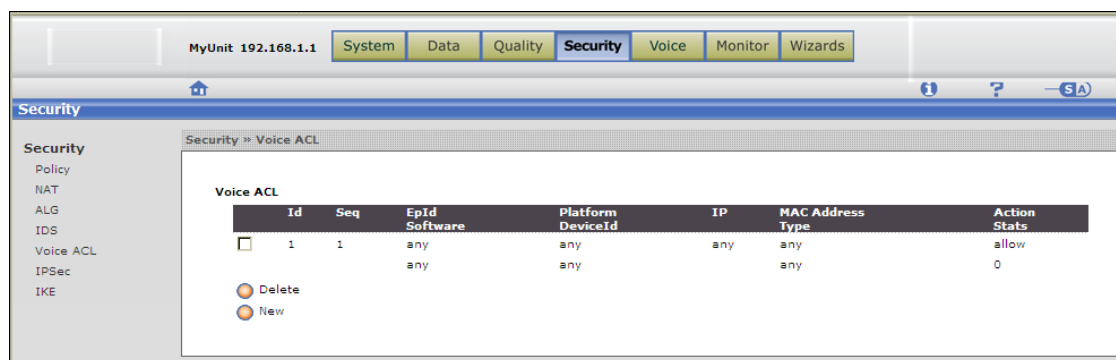
Total IDS attacks are reported on the Web UI home page in the **System** pane.

IDS also reports attacks as `Warning` entries in the system log. The log can be viewed on the Web UI home page, or with the CLI command **show logging internal**. To avoid filling the log (which can cause a denial of service), IDS reports only one attack for every 64 attacks detected.

## Voice ACL

The Access Control List (ACL) is a list of policy entries that determine which LAN endpoints are allowed to place and receive calls, for both SIP and MGCP devices. By default, the ACL includes a policy that allows all LAN endpoints to place and receive calls. To deny an endpoint call access, a policy denying access must be added to the ACL.

**Figure 40** Voice ACL page



The fields in this display are explained in the configuration instructions below, except for the Stats fields. That field reports the number of times an endpoint has been matched to this policy.

When an endpoint attempts to place or receive a call, authentication is performed. Information about the endpoint is compared to the policy entries in the ACL to determine if the endpoint is given access.

Information about the endpoint is provided by the session controller and, if available, by the Cisco Discovery Protocol (CDP). The session controller provides MAC address, IP address, signaling type, and endpoint ID. The CDP can provide Device ID, platform, and software version.

## Configuration

In the display pane, click **New** to open the configuration page. Fill in the fields as shown below. Click **Update** when finished.

To delete an entry, enable the check box next to the **Id** number on the display page, then click **Delete**.

<b>Id</b>	Enter a numeric identifier of the policy, or enter “new” for auto-numbering
<b>MAC Address</b>	MAC address of the endpoint in xx:xx:xx:xx:xx format.
<b>Epld</b>	Endpoint identifier in alphanumeric format.
<b>Software</b>	Software version of the endpoint.
<b>Platform</b>	Platform type of the endpoint.
<b>DeviceID</b>	Device ID of the endpoint.
<b>Seq</b>	Sequence number of the policy.
<b>IP</b>	IP address or range of address for the endpoints. Beginning address if entering a range of addresses.
<b>(range to)</b>	Ending IP address if entering a range of addresses.
<b>Type</b>	Signaling type of the endpoint. {any   mgcp   sip}
<b>Allow</b>	Whether the device is allowed or denied call access. Default is <b>allow</b> .

## IPSec/IKE and VPN

The BSGX4e supports Virtual Private Networks (VPNs) using the IP security (IPsec) protocol. An IPsec VPN serves as a point-to-point tunnel interface. See [page 152](#) for the VPN configuration process.

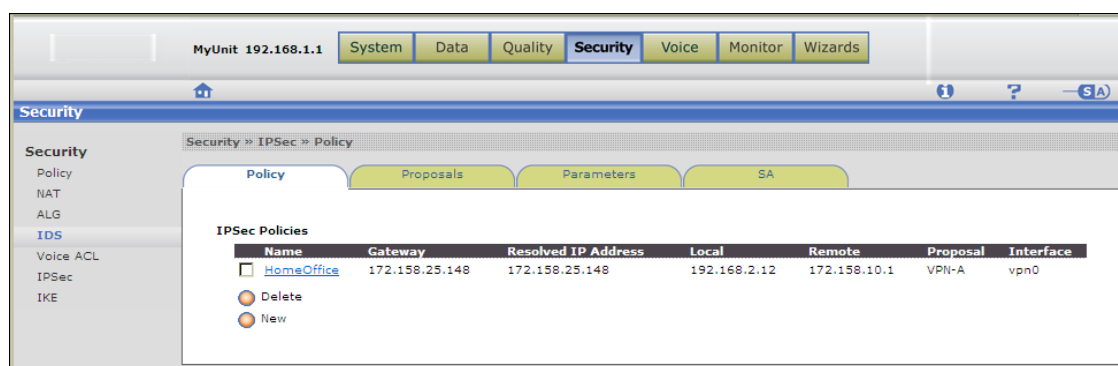
IPsec uses the Internet Key Exchange (IKE) protocol to set up its security associations (SAs). SAs determine how data is encrypted, decrypted, and authenticated by the secure gateways. When configured, the BSGX4e can function as a secure gateway.

After IPsec SAs are established the VPN becomes operational using IPsec tunneling to secure IP traffic between LANs. Each IP packet sent between LANs is encrypted inside an Encapsulated Security Payload (ESP) packet during transmission between the secure gateways.

### IPSec

IPsec provides data confidentiality, data integrity, and data authentication between peers. Configuration consists of creating a policy and a proposal, and configuring operational parameters.

**Figure 41** IPSec page



### Security > IPSec > Policy tab

An IPsec policy specifies the two secure networks that a VPN tunnel connects and the security parameters used to encrypt and decrypt traffic between the two networks. The creation of an IPsec policy also allows a VPN interface to be configured for the policy.

#### Configuration

In the display pane, click **New** to open the configuration page. Fill in the fields as shown below. Click **Update** when finished.

If a policy has already been defined, click the **Name** in the display to open the Properties page, then **Modify** to open the configuration page.

To delete an entry, enable the check box next to the policy name on the display page, then click **Delete**.

<b>Name</b>	Enter a unique name for this VPN.
<b>Gateway</b>	Enter the IP address of the remote secure gateway.
<b>Local</b>	Enter a local IP address secured by the VPN. Typically, this is a sub-network of the BSGX4e LAN (192.168.1.0/24). Valid entries are addresses specified as a range or as a subnet (x.x.x.x/yy). If specifying a range, enter the beginning address.
<b>(range to)</b>	If specifying a range for the local IP, enter the ending address.
<b>Remote</b>	Enter a remote IP address secured by the VPN. Valid values are addresses specified as a range or as a subnet (x.x.x.x/yy). If specifying a range, enter the beginning address.
<b>(range to)</b>	If specifying a range for the local IP, enter the ending address.
<b>Proposal</b>	Enter the name of the IPsec proposal. The default value is VPN-A, which is a proposal pre-defined in the BSGX4e.

## Security > IPSec > Proposals tab

An IPsec proposal is a set of security parameters used when negotiating an IPsec security association with a remote secure gateway. IPsec proposals are referenced by the IPsec policies.

The initial BSGX4e configuration provides a predefined IPsec proposal named VPN-A. This predefined proposal conforms with the recommendations for a standard IPsec cryptographic suite called VPN-A, as described in RFC 4308. It is configured with 3DES encryption and SHA authentication.

### Configuration

In the display pane, click **New** to open the configuration page. Fill in the fields as shown below. Click **Update** when finished.

To modify an existing proposal, click the **Name** in the display to open the Properties page, then **Modify** to open the configuration page. The pre-defined VPN-A proposal cannot be modified.

To delete an entry, enable the check box next to the policy name on the display page, then click **Delete**.

<b>Name</b>	Enter a unique name for this proposal.
<b>Encrypt</b>	Enter an encryption algorithm. For the AES algorithm, you can select a key size (128, 192, or 256 bits). If you select AES without a key size, IPsec uses the smallest key size supported by both peers. Your options are: <ul style="list-style-type: none"> <li>• 3DES</li> <li>• AES</li> <li>• AES128</li> <li>• AES192</li> <li>• AES256</li> </ul> The default is 3DES.

---

<b>Authentication</b>	Specify an authentication method. Your options are: <ul style="list-style-type: none"><li>• MD5</li><li>• SHA</li></ul>
-----------------------	--

---

## Security > IPSec > Parameters tab

Define the IPsec parameters for lifetimes of an IPsec security association and the Diffie-Hellman (DH) group to use for session key exchange.

The BSGX4e has two pre-defined lifetime parameters:

- ❑ Lifetime - The initial value used for negotiations with the remote host.
- ❑ Maximum Lifetime - The maximum value the BSGX4e accepts during negotiations.

## Configuration

In the display pane, click **Modify** to open the configuration page. Fill in the fields as shown below. Click **Update** when finished.

---

<b>Lifetime</b>	The security association lifetime used for negotiations. The default is 28800 sec. (8 hours).
<b>Maximum lifetime</b>	The maximum allowed security association lifetime. The default is 86400 sec. (24 hours).
<b>DH group</b>	Diffie-Hellman group to use for session key exchange. Your options are: <ul style="list-style-type: none"><li>• dh1024</li><li>• dh768</li><li>• nopfs</li><li>• auto</li></ul> <p>The default is <code>auto</code>, which provides for automatic negotiation. Use the value <code>nopfs</code> to disable <i>perfect forward secrecy</i>.</p>

---

## Security > IPSec > SA tab

This tab page displays negotiated security associations.

You can clear the display with the **Clear** button.

## IKE

The Internet Key Exchange (IKE) protocol provides utility services for IPSec. It defines how pairs of secure gateways negotiate IKE security associations (IKE SAs). The IKE SAs that the BSGX4e negotiates are determined by the configuration of IKE preshared keys and IKE parameters.

**Figure 42** IKE page

Priority	Encryption	Hash	Group
1	3DES	SHA	DH1024
2	3DES	SHA	DH768
3	3DES	MD5	DH1024
4	3DES	MD5	DH768
5	AES	SHA	DH1024
6	AES	SHA	DH768
7	AES	MD5	DH1024
8	AES	MD5	DH768
9	DES	SHA	DH1024
10	DES	SHA	DH768
11	DES	MD5	DH1024
12	DES	MD5	DH768
13	BLOWFISH	SHA	DH1024
14	BLOWFISH	SHA	DH768
15	BLOWFISH	MD5	DH1024
16	BLOWFISH	MD5	DH768

### Security > IKE > Policy tab

An IKE policy is a set of security parameters used when negotiating an IKE SA with a remote secure gateway. Sixteen predefined IKE policies are provided, offering every combination of encryption algorithm, hash digest, and Diffie-Hellman group available. The IKE policies that the BSGX4e can accept or offer are listed in order of priority.

**NOTE:** To negotiate an IKE SA, the remote gateway must have an IKE policy configured to match one of the local predefined IKE policies.

This page is display only. You cannot add to or modify these policies.

### Security > IKE > Preshared tab

This page is where you name the preshared key and the identify remote gateway with which the VPN is being established.

An IKE preshared key record specifies the preshared key used to encrypt Internet Security Association and Key Management Protocol (ISAKMP) messages. An IKE preshared key record defines the key (similar to a password) used to authenticate a remote secure gateway. ISAKMP differs from other key exchange protocols to separate it from security association management and key management exchanges.

Every IKE SA negotiation refers to a preshared key record to get the key value shared with the peer, that is, the remote secure gateway. Usually, each VPN has its own preshared key record. The same preshared key value must be configured at the remote secure gateway.

All IKE negotiations run over UDP on port 500. A firewall security policy must be configured to allow incoming UDP traffic to destination port 500 from the remote secure gateway.

The BSGX4e does not support aggressive mode IKE negotiations; the remote secure gateway must be configured to use main mode. The peer can be specified by a fixed IP address or by a host name. The DNS server resolves a host name to its current IP address. The IPsec SAs negotiated are determined by the configuration of IPsec policies and IPsec proposals.

### Configuration

In the display pane, click **New** to open the configuration page. Fill in the fields as shown below. Click **Update** when finished.

To modify an existing proposal, click the **Peer** name in the display to open the Properties page, then **Modify** to open the configuration page.

To delete an entry, enable the check box next to the policy name on the display page, then click **Delete**.

<b>Peer</b>	Host name or IP address of the remote gateway peer. Enter an IP address or host name.
<b>Key</b>	Name of the preshared key (up to 50 characters). The same preshared key must be configured at the remote gateway.

## Security > IKE > Parameters tab

The IKE security association is re-negotiated when its lifetime expires; the shorter the lifetime, the more frequently the IKE SA is re-negotiated. Therefore, a shorter lifetime increases security.

The BSGX4e has two pre-defined lifetime parameters:

- ❑ Lifetime – The initial value used for negotiations with the remote host.
- ❑ Maximum Lifetime – The maximum value the BSGX4e accepts during negotiations.

### Configuration

In the display pane, click **Modify** to open the configuration page. Fill in the fields as shown below. Click **Update** when finished.

<b>Lifetime</b>	Specify the IKE SA lifetime for negotiations. The initial setting is 86400 sec. (24 hours).
<b>Maximum lifetime</b>	Specify the maximum allowed IKE SA lifetime. The initial setting is 259200 sec. (72 hours).

## Security > IKE > SA tab

This tab page displays negotiated security associations.

You can clear the display with the **Clear** button.

## VPN

A VPN is a method of creating a secure private network over a shared insecure public network. A VPN is established by creating all the security (IPsec and IKE), routing and firewall policies between the peer hosts. The IPsec policy contains the network information that connects the peers of the VPN. Up to 10 VPN tunnels can be created concurrently.

To send WAN traffic through the VPN tunnel, the traffic is routed out the IP interface assigned to the tunnel (vpn(n)). The traffic is encrypted before it is sent. The IP interface allows features such as the VoIP session controller and user agent to be used across the VPN.

The basic procedure to create a VPN is as follows:

1. Configure IPsec policy. [\[page 147\]](#)
2. Configure the IKE pre-shared key. [\[page 150\]](#)
3. Configure the vpn(n) interface as a WAN IP interface. [\[page 70\]](#)
4. Create firewall policies for: [\[page 128\]](#)
  - ❑ LAN → vpn(n) all traffic
  - ❑ WAN → BSGX4e for security associations (source IP; UDP; port 500)
  - ❑ WAN → BSGX4e for ESP traffic (source IP; ESP protocol)
  - ❑ VPN → BSGX4e for tunneling to ISP.
5. Create a route table entry for vpn(n). [\[page 86\]](#)

## Configuration examples

The following examples show two common VPN scenarios:

- ❑ Office-to-office
- ❑ BSGX4e-to-ISP

### **Office-to-office example**

This example shows a typical configuration for a VPN between two BSGX4es located at a main office and a branch office. This example can generally apply to a BSGX4e tunneling to any VPN-capable device on the WAN.



You need the following network information to accomplish this task. The values shown are used in the example.

Shared key value: x359QWa78b3l12.

Main office IP addresses:

Main office gateway: 195.178.11.11

Main office LAN subnet: 192.168.1.0/24

Branch office IP addresses:

Branch office gateway: 194.23.7.34

Branch office LAN subnet: 192.168.2.0/24

### Configuration:

#### 1. Configure IPSec policy:

Security > IPSec

	Main Office	Branch Office
<b>Name</b>	Main	Branch
<b>Gateway</b>	194.23.7.34	195.178.11.11
<b>Local</b>	192.168.1.0/24	192.168.2.0/24
<b>(range to)</b>		
<b>Remote</b>	192.168.2.0/24	192.168.1.0/24
<b>(range to)</b>		
<b>Proposal</b>	VPN-A	VPN-A

Note the **Interface** designator listed on the display page. You need this in [Step 3](#).

#### 2. Configure the IKE pre-shared key.

Security > IKE

	Main Office	Branch Office
<b>Peer</b>	194.23.7.34	195.178.11.11
<b>Key</b>	x359QWa78b3l12	x359QWa78b3l12

3. Configure the vpn(n) interface as a WAN IP interface.

Data > IP

	Main office	Branch office
<b>Interface value</b>	vpn0 (from <a href="#">Step 1.</a> )	vpn0
<b>IP Addr/Mask</b>	10.10.10.1/24	10.10.10.2/24
<b>MTU</b>	1500 (default)	1500 (default)
<b>DHCP client</b>	off (default)	off (default)
<b>Status</b>	up (default)	up (default)
<b>Speed</b>	auto (default)	auto (default)

4. Create firewall policies for:

- ❑ LAN → vpn(n) all traffic
- ❑ WAN → BSGX4e for security associations (source IP; UDP dport 500)
- ❑ WAN → BSGX4e for ESP traffic (source IP; ESP prot)

Security > Policy

**Main office**

	Policy 1	Policy 2	Policy 3
<b>Index</b>	new	new	new
<b>From</b>	eth1	eth0	eth0
<b>To</b>	vpn0	self	self
<b>Source IP (range to)</b>	any	194.23.7.34	194.23.7.34
<b>Dest IP (range to)</b>	any	any	any
<b>Source port (range to)</b>	any	any	any
<b>Dest port (range to)</b>	any	500	any
<b>Proto</b>	any	udp	esp
<b>NAT</b>	0	0	0
<b>QoS</b>			
<b>ToS</b>	any	any	any
<b>Sequence</b>	begin	begin	begin
<b>action</b>	allow	allow	allow

**Branch office**

	<b>Policy 1</b>	<b>Policy 2</b>	<b>Policy 3</b>
<b>Index</b>	new	new	new
<b>From</b>	eth1	eth0	eth0
<b>To</b>	vpn0	self	self
<b>Source IP (range to)</b>	any	195.178.11.11	195.178.11.11
<b>Dest IP (range to)</b>	any	any	any
<b>Source port (range to)</b>	any	any	any
<b>Dest port (range to)</b>	any	500	any
<b>Proto</b>	any	udp	esp
<b>NAT</b>	0	0	0
<b>QoS</b>			
<b>ToS</b>	any	any	any
<b>Sequence</b>	begin	begin	begin
<b>action</b>	allow	allow	allow

**5.** Create a route table entry for vpn0.

Data &gt; Routes Table

	<b>Main office</b>	<b>Branch office</b>
<b>Destination</b>	192.168.2.0/24	10.10.10.2/24
<b>Gateway</b>	<i>not required</i>	<i>not required</i>
<b>Interface</b>	vpn0	vpn0

**BSGX4e-to-ISP example**

This example shows a typical configuration for a VPN between two BSGX4es located at a main office and a branch office.

You need the following network information to accomplish this task. The values shown are used in the example.

Shared key value is x232skd24scefk3o.

IP addresses used are as follows:

BSGX4e: 192.168.100.1

ISP: 192.168.100.2

VPN gateway at ISP: 10.254.254.254

**Configuration:****1.** Configure IPSec policy:

Security &gt; IPSec

<b>Name</b>	Tunnel
<b>Gateway</b>	10.254.254.254
<b>Local</b>	192.168.100.1
<b>(range to)</b>	
<b>Remote</b>	192.168.100.2
<b>(range to)</b>	
<b>Proposal</b>	VPN-A

Note the **Interface** designator shown on the display page. You need this in [Step 3](#).

**2.** Configure the IKE pre-shared key.

Security &gt; IKE

<b>Peer</b>	10.254.254.254
<b>Key</b>	x232skd24scefk3o

**3.** Configure the vpn(n) interface as a WAN IP interface.

Data &gt; IP

<b>Interface Value</b>	vpn1 (from <a href="#">Step 1.</a> )
<b>IP Addr/Mask</b>	192.168.100.1
<b>MTU</b>	1500 (default)
<b>DHCP Client</b>	off (default)
<b>Status</b>	up (default)
<b>Speed</b>	auto (default)

**4.** Enable NAT on the vpn0 interface.

Security &gt; NAT

<b>Interface</b>	vpn1
<b>Status</b>	on

**5.** Create firewall policies for:

- ❑ LAN → vpn(n) all traffic
- ❑ WAN → BSGX4e for security associations (source IP; UDP dport 500)
- ❑ WAN → BSGX4e for ESP traffic (source IP; ESP prot)
- ❑ VPN → BSGX4e for ICMP protocol (ping)

Security &gt; Policy

	Policy 1	Policy 2	Policy 3	Policy 4
<b>Index</b>	new	new	new	new
<b>From</b>	eth1	eth0	eth0	vpn0
<b>To</b>	vpn0	self	self	self
<b>Source IP (range to)</b>	any	10.254.254.254	10.254.254.254	any
<b>Dest IP (range to)</b>	any	any	any	any
<b>Source port (range to)</b>	any	any	any	any
<b>Dest port (range to)</b>	any	500	any	any
<b>Proto</b>	any	udp	esp	icmp
<b>NAT</b>	0	0	0	0
<b>QoS</b>				
<b>ToS</b>	any	any	any	any
<b>Sequence</b>	begin	begin	begin	begin
<b>action</b>	allow	allow	allow	allow

**6.** Create a route table entry for vpn0.

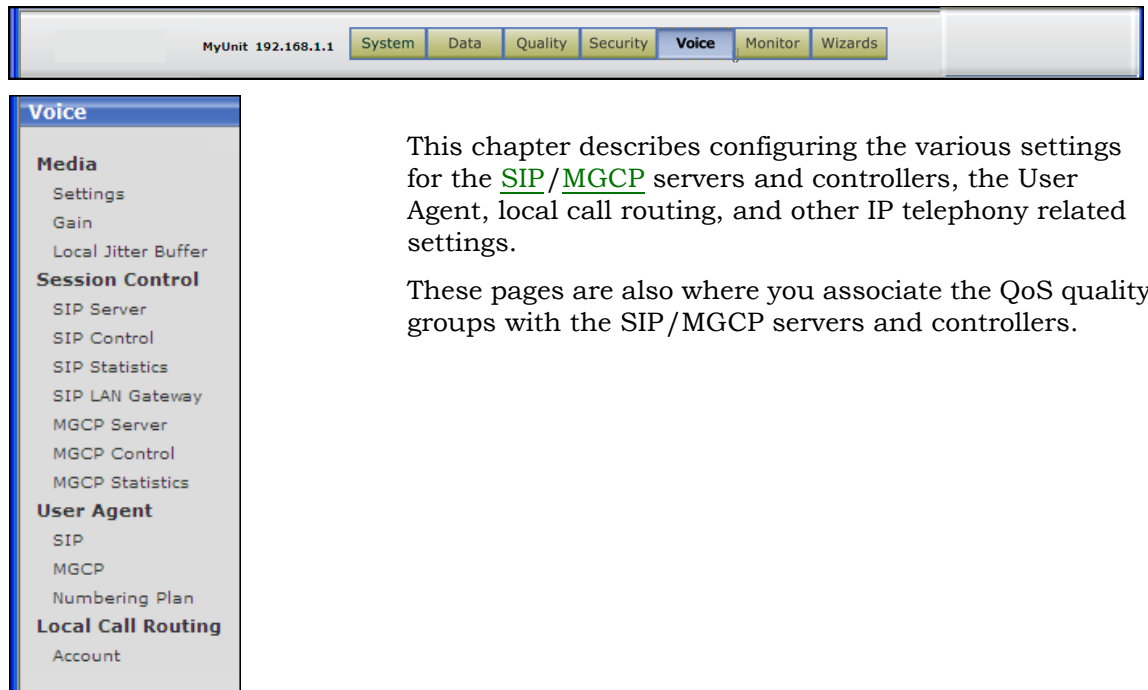
Data &gt; Routes Table

<b>Destination</b>	0.0.0.0
<b>Gateway</b>	<i>not required</i>
<b>Interface</b>	vpn0

**NOTE:** This route with Destination 0.0.0.0 sends all traffic on the tunnel unless the traffic has another explicit route. This also applies to VoIP traffic.



# 6 VOICE PAGES



The following list provides an overview of the configuration and status functions on the Voice menu button:

- **Media**
  - **Settings** ([page 161](#))  
Configures Direct Media, RTP ports, and sets the maximum simultaneous calls. Identifies the VoIP media quality group and default video bandwidth.
  - **Gain** ([page 162](#))  
Sets the transmit/receive gain for the Phone (FXS) and Line (FXO) ports.
  - **Local jitter buffer** ([page 162](#))  
Configures the jitter buffer and displays statistics.
- **Session controller** ([page 164](#))
  - **SIP / MGCP server** ([page 164](#)/[page 171](#))  
Creates a configuration profile for server access. Displays server status.
  - **SIP / MGCP control** ([page 167](#)/[page 172](#))  
Configures parameters of the session controller and associates the control signal quality group. Displays session controller status, active calls, and registered endpoints.

- ❑ **SIP / MGCP statistics** ([page 171](#)/[page 174](#))  
Displays cumulative operational statistics for control signal messages and call traffic.
- ❑ **SIP LAN gateway** ([page 171](#))  
Configures the LAN for a gateway connection.
- **User agent** (BSGX4e) ([page 175](#))
  - ❑ **SIP/MGCP** ([page 176](#)/[page 179](#))  
Configures the SIP or MGCP User Agent for analog devices.
  - ❑ **Numbering plan** ([page 181](#))  
Configures the User Agent for number-based special features.
- **Local call routing** ([page 185](#))  
Sets emergency phone connection to a PSTN and establishes LAN-to-LAN calls when a VoIP server is not reachable.



## Media

### Voice > Media > Settings

This page configures various parameters for processing video and VoIP media streams, including associating the VoIP QoS quality group with the session controller. VoIP control signals are associated in the session controller settings ([page 167](#)).

You must create the quality groups before proceeding with this section (See the section, [Group page on page 112](#)).

### Configuration

There are technical notes below the table discussing direct media and the default video bandwidth. Click **Modify** to open the configuration page. The configuration parameters are as follows:

<b>Direct media enabled</b>	Enables use of direct media ( <a href="#">RTP</a> ) connections between two endpoints on the BSGX4e LAN. Default is <b>no</b> .
<b>RTP ports (range to)</b>	Range of RTP ports to use (low# – high#). The RTP range must contain at least 1000 values and must not overlap ports configured for existing services in the BSGX4e. Normally, two ports in the range are used for each media connection, one for RTP and the other for <a href="#">RTCP</a> . Default range is <b>13000 – 14999</b> .
<b>AudioQoS</b>	QoS quality group to which the VoIP media is assigned. This group has to be created prior to this step. The Initial Setup Wizard creates a quality group named <b>voiceqos</b> for purpose.
<b>MaxConn</b>	This field is for engineering use only. Do not change the existing value.
<b>DefaultVideoBW</b>	Sets the video quality group bandwidth for a given session when the SIP video application uses a codec that is not recognized by the BSGX4e. Default is <b>640000</b> bps.

#### **Direct media**

By default, media stream routes are established between each device endpoint and the BSGX4e. The BSGX4e then bridges them to establish the end-to-end communication path to the devices on the BSGX4e LAN.

If Direct Media is enabled, media routes are established directly between two LAN endpoints for a BSGX4e LAN-to-LAN call.

#### **Default video bandwidth**

The DefaultVideoBW parameter allows you to specify a default video bandwidth when the video codec does not specify the required bandwidth for a session.

This occurs when the Session Description Protocol (SDP) codec does not contain bandwidth data, or when the video application is using a codec not supported by the BSGX4e. See [SIP video on page 113](#) for more discussion.

## Voice > Media > Gain

The Gain page of the BSGX4e 2xx series models has two tabs: FXO Gain and FXS Gain. These settings modify the [DSP](#) gain for the PHONE ([FXS](#)) and LINE ([FXO](#)) ports. The BSGX4e 4xx models do not have a PHONE port so they do not have an FXS Gain tab.

Impedance can also be modified with the Command Line Interface.

The LINE port connects the BSGX4e to the PSTN and provides limited backup phone service if SIP or MGCP servers are not available, and 911 service. The PHONE port on the BSGX4e allows you to connect an analog device, such as a phone or fax, for conversion to IP transport. See [Local call routing on page 185](#) for more details on backup and 911 service.

Each port has a Tx (transmit; [DAC](#)) and Rx (receive; [ADC](#)) setting. Negative numbers are allowed and are indicated with a dash (-).

The Tx and Rx defaults for FXO are 0 dB, and for FXS they are -6 dB.

## Voice > Media > Local Jitter Buffer

The jitter buffer adds small delay to incoming packets in order to regularize the packet flow and reduce jitter. This page has two tabs:

- ❑ The **Settings** tab for configuring the buffer, and;
- ❑ The **Stats** tab for monitoring performance.

The buffer length can be specified as *fixed* or *adaptive*. A fixed length buffer has an absolute length; an adaptive buffer has a minimum and maximum limit within which it varies with traffic demand.

When modifying the buffer length, increased length causes more delay and less loss; decreasing the length causes more loss and less delay.

### Settings tab

Click **Modify** to open the configuration page. The configuration parameters are as follows:

<b>Mode</b>	Jitter buffer type ( <b>fixed</b>   <b>adaptive</b> ). Default is adaptive.
<b>Maximum</b>	Maximum delay (ms) introduced by the jitter buffer. Applicable only to adaptive mode. Default is 120 ms.
<b>Nominal</b>	Nominal delay (ms) introduced by the jitter buffer. Default is 40 ms.
<b>Minimum</b>	Minimum delay (ms) introduced by the jitter buffer. Applicable only to adaptive mode. Default is 20 ms.

## Stats tab

The following statistics are available on the **Stats** page:

<b>Port</b>	1 – Phone (FXS) 2 – Line (FXO)
<b>RxFrames</b>	Number of packets received.
<b>CurrJitter</b>	Current average jitter detected.
<b>CurrDelay</b>	Current packet delay due to the jitter buffer (ms).
<b>MinDelay</b>	Minimum packet delay due to the jitter buffer (ms).
<b>MaxDelay</b>	Maximum packet delay due to the jitter buffer (ms).
<b>Overflowed</b>	Number of packets dropped due to overflow.
<b>Underrun</b>	Number of packets dropped due to underrun.
<b>OutOfOrder</b>	Number of packets out of sequential order.
<b>Duplicated</b>	Number of packets dropped due to duplication.
<b>LateDropped</b>	Number of packets dropped due to late arrival.

---

## Session control

This sections is where you configure SIP and MGCP servers, the session controller, and the SIP LAN gateway if needed. These pages also display SIP/MGCP statistics.

To configure either SIP or MGCP session control functions, perform this sequence of tasks:

1. Configure access to one or more SIP/MGCP servers.
2. Configure the SIP/MGCP session controller.
3. Configure the SIP/MGCP user agent.
4. Configure any SIP/MGCP devices connected to the LAN ports.

---

**NOTE:** The firewall is automatically configured to allow traffic between the session controller and the SIP or MGCP servers.

---

### Voice > Session Control > SIP Server

The SIP server configuration profile determines how the BSGX4e session controller accesses SIP proxy servers to provide VoIP service. This page has two tabs:

- **Configuration** – Server access configuration profile for the session controller.
- **Status** – Displays all the servers, the server in use, and their operational status.

A server profile can specify up to three SIP proxy servers or it can specify no servers. If no server is explicitly specified, the session controller locates a SIP proxy server using the DNS service ([page 36](#)). The DNS service is disabled by default.

## Configuration tab

Click **New** to open the configuration page. There are technical notes below the table discussing proxy servers and inbound servers. The configuration parameters for the SIP server profile are as follows:

<b>Name</b>	Enter a name for the server profile being created.
<b>Domain</b>	Registrar domain for registering SIP phones (FQDN   IP address). This parameter is required.
<b>Proxy1</b>	First SIP proxy server (either a fully qualified domain name [FQDN] or an IP address). If no proxy server is specified, the session controller uses DNS to find its proxy servers.
<b>Port1</b>	Port number of the first proxy server. The default is <b>5060</b> .
<b>Proxy2</b>	Optional second SIP proxy server (FQDN   IP address).
<b>Port2</b>	Port number of the second proxy server. The default is <b>5060</b> .
<b>Proxy3</b>	Optional third SIP proxy server (FQDN   IP address).
<b>Port3</b>	Port number of the third proxy server. The default is <b>5060</b> .
<b>IBServer1</b>	Optional additional inbound servers (single address or range). The firewall is automatically updated to allow the session control to receive SIP messages from these additional servers.
<b>IBServer2</b>	Optional additional inbound servers (single address or range).
<b>IBServer3</b>	Optional additional inbound servers (single address or range).
<b>Retries</b>	Number of retries before a SIP server is blacklisted. The default is <b>4</b> retries. (Specifying <b>0</b> disables call server failover.)
<b>Blacklist</b>	Blacklist timer in seconds. The default is <b>60</b> seconds (10 minutes).
<b>Heartbeat</b>	Indicates whether server heartbeat monitoring is enabled ( <b>yes</b>   <b>no</b> ). By checking for the server heartbeat, the session controller can determine whether the server is available. The default is <b>yes</b> . See <a href="#">caution</a> note below.
<b>HBTimer1</b>	Time interval between heartbeat packets for active servers (in seconds). The default is <b>30</b> seconds.
<b>HBTimer2</b>	Time interval between heartbeat packets for temporarily unavailable servers (in seconds). The default is <b>15</b> seconds.



**CAUTION:** Ensure the **Heartbeat** parameter is enabled.

The BSGX4e can operate in local call routing mode ([page 185](#)) after start-up. During start-up, if the session controller cannot connect with a SIP server because network connectivity is still setting up, the BSGX4e implements local call routing. Normal operation resumes only when the heartbeat monitor detects a signal from the SIP server.

### **Server failover**

Server failover prevents VoIP service interruption by accessing backup proxy servers, if configured in the server profile.

The session controller detects that the call server might be down if it:

- ❑ Cannot connect to the call server (WAN interface unplugged, no IP route, and so on.)
- ❑ Does not receive SIP replies from it.

When a proxy server might be down, the session controller attempts some number of retries before it marks the server as down. The server profile specifies the number of retries.

If the proxy server is still unavailable after the retries, it is marked as down for the duration of the blacklist timer, which is set in the server profile. After the timer expires for a downed server, the session controller attempts to re-contact the downed server.

While a SIP proxy server is marked as down, the session controller uses the next available proxy server. When a higher-priority server becomes available, the session controller switches back to that server.

If the current SIP proxy server goes down and no other server is available, the session controller repeatedly attempts to reconnect to the proxy server and resumes call service as soon as the server comes back up.

### **Inbound servers**

The SIP session controller can accept inbound messages from additional SIP servers if those servers are configured in the server profile. A single IP address or a range of addresses can be specified for the IBServer1, IBServer2, and IBServer3 parameters.

The firewall is automatically updated to accept SIP messages from the additional inbound servers.

### **Status tab**

The Status tab displays information for all SIP servers. The following status messages are also displayed:

<b>Active</b>	<b>Yes</b> – This server profile is in use.
<b>Mode</b>	<b>DNS-SRV</b> – DNS locates the proxies. <b>Manual</b> – The proxy servers are specified explicitly.
<b>Proxy1</b>	<b>(In-use)</b> – This proxy is currently in use.
<b>Proxy2</b>	<b>(Ready)</b> – This proxy is available, but is not currently in use.
<b>Proxy3</b>	<b>(Down)</b> – This proxy is not available, but is in an active state.

## Voice > Session Control > SIP Control

The Session Control page contains configuration and display tabs for processing VoIP control signals. The page has four tabs:

- ❑ **Control** – Configuration parameters for control signal processing, and association of the QoS signaling quality group. (QoS media streams are detected by the media settings ([page 161](#)).)
- ❑ **Status** – SIP session controller operational status display.
- ❑ **Calls** – Display of call traffic through the session controller.
- ❑ **Endpoints** – LAN endpoints (devices) registered through the SIP session controller.

### Control tab

Configure the parameters for detecting VoIP control signals and routing them to the SIP server on this tab page. A server profile ([page 164](#)) must be configured before it can be specified for use by the session controller.

Click **Modify** to open the configuration page. The configuration parameters for the SIP server profile are as follows:

<b>Server</b>	Select the name of the SIP server profile to be used from the drop-down list. This is the server configured on the SIP Server page ( <a href="#">page 164</a> ).
<b>Local Domain</b>	Local domain for LAN endpoints. SIP messages that do not match the domain are discarded. Optional.
<b>WAN Rx Port</b>	Port on which to listen for SIP signaling messages from the WAN. Enter the port number, or the beginning number of a range. Default is <b>5060</b> .
<b>(range to)</b>	Ending number of the WAN port range.
<b>LAN Rx Port</b>	Port on which to listen for SIP signaling messages from the LAN. Enter the port number, or the beginning number of a range. Default is <b>5060</b> .
<b>(range to)</b>	Ending number of the LAN port range.
<b>Timer T1</b>	Minimum retransmission time interval (milliseconds). Default is <b>500</b> ms.
<b>Timer T2</b>	Maximum retransmission time interval (milliseconds). Default is <b>4000</b> ms.
<b>Timer B</b>	Timeout interval for INVITE transactions (in seconds). Default is <b>16</b> seconds.
<b>Timer F</b>	Timeout interval for non-INVITE transactions (in seconds). Default is <b>32</b> seconds.
<b>Timer C</b>	Timeout interval for proxy INVITE transactions (in seconds). Default is <b>180</b> seconds (3 minutes).

<b>Max Calls</b>	<p>Call Admission Control. Maximum number of SIP calls allowed simultaneously. Default is <b>50</b>. Change this default per your license agreement.</p> <p>The number of allowable calls is defined by your license agreement. Your choices are:</p> <p>BSGX4e – 10 or 30 calls</p> <p><b>NOTE:</b> This field also sets the display scale on the System &gt; Status page. See <a href="#">System &gt; Status &gt; Current Calls panel on page 29</a>.</p>
<b>Signaling QoS Group</b>	<p>The QoS quality group for protection of the SIP signaling messages. The Initial Setup Wizard creates a quality group named <b>voiceqos</b> for this purpose.</p> <p>Select the appropriate group from the drop-down list.</p>
<b>Relay Unknown Content Types</b>	<p>Allow unknown content types to be relayed to the SIP server. Default is <b>yes</b>.</p>
<b>Switch Type</b>	<p>Vendor of server that provides forking function.</p> <p>BSGX4e interoperates with various softswitches that offer multi-line (forking) capabilities. These switches require special handling by the session controller. The details are described below.</p> <p>When you select a vendor, the session controller formats call ID codes to operate with the switch multi-line feature.</p> <p>The following softswitches are supported:</p> <ul style="list-style-type: none"> <li>• Broadsoft</li> <li>• Sylanro</li> <li>• Nortel CS 2000 (selected LG-Nortel phone models 6812 and 6830)</li> </ul> <p>Siemens and Other appear as other options, but are not currently supported. Future versions may support Siemens and other vendors. In this release, forking is disabled by default if Siemens or Other is selected.</p>
<b>Enable Forking</b>	<p>Enable and disable forking support.</p> <p>If you select Sylanro as your switch type, you must enable forking.</p> <p>For all other switch types, you must disable forking.</p>

### ***Multi-line/forking***

Multi-line/forking is the capability to route an incoming SIP call to multiple phones with the same number at different locations. Examples of this scenario include an engineer with phones at an office desk and lab station; an executive with multiple offices; a receptionist who has desks in different locations. Multi-line/forking routes an incoming call to all phone locations for these users. Many softswitch vendors offer this feature, but they all employ proprietary designs and implementation.

Forking is managed by the SIP server with which the BSGX4e communicates. The forking parameter should be enabled for those softswitches that specifically support SIP forking. Other softswitches may use a proprietary multi-line function that functions the same as SIP forking. The forking parameter need not be enabled for those switches.

Each phone registers with the BSGX4e session controller as a SIP endpoint. The endpoint is identified to a specific user by the phone number and the phone's IP address.



Any incoming SIP call for a given user is then routed by the SIP server to all of that user's registered endpoints with that phone number.

Forking also applies to an analog phone connected to the BSGX4e User Agent. The session controller registers the phone as an endpoint associated with a given user.

The maximum number of forked lines a user can have is determined by the configuration of the SIP server. If the number exceeds the limit of the server, new registration requests are declined.

## Status tab

This tab page displays the operational status of the SIP session controller (SSC).

The fields are self-explanatory. The `SSC Server Ready` field indicates whether or not the server is active.

## Calls tab

This tab page displays statistics on the current call traffic. The fields are mostly self-explanatory.

The section, **Total outbound calls from LAN**, applies to calls that originated from LAN endpoints. The section, **Total inbound calls from WAN**, applies to calls that originated from the SIP server.

A local call from a LAN endpoint to another LAN endpoint is shown twice in the statistics: it is counted both as a LAN outbound call and as a WAN inbound call.

## Endpoints tab

This tab page displays the LAN endpoints (devices) registered through the SIP session controller.

The fields are mostly self-explanatory.

`Act Calls` – Real-time count of currently active calls for the endpoint.

`Reg Timeout` – The number of seconds before the call registration expires. The initial value is taken from the `Expires` field of the SIP REGISTER method. The value is decremented each second.

## Technical Reference

### Endpoint status handling

Endpoint status handling saves LAN endpoint information in non-volatile memory so it can be retrieved after a restart. This is done when the LAN endpoint is registered to the SIP server. This function is not configurable for the SIP session controller.

### Configuring endpoints

This section provides guidelines to configure the SIP endpoints to be managed by the BSGX4e. For an endpoint to be able to place and receive calls, it must be:

- ❑ Allowed access by the Access Control List (ACL).
- ❑ Registered with the SIP server through the SIP session controller.

These requirements also apply to the SIP User Agent ([page 175](#)) because the session controller handles it as an endpoint. However, unlike other endpoints, an ACL entry cannot be configured to disallow the User Agent.

Endpoints register with the SIP server through the session controller. To be able to be registered, the SIP endpoints must be configured as follows:

- ❑ SIP registration must be enabled.
- ❑ The SIP proxy must be the LAN IP address of the BSGX4e.
- ❑ The SIP domain must be the LAN IP address of the BSGX4e.
- ❑ The SIP proxy port must be the one configured as the LAN Rx port in the SIP session controller. See [Control tab on page 167](#).
- ❑ No SIP outbound proxy is needed.
- ❑ NAT/firewall traversal must be disabled.

### Configuration example

For a Cisco SIP phone 7960, firmware POS3-07-5-00, the following configuration is required (interactive menu or text configuration file):

<b>proxy_register</b>	1 (enabled)
<b>proxy1_address</b>	LAN IP address of the BSGX4e
<b>proxy1_port</b>	LAN Rx port of the SIP session controller
<b>outbound_proxy</b>	<blank>
<b>nat_enabled</b>	0
<b>domain</b>	LAN IP address of the BSGX4e

### IP address change

If the IP address of the BSGX4e changes, all SIP registrations expire and all VoIP services stop working. If this happens you have two choices for remedy:

- ❑ Wait for the SIP server to finish its registration process, or;
- ❑ Manually unregister and re-register your SIP phones.

To force the User Agent to re-register, disable then re-enable it on the User Agent configurations pages: [page 176](#) for SIP User Agent or [page 179](#) for MGCP User Agent.

## Voice > Session Control > SIP Statistics

This page shows cumulative operational statistics for SIP signaling control messages on the **Messages** tab, and calls status on the **Calls** tab.

- **Messages tab**

The fields report error data except for the following, which report normal packet traffic:

```
WanMsgRecvCount
WanMsgProcCount
LanMsgRecvCount
LanMsgProcCount
TotalMsgRxCount
MsgPerSec
```

- **Calls tab**

The section, **Total outbound calls from LAN**, applies to calls that originated from LAN endpoints. The section, **Total inbound calls from WAN**, applies to calls that originated from the SIP server.

A local call from a LAN endpoint to another LAN endpoint is shown twice in the statistics; it is counted both as a LAN outbound call and as a WAN inbound call. This is this without Direct Media enabled.

## Voice > Session Control > SIP LAN Gateway

If a gateway device is attached to the BSGX4e's LAN switch, an IP address is required for the gateway. An optional domain name can also be provided.

Click **Modify** to access the configuration page:

<b>Domain</b>	Domain name for the SIP gateway.
<b>IP Addr</b>	IP address for the SIP gateway. Single address or beginning of range.
<b>(range to)</b>	Ending address of range.
<b>port</b>	Signaling Rx port for the SIP gateway. Single port or beginning of range. Default is <b>5060</b> .
<b>(range to)</b>	Ending port of range.

## Voice > Session Control > MGCP Server

The MGCP server configuration profile determines how the BSGX4e session controller accesses MGCP servers to provide VoIP service. This page has two tabs:

- **Configuration** – Server access configuration profile for the session controller.
- **Status** – Displays the server in use and its operational status.

The server profile allows you to specify three MGCP servers for failover purposes. (The failover description on [page 166](#) applies also to MGCP). However, unlike SIP, MGCP servers cannot be located by DNS.

## Configuration tab

Click **New** to open the configuration page. The configuration parameters for the MGCP server profile are as follows:

<b>Name</b>	Name of the server profile to be created.
<b>MGC1</b>	First Media Gateway Controller (either a fully qualified domain name [FQDN] or an IP address).
<b>Port1</b>	Port number for <b>mgc1</b> . Default is <b>2727</b> .
<b>MGC2</b>	Optional second Media Gateway Controller (FQDN   IP address).
<b>Port2</b>	Port number for <b>mgc2</b> . Default is <b>2727</b> .
<b>MGC3</b>	Optional third Media Gateway Controller (FQDN   IP address).
<b>Port3</b>	Port number for <b>mgc3</b> . Default is <b>2727</b> .
<b>Retries</b>	Number of retries before an MGC server is blacklisted. Entering <b>0</b> disables call server failover. Default is <b>5</b> retries.
<b>Blacklist</b>	Blacklist timer in seconds. Default is <b>600</b> seconds (10 minutes).

## Status tab

The Status tab displays information for the active server profile. The following status messages are also displayed:

<b>Active</b>	<b>Yes</b> – This server profile is in use.
<b>MGC1</b>	<b>(In-use)</b> – This server is currently in use.
<b>MGC2</b>	<b>(Ready)</b> – This server is available, but is not currently in use.
<b>MGC3</b>	<b>(Down)</b> – This server is not available, but is in an active state.

## Voice > Session Control > MGCP Control

The Session Control page contains configuration and display tabs for processing VoIP control signals. The page has four tabs:

- ❑ **Control** – Configuration parameters for control signal processing, and association of the QoS signaling quality group. (VoIP media streams are detected by the media settings ([page 161](#)).)
- ❑ **Status** – MGCP session controller operational status display.
- ❑ **Calls** – Display of call traffic through the session controller.
- ❑ **Endpoints** – LAN endpoints (devices) registered through the MGCP session controller.

## Control tab

Configure the parameters for detecting VoIP control signals and routing them to the MGCP server on this tab page. A server profile ([page 171](#)) must be configured before it can be specified for use by the session controller.

Click **Modify** to open the configuration page:

<b>Server</b>	Select the name of the MGCP server profile to be used from the drop-down list. This is the server configured on the MGCP Server page ( <a href="#">page 171</a> ).
<b>WAN Rx Port</b>	Port on which to listen for MGCP signaling messages from the WAN. Enter the port number, or the beginning number of a range. Default is <b>2427</b> .
<b>(range to)</b>	Ending number of the WAN port range.
<b>LAN Rx Port</b>	Port on which to listen for MGCP signaling messages from the LAN. Enter the port number, or the beginning number of a range. Default is <b>2727</b> .
<b>(range to)</b>	Ending number of the LAN port range.
<b>Keep Alive</b>	Interval between keep-alive messages sent to the MGC server. Enter zero (0) to disable. Default is 0.
<b>EP Timeout</b>	Endpoint timeout interval (in seconds). The default is 3600 seconds (one hour). See Endpoint Status Handling on <a href="#">page 174</a> .
<b>Max Calls</b>	Call Admission Control. Maximum number of MGCP calls allowed simultaneously. Default is <b>50</b> . Change this default per your license agreement. The number of allowable calls is defined by your license agreement. Your choices are: BSGX4e – 10 or 30 calls
<b>Signaling QoS Group</b>	The QoS quality group for protection of the MGCP signaling messages. The group must have been already created. See <a href="#">Quality &gt; Group &gt; Group tab on page 112</a> . Select the appropriate group from the drop-down list.

## Status tab

This tab page displays the operational status of the MGCP session controller.

The fields are self-explanatory. The MGC Server Ready field indicates whether or not the server is active.

## Calls tab

This tab page displays statistics on the current call traffic. The fields are mostly self-explanatory.

This displayed data includes when a call is active between “A party” and “B party,” the state (outbound or inbound), the protocol, the quality, and the start time and duration of the call.

## Endpoints tab

This tab page displays the LAN endpoints (devices) as registered through the MGCP session controller.

The fields are mostly self-explanatory.

**CA Port**

Port to which call signals are sent; extracted from the last MGCP message received from the MGCP server including a Notified Entity.

**Act Calls**

Currently active calls for the endpoint. It is incremented each time the LAN endpoint places or receives a call. It is decremented when the call is torn down.

**EP Timeout**

Number of seconds before the registration expires. The initial value is taken from the EP timeout setting. The value is decremented each second.

**Endpoint status handling**

Endpoint status handling saves LAN endpoint information in non-volatile memory so it can be retrieved after a restart. This is done when the LAN endpoint is registered to the MGCP session controller. This function is not configurable for the MGCP session controller.

The session controller periodically checks the status of each LAN endpoint using the MGCP method AUEP. When a LAN endpoint answers, the endpoint timer (remaining active time) is reset. If the endpoint does not answer, the MGCP session controller marks it as down and rejects all calls terminating at that endpoint.

The only configurable value in Endpoint Status Handling is the value of the endpoint timer. The default timer value is 3600 seconds (one hour). This value can be changed by the **EP Timeout** parameter on the [Control tab on page 172](#).

## Voice > Session Control > MGCP Statistics

This page shows cumulative operational statistics for MGCP signaling control messages on the **Messages** tab, and calls status on the **Calls** tab.

- **Messages** tab

The fields report error data except for the following, which report normal packet traffic:

- WanMsgRecvCount
- WanMsgProcCount
- LanMsgRecvCount
- LanMsgProcCount
- TotalMsgRxCount
- MsgPerSec

- **Calls** tab

The section, **Total outbound calls from LAN**, applies to calls that originated from LAN endpoints. The section, **Total inbound calls from WAN**, applies to calls that originated from the MGCP server.

A local call from a LAN endpoint to another LAN endpoint is shown twice in the statistics; it is counted both as a LAN outbound call and as a WAN inbound call. This is this without Direct Media enabled.

---

## User agent

---

**NOTE:** The User agent applies to only the BSGX4e.

---

The BSGX4e can act as a VoIP gateway allowing analog devices to use either SIP or MGCP. In the BSGX4e, this gateway is called a *User Agent*.

The User agent allows an analog device (phone, modem, or fax machine) to use VoIP as its communication media. The analog device must be connected to the BSGX4e's Phone (FXS) port.

The device connected to the Phone port can be a single analog device, or it can be a gateway device that, in turn, connects to multiple analog devices.

### Dependencies

- The SIP or MGCP session controller must be configured before the User Agent is enabled. See the section, [Session control on page 164](#).
- Only one configuration profile is allowed for the User Agent.
- Codecs

Up to four codecs can be configured. The order in which they are listed is the order in which negotiations are attempted.

If you configure any codec as NOT USED, negotiation attempts stop at that point. Codecs listed below this are ignored.

The supported codecs are G.711 u-law (PCMU), G.711 a-law (PCMA), and G.729, all with 10 ms or 20 ms RTP packet interval.

- Currently, Fax T.38 is not supported.
- The Phone (FXS) port must be properly configured for the User Agent to function. Setting the Country parameter configures the Phone port for the supported countries. See the section, [System > Overview > System Information panel on page 32](#) for the list of supported countries.



**CAUTION:** Phone port manual configuration must be performed only by professional personnel with a technical understanding of these telephony parameters.

## SIP page

The SIP User Agent window has three tabbed pages:

- **Configuration** – Parameters of the User Agent port.
- **Settings** – Protocols and parameters of the User Agent.
- **Status** – Operational status of the User Agent.

Read the section introduction on [page 175](#) for reference.

### Voice > User Agent > SIP > Configuration tab

This page configures the parameters for the SIP User Agent.

#### Prerequisites

- You must have an account with a SIP service provider and have the account's user ID, authentication ID, and authentication password.
- If the Phone port has been configured for MGCP, that configuration profile must be deleted before the port can be re-configured for SIP.

#### Configuration

In the display pane, click **New** to open the configuration page. If a User Agent has already been defined, click the **Port** identifier in the display to open the Properties page, then **Modify** to open the configuration page.

To delete an entry, enable the check box next to the port number on the display page, then click **Delete**.

Fill in the fields as follows. Click **Update** when finished:

<b>Port</b>	Enter "1" for the port number. This is the only value accepted.
<b>Name</b>	Name for this User Agent profile.
<b>UserID</b>	User ID of the SIP account. (required)
<b>AuthID</b>	Authentication ID of the SIP account.
<b>Password</b>	Authentication password of the SIP account.
<b>Codec1</b>	Most preferred codec and packet time selection (PCMU_10   PCMU_20   PCMA_10   PCMA_20   G729A_10   G729A_20   NOTUSED). Default is PCMU_20.
<b>Codec2</b>	Second preferred codec and packet time selection (PCMU_10   PCMU_20   PCMA_10   PCMA_20   G729A_10   G729A_20   NOTUSED). Default is PCMA_20.
<b>Codec3</b>	Third preferred codec and packet time selection (PCMU_10   PCMU_20   PCMA_10   PCMA_20   G729A_10   G729A_20   NOTUSED). Default is G729A_20.
<b>Codec4</b>	Fourth preferred codec and packet time selection (PCMU_10   PCMU_20   PCMA_10   PCMA_20   G729A_10   G729A_20   NOTUSED). Default is NOTUSED.



---

<b>RFC2833</b>	Enable/disable RFC 2833 for DTMF. Default is <b>yes</b> . RFC 2833 provides “out of band DTMF” event reports. Distortion from compression and decompression can prevent recognition of pure DTMF tones. Out-of-band DTMF sends the information by separate RTP packets.
<b>Payload</b>	If RFC 2833 is enabled, the RTP dynamic payload type can be specified. The payload code indicates the payload format (per RFC 1889). Range is <b>96-127</b> . Default is <b>101</b> .
<b>MLS</b>	Disable this feature ( <b>off</b> ), or specify the method used to invoke a second line or to switch between lines if connected to a multi-line phone or PBX. Default is <b>RFC3264</b> . <b>RFC2976</b> : Use Out-Band DTMFs signals (using the SIP Signalling INFO method) <b>RFC3264</b> : Send In-Band DTMFs signals (coded within the voice data packets) If MLS and VAD are both enabled, VAD packets are not transmitted, but received VAD packets are processed.
<b>MPT</b>	If a modem is connected to the FXS port, enables modem pass-through and forces media to G.711 echo cancellation. Default is <b>off</b> .
<b>Fax</b>	If a fax is connected to the FXS port, enables fax pass-through and either forces media to G.711 echo cancellation ( <b>on</b> ) or enables re-negotiation of the CODEC with the remote party when a fax tone is detected ( <b>auto</b> ) Default is <b>off</b> .
<b>VAD</b>	Enables Voice Activity Detection (VAD) (silence suppression). Default is <b>no</b> . Enabling VAD allows the unit to avoid sending silent RTP packets; thus, conserving resources. However, VAD can silence very low sounds, lowering voice quality. If MLS and VAD are both enabled, VAD packets are not transmitted, but received VAD packets are processed.
<b>Up</b>	Enables/disables the SIP User Agent. Default is <b>yes</b> .

---

## Voice > User Agent > SIP > Settings tab

This page modifies the SIP protocol as it applies to the User Agent. These settings do not apply to the Session Controller.

Click **Modify** to open the configuration page. Fill in the fields as follows. Click **Update** when finished:

<b>Timer T1</b>	Minimum retransmission time interval (milliseconds), per RFC 3261. The default is <b>500</b> milliseconds.
<b>Timer T2</b>	Maximum retransmission time interval (milliseconds), per RFC 3261. The default is <b>4000</b> milliseconds.
<b>Timer B</b>	Timeout interval for INVITE transactions (milliseconds), per RFC 3261. The default is <b>32000</b> milliseconds.
<b>RegExpire</b>	Timeout interval for expiration of the endpoint registration (seconds). The default is <b>3600</b> seconds (1 hour).
<b>SE Enable</b>	Enables <i>Session Expires</i> support (see <b>SE Timer</b> and <b>MIN-SE Timer</b> ), per RFC 4028. The default is <b>no</b> .
<b>SE Timer</b>	Maximum session interval if no session refresh requests are received (seconds), per RFC 4028. If the timer expires, the session ends. The default is <b>1800</b> seconds (30 minutes). Applicable if <b>SE Enable</b> is <b>yes</b> .
<b>MIN-SE Timer</b>	Minimum session interval that the User Agent can accept (seconds), per RFC 4028. The default is <b>90</b> seconds. Applicable if <b>SE Enable</b> is <b>yes</b> .
<b>On-Hold Timer</b>	Maximum interval of time that the User Agent can be put on hold with no audio or music-on-hold (seconds). If the on-hold timer expires, the call is disconnected. The default is <b>180</b> seconds (3 minutes).
<b>No-Answer Timer</b>	Maximum interval of time that the User Agent can be ringing without being answered (seconds). If the no-answer timer expires, the call is rejected with an assigned reason of either ring-timeout or call-forwarding on no-answer (if the feature is enabled ( <a href="#">page 181</a> )). The default is <b>60</b> seconds.
<b>End of dial digit (#)</b>	Whether the hash (#) character indicates the end of the dialed digit string; if it does, the # character is stripped from the digit string ( <b>yes</b>   <b>no</b> ). The default is <b>yes</b> .
<b>Inter Digit Timeout (secs)</b>	Maximum time allowed (seconds) between the dialing of digits. The default is <b>3</b> seconds. When the interdigit timer expires, the gateway assumes that the digit string is complete and interprets it according to its numbering plan. This timer does not apply to an emergency call; when the gateway receives the emergency number (911), the call is placed immediately.

## Voice > User Agent > SIP > Status tab

This page displays the status of the SIP User Agent.

The field entries are as follows:

<b>RegStatus</b>	Reports if the User Agent is correctly registered with the SIP server.
<b>Line 1</b>	<p>Possible messages are:</p> <p>Idle – The analog device is on-hook.</p> <p>OB (OutBound) Calling – The analog device is off-hook or a phone number is being dialed.</p> <p>OB (OutBound) Proceeding – The remote party is ringing.</p> <p>IB (InBound) Proceeding – The analog device is ringing.</p> <p>Disconnecting – The remote party is disconnected.</p> <p>Connected – The analog device is in communication.</p>
<b>Line 2</b>	This field is populated when the multi-line support option ( <a href="#">page 177</a> ) is enable, which it is by default. The messages are the same as for Line 1.

## MGCP page

The MGCP User Agent window has three tabbed pages:

- ❑ Configuration – Parameters of the User Agent port.
- ❑ Settings – MGCP protocol as it applies to the User Agent.
- ❑ Status – Operational status of the User Agent.

Read the section introduction on [page 175](#) for reference.

## Voice > User Agent > MGCP > Configuration tab

This page configures the parameters for the User Agent port.

### Prerequisites

- You must have an account with an MGCP service provider and have the MGCP session controller configured and operational.
- If the FXS port has been configured for SIP, that configuration profile must be deleted before the port can be re-configured for MGCP.

### Configuration

In the display pane, click **New** to open the configuration page. If a User Agent has already been defined, click the **Port** identifier in the display to open the Properties page, then **Modify** to open the configuration page.

To delete an entry, enable the check box next to the port number on the display page, then click **Delete**.

Fill in the fields as follows. Click **Update** when finished:

<b>Port</b>	Number of the FXS port.
<b>Name</b>	Name for this User Agent profile.
<b>UserID</b>	Authentication information required by the MGCP server.
<b>Codec1</b>	Most preferred codec and packet time selection (PCMU_10   PCMU_20   PCMA_10   PCMA_20   G729A_10   G729A_20   NOTUSED). Default is PCMU_20.
<b>Codec2</b>	Second preferred codec and packet time selection (PCMU_10   PCMU_20   PCMA_10   PCMA_20   G729A_10   G729A_20   NOTUSED). Default is PCMA_20.
<b>Codec3</b>	Third preferred codec and packet time selection (PCMU_10   PCMU_20   PCMA_10   PCMA_20   G729A_10   G729A_20   NOTUSED). Default is G729A_20.
<b>Codec4</b>	Fourth preferred codec and packet time selection (PCMU_10   PCMU_20   PCMA_10   PCMA_20   G729A_10   G729A_20   NOTUSED). Default is NOTUSED.
<b>RFC2833</b>	Enable/disable RFC 2833 for DTMF. Default is <b>yes</b> . RFC 2833 provides "out of band DTMF" event reports. Distortion from compression and decompression can prevent recognition of pure DTMF tones. Out-of-band DTMF sends the information by separate RTP packets.
<b>Payload</b>	If RFC 2833 is enabled, the RTP dynamic payload type can be specified. Range is 96-127. Default is 101.
<b>MPT</b>	If a modem is connected to the FXS port, enables modem pass-through and forces media to G.711 echo cancellation. Default is <b>off</b> .
<b>Fax</b>	If a fax is connected to the FXS port, enables fax pass-through and either forces media to G.711 echo cancellation ( <b>on</b> ) or enables re-negotiation of the CODEC with the remote party when a fax tone is detected ( <b>auto</b> ) Default is <b>off</b> .
<b>VAD</b>	Enables Voice Activity Detection (VAD) (silence suppression). Default is <b>no</b> . Enabling VAD allows the unit to avoid sending silent RTP packets; thus, conserving resources. However, VAD can silence very low sounds, lowering voice quality. If MLS and VAD are both enabled, VAD packets are not transmitted, but received VAD packets are processed.
<b>Up</b>	Enables/disables the MGCP User Agent. Default is <b>yes</b> .

## Voice > User Agent > MGCP > Settings tab

This page modifies the MGCP protocol as it applies to the User Agent. The MGCP protocol can be modified for inter-operability purposes within the MGCP environment. These settings do not apply to the Session Controller.

Click **Modify** to open the configuration page. Fill in the fields as follows. Click **Update** when finished:

<b>DomainFormat</b>	MAC address is the only format supported in this release.
<b>MasReTxNum</b>	Maximum number of re-transmissions when a request does not get an answer. Default is 5.

## Voice > User Agent > MGCP > Status tab

This page displays the status of the SIP User Agent.

The `LineStatus` field entries are as follows:

<b>Inactive</b>	The port is not up.
<b>Idle</b>	The analog device is on-hook.
<b>OB (OutBound) Calling</b>	The analog device is off-hook or a phone number is being dialed.
<b>OB (OutBound) Proceeding</b>	The remote party is ringing.
<b>IB (InBound) Proceeding</b>	The analog device is ringing.
<b>Disconnecting</b>	The remote party is disconnected.
<b>Connected</b>	The analog device is in communication.

## Voice > User Agent > Numbering Plan

This feature applies only to a SIP User Agent, not an MGCP User Agent.

When an analog device, such as a phone, is connected to the Phone port, a numbering plan might be needed to make full use of the features of the device. The SIP User Agent uses a numbering plan to interpret any feature-related string entered from the analog device.

The numbering plan consists of a collection of entries, each defining how a specific string from an analog device is to be interpreted. Each string is categorized as either a phone number to be dialed or a service code to invoke a feature. The User Agent compares the string from the device to the entries in the numbering plan and translates it as needed before the string is sent to the SIP server.

- For phone numbers, the string of digits can be translated as follows:
  - Digits can be stripped from the beginning of the number.
  - Digits can be prepended to the beginning of the number.
- For service codes, the digits dialed are sent without modification.

For the user to activate a service, he or she enters the defined number string and adds a hash character [#]. For example, if the Do Not Disturb feature is defined to be \*78, then the user enters \*78# to activate the service.

---

**NOTE:** The SIP User Agent must be configured before the numbering plan is configured. See [page 176](#).

---

## Configuration

In the display pane, click **New** to open the configuration page. Fill in the fields as shown below. Click **Update** when finished.

If a numbering plan has already been defined, click the **Number** in the display to open the Properties page, then **Modify** to open the configuration page.

To delete an entry, enable the check box next to the **Number** in the display page, then click **Delete**.

<b>Number</b>	String translated by this entry. If <b>Type</b> is <b>Number</b> , this field denotes the beginning digits of the number to be translated.
<b>Type</b>	Indicates whether the entry is for a number or a service code ( <b>Number</b>   <b>Service</b> ).
<b>Feature</b>	If <b>Type</b> is <b>Service</b> , select one of the following service codes: <b>None</b> – No feature applied. (Default) <b>SDND</b> – Set Do Not Disturb. SIP server marks the SIP gateway as busy. <b>CDND</b> – Clear Do Not Disturb <b>SFWA</b> – Set Forward All (calls) <b>CFWA</b> – Clear Forward All <b>SFWB</b> – Set Forward on Busy <b>CFWB</b> – Clear Forward on Busy <b>SFWNA(1)</b> – Set Forward No Answer. Forwards the call after the no-answer timer expires. Timer is set in the SIP User Agent ( <a href="#">page 178</a> ). Default is 60 sec. <b>CFWNA</b> – Clear Forward No Answer <b>BXFER</b> – Blind Transfer. Transfers a call and disconnects your line.
<b>Length</b>	Expected length of this number entry.
<b>StripCount</b>	Number of digits to strip off from the beginning of the number.
<b>Prepend</b>	Digits to prepend to the beginning of the number.

## Configuration and application examples

### *Phone number prepend*

This example configures a numbering plan entry to prepend a zero (0) to every phone number of length nine (9) that begins with a one (1). For example, if the phone number dialed is 123456789, the phone number called by the SIP User Agent is 0123456789.

<b>Number</b>	1
<b>Type</b>	Number
<b>Length</b>	9
<b>Prepend</b>	0

***Do not disturb***

This example configures two numbering plan entries to enable / disable use of the Do Not Disturb feature, such that:

- ❑ To set Do Not Disturb for a phone, enter **\*78#**.
- ❑ To clear the Do Not Disturb state for a phone, enter **\*79#**.

Set Do Not Disturb:

<b>Number</b>	*78
<b>Type</b>	Service
<b>Feature</b>	SDND (set do-not-disturb)

Clear Do Not Disturb:

<b>Number</b>	*79
<b>Type</b>	Service
<b>Feature</b>	CDND (clear do-not-disturb)

***Forward all calls***

This example configures two numbering plan entries to enable / disable use of the Call Forwarding feature, such that:

- ❑ To forward all calls to another phone, the entry is \*90, followed by the phone number and the hash character (#). For example, to forward calls to phone extension 4985, enter **\*904985#**.
- ❑ To clear call forwarding for a phone, enter **\*91#**.

Set Forward All:

<b>Number</b>	*90
<b>Type</b>	Service
<b>Feature</b>	SFWA (Set Forward All)

Clear Forward All:

<b>Number</b>	*91
<b>Type</b>	Service
<b>Feature</b>	CFWA (Clear Forward All)

**Forward no answer**

This example configures two numbering plan entries to enable / disable use of the Call Forwarding-No Answer feature, such that:

- ❑ To forward unanswered calls to another phone, the entry is \*93, followed by the phone number and the hash character (#). For example, to forward unanswered calls to phone extension 4985, enter **\*934985#**.
- ❑ To clear unanswered call forwarding for a phone, enter **\*94#**.

Set forward no answer:

**Number**     \*93  
**Type**        Service  
**Feature**     SFWNA (Set Forward No Answer)

Clear forward no answer:

**Number**     \*94  
**Type**        Service  
**Feature**     CFWNA (Clear Forward No Answer)

**Blind transfer**

This example configures a numbering plan entry to enable the use of the blind transfer feature, such that:

- ❑ The user can transfer an existing call to another number and disconnect from the call.
- ❑ The sequence of user actions to transfer a call to extension 4567 is:
  - A call is in progress.
  - Press the phone's **Flash** button.
  - Enter **\*224567#**.
  - Hang up.

Configure blind transfer:

**Number**     \*22  
**Type**        Service  
**Feature**     BXFER (blind transfer)



---

## Local call routing

The Local Call Routing page has three tabs:

- ❑ **Account** – Create an account that identifies the dialing number of a phone on the LAN.
- ❑ **Connection** – Displays existing local calls.
- ❑ **Settings** – Configuration parameters for the Line port.

The BSGX4e can provide backup PSTN phone service if VoIP service is unavailable. If there is power to the unit, local call routing (**LCR**) connects internal LAN-to-LAN calls, and it routes external calls to the LINE (FXO) port, where they are converted from IP to analog. The LINE port connects to a PSTN at the central office.

A VoIP service interruption can happen if the WAN connection fails, the call server connection fails, or no call server is available. However, it is not considered a service interruption when a VoIP call cannot be placed due to lack of bandwidth.

- Local Calls

In LCR mode, LAN VoIP phones (and analog phones on the PHONE port of the 2xx series models) can place and receive *local calls*, meaning LAN-to-LAN calls, which do not go out to the WAN. Local calls are established through the BSGX4e acting as a VoIP server.

- External Calls

Limited external call service is available through the LINE port when connected to a PSTN line to a central office. Only outgoing calls are supported. Only basic telephone services are supported.

- Emergency Calls

All emergency calls (911 in North America) are routed by LCR to the LINE port. This is true whether or not VoIP service is available.

When VoIP call service resumes, external calls are automatically received and placed as before.

### Voice > Local Call Routing > Account tab

For local call routing, the BSGX4e needs to know the telephone numbers of the local endpoints. An LCR account provides that information when the user ID or endpoint ID does not, as is the case if those fields are alphabetic or alphanumeric. For example, when a SIP account is defined by a name string, the LCR account defines the telephone number of that account.

---

**NOTE:** LCR accounts are not required if the IDs of the LAN endpoints are numeric, not alphanumeric.

---

If LCR accounts are not configured, VoIP phones with alphanumeric IDs can only receive calls from other VoIP phones that allow the entry of alphanumeric IDs. Other entities are not able to place calls to VoIP phones having alphanumeric IDs.

## Configuration

In the display pane, click **New** to open the configuration page. Fill in the fields as shown below. Click **Update** when finished.

To delete an entry, enable the check box next to the DN number on the display page, then click **Delete**.

<b>DN</b>	Phone number of the account. A 4-digit extension for local calls is acceptable.
<b>Type</b>	Signaling protocol used by the endpoint ( <b>SIP</b>   <b>MGCP</b> ).
<b>ID</b>	ID of the SIP or MGCP endpoint.

## Voice > Local Call Routing >Connection tab

This tab page displays existing LCR connections.

## Voice > Local Call Routing >Settings tab

This tab page configures various parameters that define how the LCR functions. To change parameter values on this page, click **Modify** and enter values as described below.

**NOTE:** The emergency numbers are set by the country code entered into [System > Overview > System Information panel on page 32](#). In this software release, you cannot override these settings here on the **Modify** page.

<b>LCBMode</b>	Local call backup mode: <ul style="list-style-type: none"> <li>• <b>INT</b> (Integrated Gateway) for the Line (FXO) port.</li> <li>• <b>LGW</b> (LAN Gateway) for a SIP/PSTN gateway on the LAN.</li> </ul> Only one gateway can be configured. The default is <b>INT</b> .
<b>ECPolice</b>	Emergency call number for police. The default is <b>911</b> .
<b>ECFire</b>	Emergency call number for fire. The default is <b>911</b> .
<b>ECAmbulance</b>	Emergency call number for ambulance. The default is <b>911</b> .
<b>ECMisc</b>	Emergency call number for other services. The default is <b>911</b> .
<b>OBAccess</b>	Outbound access prefix digit, such as 9 in 9-555-1001. Applies only to hosted PBX service. The default is <b>9</b> .
<b>AreaCode</b>	Area code of this installation, such as, 408 in (408) 555-1001.
<b>COPrefix</b>	Central office prefix of this installation , such as 555 in (408) 555-1001.
<b>ENLength</b>	Extension number length, such as 4 for the last four digits in (408) 555-1001. The default is <b>4</b> .
<b>ECthroughFXO</b>	Force the emergency call (ECNumber) to be routed through the Line port (or gateway) in normal mode, that is, not in survival mode. A <b>no</b> setting routes emergency calls through VoIP when in normal mode. Default is <b>yes</b> .

The following example defines the local numbering plan as follows:

prefix for outbound calls (OBAccess): **9**  
area code: **408**  
central office prefix (COPrefix): **555**  
length of extension number (ENLength): **4**

This configuration supports calls as follows:

Number dialed	Action
2210	Four-digit call so only local accounts are checked.
9411	Outbound prefix so number is interpreted as outbound call for 411.
95552210	Outbound prefix, but also central office prefix, so only local accounts are checked for 2210.
96872210	Outbound prefix, but not central office prefix, so route 6872210 to PSTN.
914085552210	Central office prefix so only local accounts are checked for 2210.



---

# APPENDIX 12–QUALITY OF SERVICE

This Appendix provides a technical description of the theory and application of QoS (Quality of Service) in the BSGX4e.

QoS is a method to reserve bandwidth and establish transmission priorities for critical services during those times when your Internet link is at full capacity. The most common application of QoS in the BSGX4e is for VoIP, where it provides uninterrupted service.

---

## Configuration summary

This summary describes the layer 3 QoS configuration process. The layer 2 configuration process is relatively simple and is covered in the section [QoS page on page 98](#).

The QoS configuration process for SIP/MGCP devices is shorter than for other media types because these devices are automatically detected by the BSGX4e's session controller. All other traffic has to be manually identified. Therefore, two configuration summaries are provided.

### SIP/MGCP Traffic

The following list summarizes the configuration steps you must perform to make QoS functional.

1. Configure the WAN interface. [Interfaces on page 70](#)
2. Configure the media settings, SIP or MGCP server, and User Agent (BSGX4e). [Voice > Media > Settings on page 161](#); [Session control on page 164](#); [User agent on page 175](#)
3. Configure the QoS link. [Link page on page 110](#)
4. Create quality groups. [Group page on page 112](#)
5. Configure Downstream QoS if this feature is enabled in any quality group. [Downstream QoS page on page 118](#)
6. Associate the quality groups with the session controller. [[Voice > Media > Settings on page 161](#); [Voice > Session Control > SIP Control on page 167](#)] Note the special group that applies to the ARP/PPP control signals. [ARP/PPP page on page 121](#)

## Other traffic

The configuration procedure for any other traffic stream to which you want to apply QoS is basically the same except for [Step 6](#). Rather than associating the quality group to the session controller, you must create a firewall policy and specify the quality group there.

Be cautious about enabling Downstream QoS in too many quality groups (see [Downstream QoS page on page 118](#)). This feature provides inbound bandwidth for VoIP payload and control streams that use UDP by limiting TCP traffic.

---

## QoS overview

The BSGX4e Business Gateway uses QoS to manage internal traffic contention that is created when LAN traffic coming into the unit from the four high-speed LAN ports exceed the capacity of the internal routing engine or the uplink capacity of the WAN port.

There are two points of traffic contention within the BSGX4e:

- ❑ Layer 2  
Traffic coming into the four LAN ports creates a 400 Mbps flow that goes to a 100 Mbps router.
- ❑ Layer 3  
Traffic from the router plus other traffic processed by the BSGX4e (such as VoIP flows from the session controller) are routed to the WAN, whose capacity is determined by your service contract.

The layer 2 and layer 3 QoS processes work independent of each other. Accordingly, this section discusses layer 2 and layer 3 QoS separately.

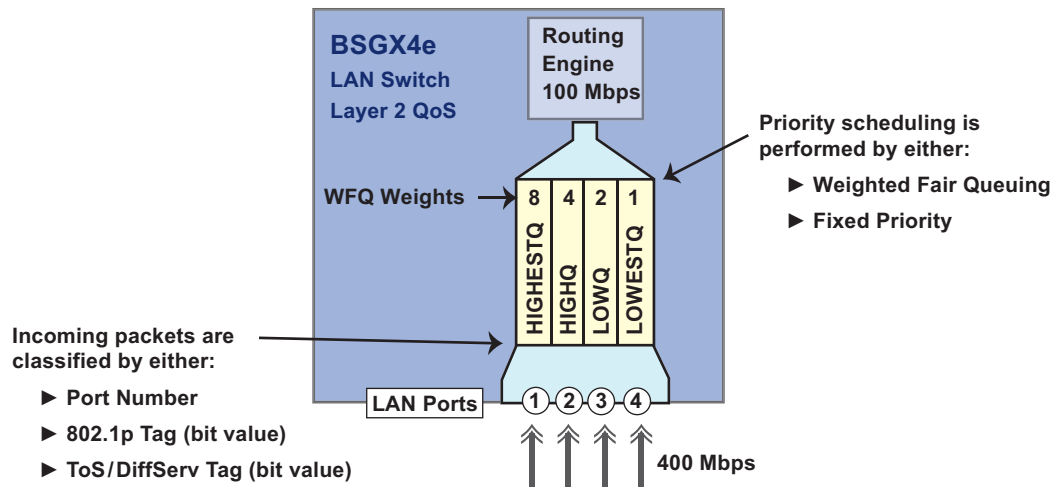
During those periods of low congestion, QoS does not significantly affect traffic. But when high traffic levels cause congestion, QoS guarantees quality service for all QoS-managed applications, up to bandwidth limits.

## Quality of service – Layer 2

Traffic contention on the LAN side of the BSGX4e is caused by the four 100 Mbps LAN ports feeding a single 100 Mbps router. This contention is managed by routing traffic into four priority queues, which are labeled HIGHESTQ, HIGHQ, LOWQ, and LOWESTQ.

[Figure 43](#) shows this contention and the priority queues.

**Figure 43** Layer 2 QoS contention



### Priority classification

Incoming traffic is detected for a priority queue by setting the BSGX4e LAN switch to use one of the three following classifications types. See [QoS page on page 98](#) for the configuration process.

- ❑ Port number

Associate each BSGX4e LAN port with a priority queue.

- ❑ IEEE 802.1p bit value (CoS)

Used with VLANs. Configure the LAN devices to set the appropriate 802.1p priority bit value for the desired priority level. The BSGX4e associates that value with a priority queue.

This *IEEE 802.1p* priority notation is commonly called CoS (class of service). It is three bits in the User field of the ISL frame header.

- ToS (type of service) / DiffServ bit

Configure the LAN devices to set the appropriate ToS priority bit value (8 bits in the IP header) for the desired priority level. The BSGX4e associates that value with a priority queue.

See [Figure 44](#) on [page 193](#) for application scenario examples.

---

**NOTE:** A static ARL map assigns a priority to a specific MAC address / LAN port combination. That priority setting applies regardless of the priority settings made in this section. See [Data > Switch > ARL on page 101](#).

---

## Priority scheduling

After the incoming traffic has been classified and sent to the priority queues, the scheduling method determines how those queues are emptied. You can set the BSGX4e to use one of two scheduling methods:

- Weighted Fair Queuing (WFQ)

All queues are serviced depending on the weight assigned to the queue. The weighting of the four queues is:

HIGHESTQ – 8  
HIGHQ – 4  
LOWQ – 2  
LOWESTQ – 1

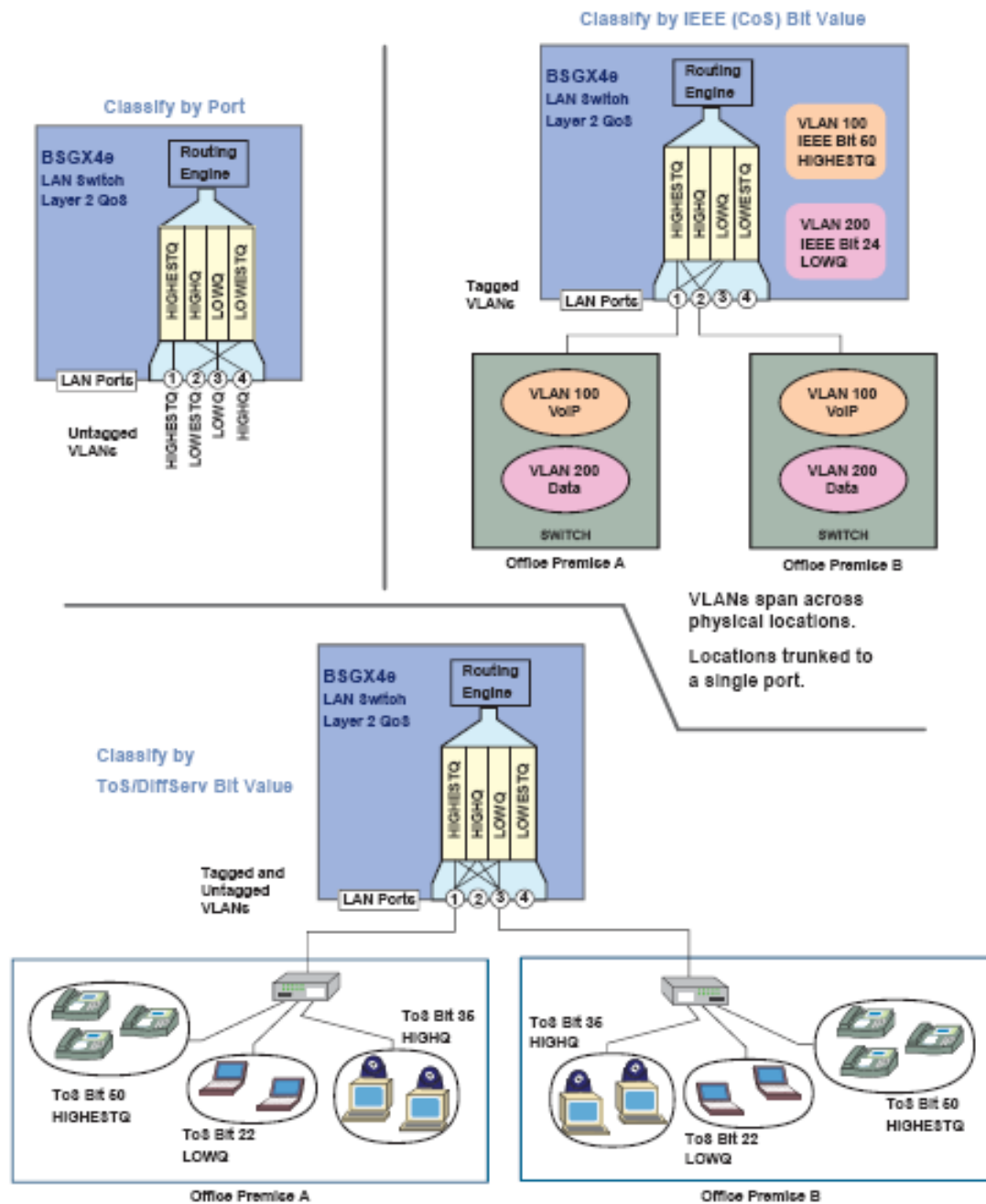
For every 8 packets sent from the HIGHESTQ queue, 4 packets are sent from the HIGHQ queue, 2 packet are sent from the LOWQ queue, and 1 packet is sent from the LOWESTQ queue,

All queues eventually receive service, but all queues can also experience delay.

- Fixed Queuing

All packets are serviced from the highest priority queue first, then the next lower-priority queue is serviced, and so on. Starvation can occur in lower-priority queues because the traffic load from a higher-priority queue can prevent lower-priority queues from being serviced.



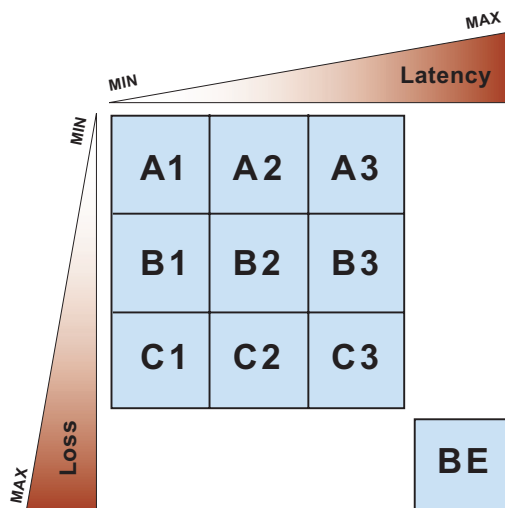
**Figure 44** Layer 2 QoS Application Scenarios

## Guarantee of service – Layer 3

The BSGX4e implements QoS through a patented process called GoS™ (Guarantee of Service), which applies to outbound (LAN → WAN) traffic. Rather than providing standard QoS with its linear ranking of quality levels based on one quality factor, GoS provides *quality groups* that establish guaranteed bandwidth for QoS-managed

applications, and it uses a matrix of ten *quality classes* that combine different levels of prioritizing based on latency (delay) and loss (discarded data) characteristics (see [Figure 45](#)). Loss and latency are used to calculate the most intelligent queuing priorities to achieve the highest quality transmission for all media types.

**Figure 45** GoS Quality Class Matrix



Typically, voice media requires low latency and jitter, while video and data media requires low loss.

Quality Class Examples:

A3 = High latency + low loss

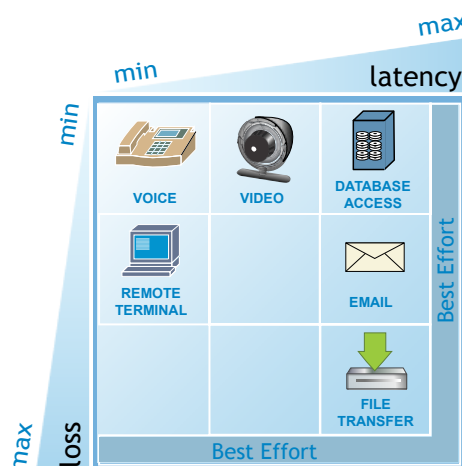
C1 = Low latency + high loss

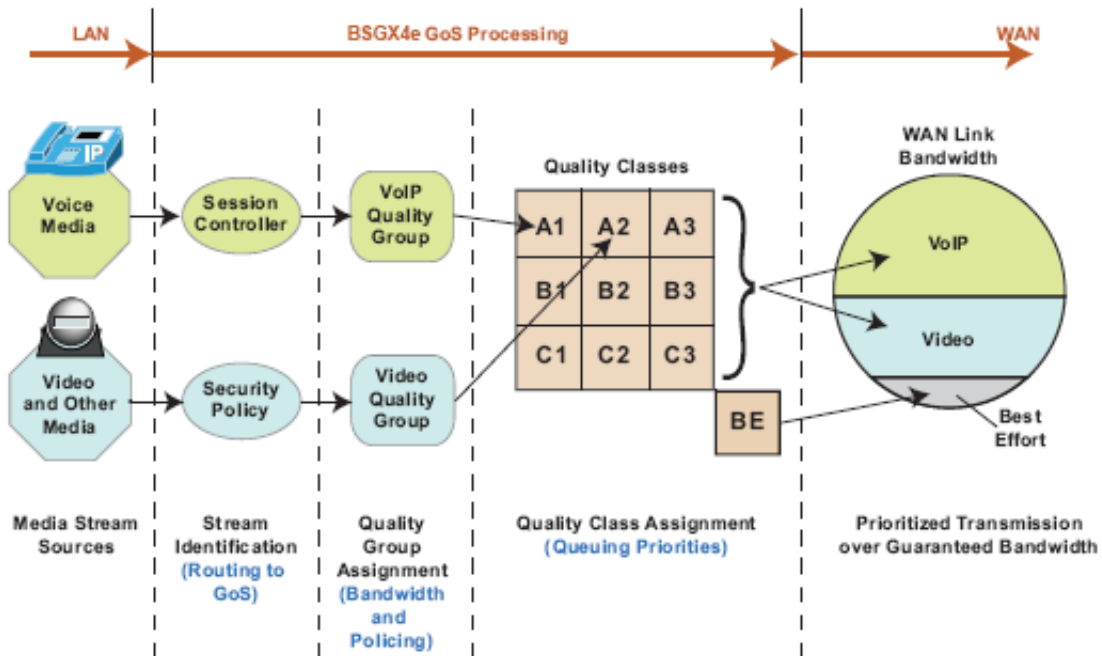
BE = Best Effort (no prioritizing)  
Highest latency + highest loss

As shown in [Figure 46](#), each type of media stream identified for GoS management is first assigned to a quality group. A quality group specifies the amount of bandwidth guaranteed for the media stream and applies the *policing* type. There are two types of policing:

- ❑ Strict – An absolute bandwidth rate. Traffic that exceeds the designated rate is discarded.
- ❑ CAR (committed access rate) – A committed (absolute) rate, plus the ability to use available BE bandwidth, up to a designated limit. Traffic that exceeds the committed rate is queued and then bursts into any BE space available between packets.

A quality group is then assigned to a quality class. A quality class defines a stream's sensitivity to latency and loss. That information is then used to prioritize and process traffic waiting in queue during times in which the WAN link is full.



**Figure 46** GoS process flow

## Functional characteristics

Functional characteristics of GoS include:

- The sum total of bandwidth allocated to all quality groups can be up to 90% of available WAN bandwidth.
- The minimum bandwidth allocation to any quality group is 64 Kbps.
- Bandwidth allocated to a quality group is *guaranteed*. This means bandwidth is taken from BE and reserved for the quality group as needed per session, up to the specified limit. The amount of reserved bandwidth is determined for each session request, with the remaining guaranteed bandwidth left for BE traffic.
- Multiple media streams can be assigned to one quality group.
- Multiple quality groups can be assigned to one quality class.
- Voice streams from IP phones are identified automatically by the *session controller* in the BSGX4e. An IP phone identifies itself by registering with the session controller when it is first connected to the unit. The quality group defined for VoIP is associated with the session controller.
- Other media streams managed by GoS must be manually configured to define how they are identified. This is accomplished by creating security policies, which have fields to identify a stream and associate it with a quality group. See [Managing other traffic on page 197](#) for more discussion.
- The GoS processing described here applies to outbound traffic. Downstream QoS can be enabled to accommodate inbound traffic. See the section [Downstream QoS page on page 118](#) for details.

## Media and control signals

Various devices and functions use both a media (payload) stream and a control signal stream. For a critical device or function, you protect the media stream by putting it under QoS management. But, in many cases, the media stream does not transmit if the control signal is interrupted, so the control signal must also be protected from packet loss by assigning it to a quality group.

For any device or function where you want both media and control streams to be managed by QoS, you must decide if you want both streams be in the same quality group or separate quality groups.

---

**NOTE:** The Initial Setup Wizard creates a control quality group if the Default button on the QoS page is clicked. This quality group is designed for the control signals of ARP and PPP protocols (see [page 121](#)). Control signals from other functions can also use this quality group.

---

These guidelines help you determine the most efficient use of QoS:

- The minimum bandwidth allocation to a quality group is 64 Kbps. But, typically, a control signal consists of a small data rate. If you put each control signal into its own quality group, you can limit the number of quality groups you can create, since the sum of all bandwidth allocated to quality groups cannot exceed 90% of available bandwidth.
- One scheme is to create a Control quality group and assign all control signals to that group. This is practical when you have several devices and functions that use small control signals. As a general guideline, this scheme applies if you operate more than 10 IP phones. The recommended configuration for this quality group is:

<b>Link</b>	eth0
<b>QG</b>	A2
<b>Type</b>	car
<b>Committed</b>	64000
<b>Burst</b>	<i>Note 1</i>
<b>Downstream QoS</b>	yes

**Note 1:** Set the burst rate to at least 200000 if you have a high-rate bandwidth. If your bandwidth is less than 200 Kbps, set the burst rate equal to your bandwidth rate.

- If you have only a few devices and functions under QoS (less than 10 IP phones in operation), you can assign the media and control signals to the same quality group. Since the control signal is small, it does not consume a significant amount of the quality group's bandwidth. Also, since there is no Control quality group, the media group can be made 64 Kbps larger.

## Managing other traffic

Any media stream can be placed under QoS management if the stream can be uniquely identified.

For any given media stream to be processed by QoS, the BSGX4e must be able to distinguish that stream from all others, and it must be able to identify the type of communication it contains (voice, video or data). The BSGX4e automatically detects SIP voice and video streams by the SIP applications registering with the session controller, but a non-SIP video or data stream must be manually identified. This is accomplished by configuring a security policy ([page 130](#)) for the non-SIP stream where you can identify it by any of several parameters and assign it to a quality group.



**CAUTION:** A video stream can have high spikes of bandwidth demand. The bandwidth allocated to a video quality group must be high enough to accommodate those spikes. Therefore, ensure that you have sufficient WAN bandwidth to create the needed high-bandwidth quality group.

SIP video is discussed in [Group page on page 112](#).

## Call capacity

A common question is how many calls can be supported by a particular BSGX4e model with a given interface type. The call capacity varies with such factors as the interface, encapsulation, codec, and available bandwidth.

[Table 26](#) provides a call bandwidth value for the various interfaces of BSGX4e and the most common codecs. The available WAN bandwidth can be affected by numerous factors. You need to measure or estimate your effective bandwidth through the BSGX4e and, where applicable, through any modems, switch, or other device immediately upstream from the BSGX4e. Remember that QoS is limited to 90% of the WAN link rate, and the quality group carrying the call also has a specific bandwidth limit.

The calculations in the table include the packet header size for the various interfaces and encapsulation methods.

**Table 26** Bandwidth for each call

Model link type	Interface / Encapsulation	CODEC	Call size (bps)
F200	Ethernet	G.729 20 ms	39200
Ethernet	Ethernet	G.729 10 ms	70400
	Ethernet	G.711 20 ms	95200
	Ethernet	G.711 10 ms	126400
	VLAN	G.729 20 ms	40800
	VLAN	G.729 10 ms	73600
	VLAN	G.711 20 ms	96800
	VLAN	G.711 10 ms	129600
	PPPoE	G.729 20 ms	42400
	PPPoE	G.729 10 ms	76800
	PPPoE	G.711 20 ms	98400
	PPPoE	G.711 10 ms	132800

## APPENDIX 13–GLOSSARY

<b>3PCC</b>	3rd Party Call Control
<b>ACL</b>	Access Control List–policies that determine which LAN endpoints can place and receive calls
<b>ADC</b>	Analog/Digital Converter
<b>ALG</b>	Application Layer Gateway
<b>ARL</b>	Address Resolution Logic
<b>ARP</b>	Address Resolution Protocol–protocol to automatically map IP addresses to hardware MAC addresses
<b>CAC</b>	Call Admission Control
<b>CDP</b>	Cisco Discovery Protocol
<b>CLI</b>	Command Line Interface
<b>CO</b>	Central Office–refers to the connection to the PSTN
<b>DAC</b>	Digital/Analog Converter
<b>DHCP</b>	Dynamic Host Configuration Protocol–used to assign and manage IP addresses for a network
<b>DNS</b>	Domain Name Server
<b>DSP</b>	Digital Signal Processor–a special-purpose CPU that provides ultra-fast instruction sequences, which are commonly used in math-intensive signal processing
<b>EAC</b>	Endpoint Access Control
<b>EP</b>	Endpoint, port of a gateway or a phone
<b>ESH</b>	Endpoint Status Handling–session controller feature that monitors status of LAN endpoints
<b>ESP</b>	Encapsulated Security Payload–protocol that defines the encrypted packets sent through a VPN tunnel
<b>Failover</b>	Backup system used to continue operations if the main device go down–during a power interruption, an analog telephone connected to the device can place emergency calls.
<b>FIFO</b>	First-In First-Out–a queued method for storing and retrieving data

<b>FQDN</b>	Fully Qualified Domain Name, consisting of host and domains, for example <i>www.yahoo.com</i> . The host is <i>www</i> , the second-level domain is <i>yahoo</i> , and the top-level domain is <i>com</i> .
<b>FTP</b>	File Transfer Protocol—an application layer protocol that uses TCP and Telnet services to transfer data files between machines or hosts
<b>FXO</b>	Foreign Exchange Office—provides interface on a VoIP device to connect to a PSTN
<b>FXS</b>	Foreign Exchange Station—device interface that connects to an analog device such as a POTS telephone or fax machine
<b>GoS™</b>	Guarantee of Service
<b>HTTP</b>	Hypertext Transfer Protocol—protocol for transferring files on the Web
<b>HTTPS</b>	HTTP over SSL—protocol enabling the secured transmission of Web pages
<b>ICMP</b>	Internet Control Message Protocol—extension of the Internet Protocol (IP) used to generate message and control packets
<b>IDS</b>	Intrusion Detection System—defends the device from attacks arriving from the WAN
<b>IKE</b>	Internet Key Exchange—protocol used to negotiate the initial security association between gateways of a VPN tunnel
<b>IP</b>	Internet Protocol—a packet-based protocol for delivering data across networks
<b>IPsec</b>	Internet Protocol Security—protocol used to secure VPNs across an IP network
<b>LAN</b>	Local Area Network
<b>LCR</b>	Local Call Routing—the telephone service that the device provides without the assistance of a VoIP call server on the WAN
<b>MAC</b>	Media Access Control—a MAC address is a hardware address that uniquely identifies each network device.
<b>MIB</b>	Management Information Base—the hierarchical database used by the simple network management protocol (SNMP) to describe the particular device being monitored. MIB objects are identified using ASN.1 syntax
<b>MGC</b>	Media Gateway Controller
<b>MGCP</b>	Media Gateway Control Protocol
<b>NAS</b>	Network Access Server—a gateway device that acts as the single point of access to a resource; the device references an authentication server to determine if access is granted
<b>NAT</b>	Network Address Translation—also known as Network Address Translator
<b>NTP</b>	Network Time Protocol—see SNTP
<b>PCM</b>	Pulse Code Modulation
<b>PMON</b>	Protocol Monitoring—tool available to trace incoming traffic



<b>PoE</b>	Power over Ethernet–transmission of DC power over an Ethernet cable by carrying power in the unused 4/5 and 7/8 wires. PoE allows devices to be installed at remote locations where there is no external power source.
<b>POTS</b>	Plain Old Telephone Service
<b>PPP</b>	Point-to-Point Protocol–protocol used over serial lines to support Internet connections
<b>PPPoE</b>	PPP protocol over Ethernet–used to connect the WAN interface of the device to a PPPoE access concentrator
<b>PSTN</b>	Public Switched Telephone Network
<b>PVC</b>	Permanent Virtual Circuit
<b>QoS</b>	Quality of Service–techniques used to assure a given level of performance as measured by the transmission rate and error rates
<b>RADIUS</b>	Remote Authentication Dial-In User Service–a client/server protocol and software that enables remote authentication of users attempting to log in to the unit
<b>RIP</b>	Routing Information Protocol–protocol for exchanging routing information within a network
<b>RTCP</b>	Real Time Transport Control Protocol (or RTP Control Protocol)
<b>RTP</b>	Real-Time Transfer Protocol
<b>SA</b>	Security Association–used by IKE and IPsec to determine how data is encrypted, decrypted, and authenticated by the secure gateways
<b>SC</b>	Session Controller
<b>SFC</b>	Stateful Flow Controller
<b>SFTP</b>	Simple File Transfer Protocol–can be used to transfer software upgrades to the device
<b>SHA</b>	Strong password HAsHING
<b>SIP</b>	Session Initiation Protocol
<b>SIP UA</b>	SIP User Agent
<b>SLIC</b>	Subscriber Line Interface Circuit
<b>SNMP</b>	Simple Network Management Protocol–protocol to monitor and control devices in a TCP/IP network
<b>SNTP</b>	Simple Network Time Protocol–an adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks in the Internet
<b>SRV</b>	DNS method/messages for location of services
<b>SSH</b>	Secure Shell–protocol used to secure remote connections to the unit
<b>SSL</b>	Secure Socket Layer–protocol used to secure remote connections to the unit
<b>SSP</b>	SIP Signaling Proxy–SIP session controller feature that relays SIP messages between SIP endpoints and SIP servers

<b>Stateful</b>	Maintains the last-known or current status of an application
<b>TACACS+</b>	Terminal Access Controller Access-Control System Plus is a protocol that provides access control for routers, network access servers, and other networked computing devices with one or more centralized servers. TACACS+ provides separate authentication, authorization, and accounting services and uses the TCP protocol.
<b>TCP</b>	Transmission Control Protocol—packet-switching protocol used with the Internet Protocol (IP)
<b>TDM</b>	Time Division Multiplex
<b>Telnet</b>	Protocol that provides remote terminal connection service
<b>TFTP</b>	Trivial File Transfer Protocol
<b>UA</b>	User Agent—also known as the integrated gateway, it is the device software that enables an analog device connected to an FXS port to place and receive calls
<b>UDP</b>	User Datagram Protocol—a connectionless protocol that allows direct delivery and receipt of datagrams, without acknowledgements or guarantee of delivery
<b>VLAN</b>	Virtual LAN, a logical subcomponent of a physical network—functions as a separate network to isolate its traffic from the rest of the network
<b>VIF</b>	Virtual interface—a virtual WAN interface created for VLANs
<b>VoIP</b>	Voice over Internet Protocol
<b>VPM</b>	Voice Processing Module
<b>VPN</b>	Virtual Private Network—a means for secure communication across an insecure network, such as the Internet
<b>VQM</b>	Voice Quality Monitoring—tool to measure voice quality and trigger alarms if quality falls below a given level
<b>WAN</b>	Wide Area Network
<b>Web</b>	Also known as the World Wide Web or www—the collection of sites accessible through the Internet
<b>Web browser</b>	A client program that initiates requests to a Web server and displays the information that the server returns

---

**Numerics**

802.1p [191](#)

911 [185](#)

---

**A**

access, user defaults [42](#)

ACL (Access Control List) [145](#)

alarms, call [106](#), [107](#)

ALG (Application Layer Gateway) [139](#)

analog device, connecting [162](#)

ARL (Address Resolution Logic) [101](#)

ARP

dynamic and static [86](#)

interfaces [89](#)

proxy ARP [89](#)

QoS [121](#)

table [88](#)

attacks, IDS [140](#)

authentication record, configure [54](#)

authentication, password [43](#)

authorization, password [44](#), [45](#)

---

**B**

bandwidth

allocation [196](#)

committed [114](#)

in QoS [193](#)

Best Effort [111](#)

bootloader upgrade [62](#)

browser font size [25](#)

Button Bar [22](#)

---

**C**

call bandwidth [198](#)

call features [181](#)

call load [29](#)

calls, maximum licensed [168](#), [173](#)

Certificate Signing Request [61](#)

CLI command shell [32](#)

codec, supported [107](#)

codecs, user agent [175](#)

command shell [32](#)

configuration display [63](#)

configuration file [63](#)

control signal [167](#), [172](#)

control signals [113](#)

CoS (class of service) [100](#), [191](#)

country [31](#)

country of operation [32](#)

current calls [29](#)

---

**D**

default configuration [24](#)

denial of service [142](#)

DHCP

client [47](#), [71](#)

relay [85](#)

server [47](#)

DHCP and DNS [48](#)

DHCP client [72](#)

DiffServ [192](#)

Direct Media [161](#)

DNS client

backup scenario [38](#)

configuration [36](#)

DNS relay

configure [79](#)

current sessions [80](#)

intro [78](#)

source [80](#)

DNS with DHCP [48](#)

DNS, configuration source [37](#)

DNS, dynamic [39](#)

Downstream QoS [118](#)

---

**E**

emergency calls [185](#)

encapsulation types [120](#)

endpoint call access [145](#)

endpoints [167](#), [172](#)

configuring [169](#)

LAN [169](#), [173](#)

ESP (Encapsulated Security Payload) [147](#)

Ethernet (eth0) [70](#)

---

**F**

Factory Defaults [24](#)

failover, MGCP [171](#)

failover, SIP [166](#)

fax [175](#), [177](#), [180](#)

firewall

security policies [125](#)

session controller [164](#)

timer [131](#)

Fixed Queuing [192](#)

flood attack [142](#)

FXO port [162](#)

FXS port [162](#), [175](#)

## G

gateway on Phone port [171](#)

gateway, analog [175](#)

GoS

defined [193](#)

functional characteristics [195](#)

## H

hardware components [32](#)

## I

IDS

flood attack [142](#)

packet anomalies [141](#)

scan attacks [144](#)

spoof attacks [144](#)

IDS (Intrusion Detection System) [140](#)

IKE (Internet Key Exchange)

configuration [150](#)

description [147](#)

firewall policy [151](#)

Initial Configuration Wizard [115](#)

interface

display [70](#)

Ethernet (eth0) [70](#)

internal log [64](#)

IP address, dynamic [47](#)

IP ToS [114](#)

IPsec

configuration [147](#)

description [147](#)

## J

jitter buffer [162](#)

jitter buffer settings [107](#)

## L

LAN switch

description [95](#)

duplex mode [96](#)

flow control [96](#)

ports [96](#)

QoS [98](#)

speed [96](#)

status [95](#)

LAN-to-LAN calls [161](#), [185](#)

LINE port [162](#)

link rate [111](#)

link, QoS [110](#)

local call routing [185](#)

Log Out [24](#)

log, system [64](#)

login [25](#), [43](#)

login problems [25](#)

## M

MAC address

proxy ARP [89](#)

routing to [86](#)

static ARP [88](#)

switch by [101](#)

max call display [29](#)

maximum licensed calls [168](#), [173](#)

media streams [161](#)

message destinations [66](#)

message type and severity [66](#)

MGCP, operational statistics [174](#)

MIB [56](#)

mirroring [97](#)

modem [175](#), [177](#), [180](#)

MoS (Mean Opinion Score) [107](#)

MTU (max transmission unit) [71](#)

Multicasting [94](#)

multi-line support (MLS) [177](#)

multimedia [113](#)

## N

NAPT (network address port translation) [132](#)

NAT (Network Address Translation) [132](#)

Network Address Translation (NAT)

interfaces display [134](#)

policies [133](#)

policy configuration [134](#)

public address [135](#)

numbering plan [181](#)

## O

Operations Pane [24](#)

**P**

packet fragment attacks [141](#)  
packet size, *see* MTU  
password [43](#)  
    authentication [44](#), [45](#)  
PAT (port address translation) [132](#)  
permissions [46](#)  
permissions, read/write [42](#)  
Phone port [162](#), [175](#)  
Phone port gateway [171](#)  
phone, analog [175](#)  
point-to-point tunnel [147](#)  
policing [194](#)  
port mirroring [97](#)  
PPP  
    link [73](#)  
    QoS [121](#)  
PPTP [139](#), [140](#)  
prioritize traffic [194](#)  
priority queues [191](#)  
proxy ARP [89](#)  
PSTN [162](#)

**Q**

QoS  
    ARP/PPP [121](#)  
    call bandwidth [198](#)  
    control signal [121](#), [167](#), [172](#)  
    downstream [118](#)  
    initial config wizard [115](#)  
    Layer 2 and 3 [190](#)  
    layer-2, LAN [98](#)  
    link, WAN [110](#), [111](#)  
    media streams [161](#)  
    overview [193](#)  
    PPTP [140](#)  
    quality group [112](#)  
quality class  
    defined [194](#)  
    setting [114](#)  
quality group  
    associate with [195](#)  
    configure [112](#)  
    defaults [116](#)  
    defined [193](#)  
    media and control signals [196](#)  
    media stream [161](#)  
queues [191](#)

**R**

RAM [32](#)  
read/write permissions [42](#)

relay services [78](#)  
reload configuration [24](#)  
restore configuration [63](#)  
R-Factor [107](#)  
RIP (Routing Information Protocol)  
routing  
    dynamic and static [86](#)  
    intro [86](#)  
    RIP [94](#)  
    routing table [87](#)  
routing engine [30](#)  
RSA encrypted [60](#)  
RTP ports range [161](#)  
running time [30](#), [32](#)

**S**

save changes [24](#)  
scan protection [144](#)  
secure gateway [147](#)  
Secure Socket Layer. *See* SSL  
security associations [147](#)  
security policies  
    constraints [125](#)  
    create new [130](#)  
    defaults [126](#)  
    Initial Configuration Wizard [127](#)  
    sequence of [125](#)  
    WAN interfaces [127](#)  
security, packet processing [124](#)  
server failover [166](#)  
service code [181](#)  
service interruption [185](#)  
services defaults [33](#)  
session controller [164](#), [171](#), [195](#)  
severity levels, system log [67](#)  
SIP  
    operational statistics [171](#)  
    server [164](#)  
SIP Data [113](#)  
SIP forking [168](#)  
SIP video [113](#)  
SNMP [56](#)  
SNTP  
    client [35](#)  
    relay [83](#)  
software  
    image [62](#)  
    upgrade [62](#)  
spoof attacks [144](#)  
SSH server [35](#)  
SSL  
    certificate [61](#)

---

- Certificate Signing Request [61](#)
  - intro [59](#)
  - key [59](#), [60](#)
- static IP address [25](#)
- statistics, cumulative
  - downstream QoS [120](#)
  - IP interface [72](#)
  - QoS link, best effort [111](#)
  - quality groups [116](#)
- statistics, instant
  - call quality [107](#)
  - quality groups [117](#)
- status, system overview [29](#)
- subnet [135](#)
- survivability [30](#)
- syslog [65](#)
- system information [31](#)
- system log [64](#)
  - destinations [66](#)
  - external server [65](#)
  - severity levels [67](#)

---

## T

- tagged VLAN [103](#)
- technical support session [64](#)
- Telnet [34](#)
- TFTP relay [80](#)
- ToS (type of service) [100](#), [192](#)
- traps (SNMP) [56](#)

---

## U

- unit name [31](#)
- untagged VLAN [103](#)
- user accounts [41](#), [43](#)

- User Agent
  - defined [175](#)
  - MGCP [179](#)
  - SIP [176](#)
- user mode [22](#)

---

## V

- video [113](#)
- virtual interface [75](#)
- VLAN
  - address range [73](#)
  - configuration [76](#)
  - LAN ports [103](#)
  - number of [76](#)
  - QoS [100](#), [191](#)
  - tagged/untagged [103](#)
  - virtual interface [75](#)
- VLSM (Variable-Length Subnet Mask) [94](#)
- Voice Activity Detection [177](#), [180](#)
- voice, identifying [195](#)
- VoIP
  - analog devices [175](#)
  - gateway [175](#)
- VPN (Virtual Private Network)
  - configuration [152](#)
  - description [147](#)

---

## W

- WAN configuration [70](#)
- web server [34](#)
- Web UI
  - connecting to [25](#)
  - introduction [21](#)
  - login [25](#)
- Weighted Fair Queuing (WFQ) [192](#)