CLI Reference Guide

BSGX4e
Business Gateway

NN47928-107
Software Release 2.1.1

BSGX4e 1.2
Business Services Gateway

Document Status: **Standard**

Document Version: **01.01**

Document Number: **NN47928-107**

Date: **July 2008**

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

1 About this guide

This chapter describes the intended audience for the Command Line Interface (CLI) Reference Guide, conventions, how the guide is organized, and how to get help.

This guide provides guidelines for configuring and monitoring the Business Service Gateway (BSG) X4e 2.1.1. The guide is designed for network managers, administrators, and technicians who are responsible for the management of networking equipment in enterprise and service provider environments. Knowledge of telecommunication technologies and standards, including telephony and Internet protocols, is assumed.

For installation information, see the appropriate installation guide (see Documentation on page 8).

Organization

The following table describes the content and organization of this guide.

Table 1 User guide organization

Chapter Title	Contents
2 Command interface overview	This chapter describes how to use the CLI for the BSGX4e 2.1.1.
Configuration Commands	This chapter lists the configuration commands in alphabetical order.

Conventions

The conventions listed in this section are used throughout the guide.

Command prompt convention

This guide assumes that the CLI is your primary method of interaction with the device. When using the CLI, you enter each command on a command line following the command prompt. The command prompt consists of a string followed by the **>** character. Because the string can be easily changed, by convention, this guide shows the command prompt as the > character only.

Text font conventions

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

Table 2 Text conventions

Font	Purpose
Note	Emphasizes information to improve product use.
Important	Indicates important information or instructions that must be followed.
Caution	Indicates how to avoid equipment damage or faulty application.
Warning	Issues warnings to avoid personal injury.
italic emphasis	Shows book titles, special terms, or emphasis.
bold emphasis	Shows strong emphasis.
`command`	Indicates a command that must be written as is. For example: **`config`**
`[parameter]`	Indicates a parameter associated with a command. This parameter must be written as is. For example: **`source [auto | dhcp | ppp | user]`**
<value>	Indicates the syntax description for a value. For example: **`config system info unit`** *<name>* In the previous example, <name> is the description of what is required for this field. A real name must be entered. For example: **`config system info unit BSGX4e`**

Documentation

The documentation CD shipped with the unit includes PDF files containing the following guides:

- BSGX4e Installation Guide
- BSGX4e Quick Start Guide
- BSGX4e CLI Reference Guide (this guide)
- BSGX4e Web UI Reference Guide

The PDF files are also available on the Nortel Web site: www.nortel.com

To view PDF files, use Adobe Acrobat® Reader® 5.0, or newer. Adobe Acrobat Reader can be obtained free from the Adobe Web site: www.adobe.com/products.

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

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

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

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.

2 COMMAND INTERFACE OVERVIEW

This chapter describes how to use the Command Line Interface (CLI) for the BSGX4e. The CLI provides commands for every function of the device. It also provides online help and an interactive mode for easier command entry.

This chapter discusses the following topics:

Command entry

This chapter assumes the BSGX4e has been installed in a working network as described in the Installation Guide and the Initial Configuration Guide. It also assumes that you can log in to the device from a terminal session at your workstation or the console.

A command prompt displays after logging in to the BSGX4e from a terminal session. The command prompt consists of a string followed by the **>** character. The string can be customized as described in the next section. Because the string can be changed, the convention in this guide is to show the command prompt as the **>** character:

```
>
```

Note: If your log in fails, retry the log in procedure to ensure you did not make a typing error. If log in fails again, a likely cause is your PC having a static IP address rather than using DHCP to obtain a dynamic address.

Enter any command in response to this prompt. However, if you logged in with a user ID that does not have authority to execute the command, the unit responds as in the following example:

```
> reboot
Invalid access for user 'user'!
```

For more information about the authority granted to user accounts, see User commands on page 168.

The Command Line Interpreter executes a command as soon as it is received.

- If the entire command is entered on one line, the command is executed immediately after the <**enter**> key is typed.
- If the command is entered in interactive mode (see Interactive mode on page 19), the command is executed as soon as its entry is complete (after entry of `exit` or <**ctrl-z**>).

Note: Although `config` commands change the current configuration immediately, the changes can be lost if the unit restarts. To save the changes to permanent memory, enter a **save** command.

Online help

To get online help with commands while logged in to the device, use the Help command.

General help

To list general information about the CLI, perform the following steps.

1. Type h**elp** after a command prompt and press the enter key:

   > help

   A long list appears. Commands are listed under the following headings:

   Maintenance Commands:

   Command Groups (CLI commands):

2. Notice the help listing describes how to get more specific command help for maintenance commands:

```
Help Summary:
------------

Maintenance Commands:

Type the name of any of the maintenance commands to execute
it. You can also
use the '?' to bring up help at any time. This displays
context help or help on the various parameters. For example,
'cp ?' to display help information for the 'cp' maintenance
command.

Command Groups:

You interact with these configurable items in a simple manner
by using a few
commands.

Commands:

config [command group] [command sub-group] [PK] [parameter <value>]

[command group] is the name of the group of commands, 'sip'
for example.
[command sub-group] is the name of the sub-group of commands,
'sc settings' for
example.
[parameter] is the name of a parameter, 'wanrxport' for
example.
<value> is the value of a parameter, '5060' for example.
[PK] is the primary key, some elements require this, others do
not.
You can choose to specify parameters. If no parameters are
specified, interactive edit mode starts. Each parameter can be
configured separately.
To abort the interactive edit mode enter ctrl^c, to save enter
ctrl^z or 'exit.'

Valid commands are:
```

```
config  - Configure an element's parameters
display - Displays the current configuration of an element
del     - Delete a particular element
show    - Shows the current active information about an
element
stats   - Statistics about a particular element
clear   - Clears statistics for an element

Parameter:

Boolean parameters are set by their name, unset by the 'no'
parameter.
IP parameters can be ranged, have masks (/24). For example,
192.16.1.20-192.16.1.25 and 192.168.1.1/24 are both valid IP
parameters.
Certain numeric parameters take a '+' or a '-' preceding the
numeric value as in
the case of 'config voice fxo gain tx -5.'
For parameters which are an enumerated type, you can cycle
through options with
'<TAB>' while in interactive edit mode.

Custom Help:

Type help command mng-element
This provides help on the element. For example, 'help config
interface ip.'
You can also use the '<TAB>' and '?' keys to display
additional help:
'config interface ip <TAB>' or 'config interface ip?'.
```

Specific help

Perform one of the following actions for specific help.

- Specify the command on the **help** command
- Enter part of the command followed by the **Tab** key or the **?** key

For example, for information about the command to configure an IP interface, enter any of the following commands:

- > help config interface ip
- > config interface ip?
- > config interface ip<TAB>

In response to any of the preceding commands, the online help display lists the parameters for **config interface ip**, as follows:

```
> config interface ip

[if]       Interface to change behavior of (eth0 | eth1)
ip          IP address and mask of interface
mtu        The Maximum Transmission Unit (MTU) of the
            interface (72-1500)
dhcpclient Obtain address using DHCP (no | yes)
status      Configuration status of the interface (up | down)
speed      Speed/Duplex (Auto | 10Half | 10Full | 100Half |
            100Full)
```

CLI command syntax

The following syntax applies to CLI commands:

config [command group] [command sub-group] [PK] [**parameter** *<value>*]

For a description of the syntax, see General help on page 13.

Enter a **command group** followed by a **?**, to list all **subcommand groups**. For example:

```
>config ids?
ids anomaly                          Anomaly based IDS prevention
ids flood activity                 IDS Flood protection
ids flood settings                 IDS Flood protection
ids scan                           IDS Scan protection
ids spoof                          IDS spoofing protection
```

Enter a **command group** and **sub-command** group and a **?** to see the **[PK]** and **parameters** associated with that sub-command. For example:

```
> config ids anomaly

attack    Attack type to detect and drop
          (fragoverlap|fragoverrun|fragtooshort)
active    Whether or not attack detection is applied
          (no | yes)
```

In the previous example, **attack** is a parameter and the values are **fragoverlap**, **fragoverrun,** and **fragtooshort**. For detailed information about parameters and values, see Parameter values on page 16.

Parameter values

In general, a parameter is specified by its name followed by its value. For example, *port 2600* specifies the value *2600* for the *port* parameter.

The following lists exceptions for specifying parameter values:

- Primary Key

  If the first parameter for a command is listed in brackets (such as [name]), it is a primary key parameter and specifies the object of the command. The primary key value is specified without its parameter name.
  For example, the first parameter of the command **config ids spoof** is listed as **[name]** and the second parameter as **type**. When you enter the command, specify just the value for the first parameter, but both the name and its value for the second parameter.

  ```
  > config ids spoof eth1 type trusted
  ```

- Booleans

Boolean parameters are parameters with two states (on/off or yes/no). To specify the on/yes state, you can specify just the parameter name, omitting any value. To specify the off/no state, you can specify the parameter name followed by the **no** value.

For example, the following command specifies the on/yes state for its **enabled** parameter:

```
> config user account user1 enabled
```

To specify the off/no state for the **enabled** parameter, specify:

```
> config user account user1 enabled no
```

- IP address ranges

  When an IP address range is specified, it can be specified by a hyphen between the first and last addresses of the range (`192.16.1.20-192.16.1.25`) or by a subnet mask suffix (`192.168.1.1/24`).

- Numeric offsets

  Certain numeric parameters take a plus (**+**) or a minus (**-**) preceding the numeric value to indicate an offset. For example, to configure a gain of -5, specify:

```
> config voice fxo gain tx -5
```

Command keyword NO

The keyword `no` is used to turn off a boolean parameter or to clear string parameters (that is, to fill the string value with blanks).

The **no** keyword must always be used before the affected parameter. For example, the following command turns off the Netflow agent by turning off the boolean parameter **enabled**.

```
> config netflow agent no enabled
```

As an example of using **no** to clear a string parameter, the following command clears the name of the unit. (The default unit name is MyUnit.)

```
> config system info no unit
```

- To see the result, enter:

```
> show system info
```

- The Unit Name is now blank:

```
System Info:

   Unit Name
   Bootcode Ver     1.10.0012
   App. Ver         2.1.0-00E-0085
   System Type      BSGX4e
   Memory           106/128 MB
   MAC 0            00:15:93:FE:01:18
   MAC 1            00:15:93:FE:01:19
   Serial           140
```

```
Country          United States of America (US)
Temp             Unsupported
Up time          0y 5d 20h 43m 37s
Reset by         software reset
```

Command keyword ALL

The keyword **all** is used to perform the command on all entries. The command action can be modification, deletion, clearing of statistics, or display.

For example, the following command changes the specified parameter for *all* QoS Quality Groups. (The command changes the **iptos** parameter value to 248.)

```
> config qos group iptos all 248
```

- To see the result, enter:

```
> show qos group all

QoS Quality Groups:

Name        Link  QG    Type     Committed  Burst      IPToS COS
-------------------------------------------------------------------
Management  eth0  A2    car      1000000    100000000  248   no
VoIP        eth0  A1    policed  89000000   0          248   no
```

As another example, the following command deletes *all* QoS Quality Groups.

```
> del qos group all
```

Interactive mode

Interactive mode allows a command to be entered all on one line or split between two or more lines. With single line entry, the command and all its parameters are typed before you press **<enter>**. In interactive mode, the command is entered on one line, but its parameters can be entered on one or more following lines.

Interactive mode is provided for most CLI commands. Some commands require that the command and its *primary key* be entered on the first line. The primary key is the object of the command, such as a user account name. In the parameter lists in this guide, a primary key parameter is shown in brackets.

To get help while in interactive mode, enter a question mark (**?**).

In the following example, the command **config security nat policy** and its primary key `new` are entered on the first line, and then the other command parameters are entered on following lines:

```
> config security nat policy new
Entering interactive mode: ctrl^z | 'exit', ctrl^c | 'quit'
                           TAB to cycle parameter options
nat-pol-new#> type rport
nat-pol-new#> address 10.0.1.130
nat-pol-new#> port 2600
nat-pol-new#> exit
```

Note: The command prompt changes while in interactive mode.

Note: To leave interactive mode, enter **exit** or the key combination **ctrl-z** to execute the command, or enter **quit** or the key combination **ctrl-c** to cancel the command.

3 CONFIGURATION COMMANDS

This chapter lists the BSGX4e configuration commands in alphabetical order. Configuration commands have the following syntax:

config [command group] [command sub-group] [PK] [**parameter** *<value>*]

See General help on page 13 for a description of the syntax.

The following are configuration commands:

Audit status command

Audit logging logs events that affect system security, such as system configuration changes and invalid log in attempts.

Use this command to configure audit logging:

audit status

audit status

Use this command to configure audit logging. Audit logging fills a table of 100 entries in FIFO order.

Note: In the current version, the audit log is saved on compact flash.

Syntax

```
config audit status enabled [yes|no]
```

Parameters

enabled yes|no	Enable/disable audit logging. The default is enabled (yes).

Example

```
> config audit status enabled no
```

The following example accesses a stored audit log.

Example

```
> ls /cf0usr/Audit
.
..
auditlog

> cat /cf0usr/Audit/auditlog
08:33:11: admin CONFIG shell terminal
09:35:14: nnadmin INVALID LOGON at TUE MAY 15 09:35:14 2007
09:35:19: nnadmin INVALID LOGON at TUE MAY 15 09:35:19 2007
09:36:38: admin CONFIG sip ua port 1
11:46:12: admin CONFIG system images 1
```

Related commands

```
display audit status
show audit status
```

ARP command

This section describes how to configure ARP:

- arp table

arp table

ARP is a network layer protocol that automatically maps IP addresses to hardware Media Access Control (MAC) addresses. When a network node sends data to an IP address on its segment, it broadcasts an ARP request to resolve the IP address to an Ethernet MAC address.

ARP runs over Ethernet only.

ARP maintains the ARP table in the BSGX4e. Each entry in the table maps an IP address to a MAC address. The entries can be dynamic or static:

- A dynamic ARP entry is automatically configured and is automatically flushed after a certain period of time.
- A static ARP entry is manually configured and is only flushed manually.

The ARP table only maps IP addresses within the IP sub-network assigned to the BSGX4e. To see the IP address subnets, enter the command **`show interface ip`**.

Syntax

`config arp` *<host>* **`macaddress`** *<address>*

Parameters

host	Enter the IP address for the host.
`mac address` *address*	Enter the MAC address.

Example

```
> config arp 192.168.134.163 macaddress 00:11:22:33:44:55
```

Related commands

```
del arp table
display arp table
show arp table
```

Calls analyser command

Voice Quality Monitoring (VQM) measures call quality and monitors calls. Video is not monitored. The VQM analyser simulates a jitter buffer to analyze VoIP media streams to deduce information such as packet loss, delay, and jitter. Based on these parameters, VQM calculates R-Factors and Mean Opinion Scores updated in real-time over the duration of calls. The alarm levels and the duration of an alarm are also specified. Alarms are reported in the system log as INFORM messages. The VQM analyser also reports statistics for every VoIP media stream that flows through the routing engine. The flows that are analysed depend on whether the call is a local call or an external call and whether direct media (the **dm** media setting) is enabled in the Media Settings command. See media settings on page 71 for more information.

For external calls (either between the LAN to the WAN or between the User Agent to the WAN), only the inbound flow (from the WAN) is monitored by VQM. Similarly, for local calls between the User Agent and the LAN, only the inbound flow (from the LAN) is monitored. However, for local calls between LAN endpoints, the **dm** setting determines if the flow is monitored.

- If **dm** is enabled, the session controller can directly establish RTP flows between two LAN endpoints. The VQM analyser cannot measure those direct media flows.
- If **dm** is disabled, the RTP flows between LAN endpoints are bridged by the routing engine and both flows can be measured by VQM.

Use this command to configure voice quality monitoring:

call analyzer

call analyzer

Use this command to configure voice quality monitoring.

Syntax

config

jb [static|adpative] **min** *<buffer size>* **max** *<buffer size>* **nom** *<level>* **rtdelay** <ms> **quality** [yes|no] **burst** [yes|no] **delay** [yes|no] **rquality** <seconds> **rburst** <seconds> **burstmin** <ms> **delaymax** <ms> **qalertclear** <seconds> **balertclear** <seconds> **dalertclear** <seconds>

Parameters

jb static|adaptive	Specify a static or adaptive jitter buffer**.**
min *buffer size*	Specify the minimum size of the simulated jitter buffer. The default is **10.**
max *buffer size*	Specify the maximum size of the simulated jitter buffer. The default is **60.**
nom *level*	Specify the nominal size of the simulated jitter buffer. The default is **30.**
rtdelay *ms*	Estimate of round trip delay if no RTCP records are detected. The default is **60** milliseconds (ms).
quality yes|no	Enable alarms for low quality R-factor. The default is **yes**.
burst yes|no	Enable alarms for excessive bursting. The default is **yes**.
delay yes|no	Enable alarms for excessive bursting. The default is **yes**.
rquality *seconds*	Alarm trigger for low quality R-Factor. The default is **60**.
rburst *seconds*	Alarm trigger for excessive bursting. The default is **60**.
burstmin *ms*	Minimum alarm trigger for excessive bursting duration (in ms). The default is **500** ms.
delaymax *ms*	Maximum alarm trigger for excessive delay (in ms). The default is **450** ms.
qalertclear *seconds*	Minimum duration until the low quality alarm is cleared. The default is **3** seconds.
balertclear *seconds*	Minimum duration until the excessive bursting alarm is cleared. The default is **3** seconds.
dalertclear *seconds*	Minimum duration until the excessive delay alarm is cleared. The default is **3** seconds.

Example

```
> config call analyser jb static quality yes burst yes delay
yes rquality 50 rburst 50 minburst 1000 maxdelay 100
```

Related commands

```
display calls analyser
show calls analyser
show calls current
show calls history
show calls alarms
show calls quality
stats calls quality
```

DHCP server command

DHCP provides configuration parameters to IP hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP Server to a host and a mechanism for allocating network addresses to hosts. DHCP is built on a client/server model, where designated DHCP Server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts. The DHCP Server identifies the IP subnet in which the DHCP client resides, and can assign an IP address from a pool of valid IP addresses in that subnet.

Use the following commands to configure the DHCP Server:

- dhcps group
- dhcps host
- dhcps option
- dhcps pool
- dhcps vendorclass

dhcps group

Use this command to configure a name for a DHCP server (DHCPS) group. This name is necessary for configuring other DHCPS commands.

Syntax **config dhcps group** *<name>*

Parameter

name	Enter a name for this DHCP server group.

Example

```
> config dhcps group engineering
```

Related commands

```
del dhcps group
display dhcps group
show dhcps group
```

dhcps host

The DHCPS host configures the server so that a client with a given MAC always receives the same IP address as well as overrides the options specified for the pool covering the interface on which the request was received.

Syntax

config dhcps host [new|*<id>*] **macaddress** *<mac address>* **ip** *<ip address>* **optiongroup** *<string>* **description** *<string>*

Parameters

id	Enter new for a new host or an exiting ID for reconfiguring.
macaddress *mac address*	Enter the DHCP MAC address of the host.
ip *ip address*	Enter the IP address to assign to the host. The IP address must be in the range of the subnet assigned to the interface on which the DHCP server is defined.
optiongroup *string*	Enter the option group name, as specified in dhcps option.
description *string*	Enter an optional description for this host.

Example

```
> config dhcps host new macaddress 11:22:33:44:55:66 ip
192.168.1.9 optiongroup test description "test host"
```

Related commands

```
del dhcps host
display dhcps host
show dhcps group
show dhcps host
show dhcps option
```

dhcps option

A DHCP option is information that can be sent to a client when assigning a client an IP address. Any given option code name can be configured with different values when assigned to different groups.

Each DHCP option has a code, but these codes are not displayed to users. Users deal only with option names.

Use this command to configure the DHCP server (DHCPS) option settings.

Syntax

```
config dhcps option [new|<id>] group <name> code (bootfile-name|domain-name|domain-name-servers|ntp-servers|option-150|option-151|option-160|option-161|routers|tftp-server-name|time-offset) value <value>
```

Parameters

id	Enter new for a new host or an existing ID for reconfiguring.
group *name*	Enter the name of the group. Once entered, this information can not be changed.
code *type*	Enter the code type. If the tftp-server-name and option-150 are both configured, the DHCP client device uses the option-150 as tftp server address, and not the tftp-server-name address. This also applies to option 160 when it is configured with option tftpserver-name.
value *value*	Enter the value of the code. The time offset unit can be entered as either HH:MM or NNNN seconds. The time offset from Coordinated Universal Time (UTC). Specify time East of UTC as positive (+) and West as negative (–).

Example

```
> config dhcps option new group test code time-offset value 10
```

Related commands

```
display dhcps option
del dhcps option
show dhcps group
show dhcps option
```

dhcps pool

The DHCPS manages a pool of IP addresses and also has information about client configuration parameters, such as the default gateway, the domain name, and DNS servers. A query for information or IP addresses is typically initiated immediately after booting up and must be completed before the client can initiate IP-based communication with other hosts. The DHCPS replies to the client with an IP address, subnet mask, default gateway, and other requested information such as DNS server, and so on. Use this command to configure the DHCP pool information.

Note: The DHCP server can not be running while the DHCP relay is enabled.

Syntax

config dhcps pool interface *<if>* **enabled** [yes|no] **subnet** *<address>* **netmask** *<address>* **ip** *<ipaddress>* **broadcast** *<address>* **lease** *<days>* **gateway** *<address>* **dns1** *<address>* **optiongroup** *<name>*

Parameters

interface *if*	Enter the interface type for this pool.
enabled yes|no	Enable/disable this pool.
subnet *address*	Enter the subnet address in x.x.x.x format. This address is the same as the address defined on the interface on which the DCHP server is defined.
netmask *address*	Enter the netmask address in x.x.x.x format. This address is the same as the address defined on the interface on which the DCHP server is defined.
ip *ip address*	Enter the IP address in x.x.x.x format. The IP range must be in the range of the subnet assigned to the interface on which the dhcp server is defined. The default range is 192.168.1.50 to 192.168.1.250.
broadcast *address*	Enter the broadcast address in x.x.x.x format. This address is the same as the address defined on the interface on which the DCHP server is defined.
lease *days*	Specify the number of days to provide a lease. The valid range is 1–7.
gateway *address*	Enter the default router address in x.x.x.x format.
dns1 *address*	Enter the address of the primary DNS server.
optiongroup *name*	Enter the name of a group of options to be sent to the client with its IP address. This name is specified in dhcps option.

Example

This example configures a DHCP server on the eth1 interface (10.0.1.1/24) of the BSGX4e.

```
> config dhcps pool eth1
Entering interactive mode ctrl^z | 'exit', ctrl^c | 'quit'
```

```
*dhcps-pool-eth1#*> subnet 10.0.1.0
*dhcps-pool-eth1#*> netmask 255.255.255.0
*dhcps-pool-eth1#*> ip 10.0.1.100 - 10.0.1.200
*dhcps-pool-eth1#*> broadcast 10.0.1.255
*dhcps-pool-eth1#*> lease 1
*dhcps-pool-eth1#*> gateway 10.0.1.1
*dhcps-pool-eth1#*> dns1 10.0.1.1
*dhcps-pool-eth1#*> optiongroup name
```

Related commands

```
del dhcps pool
del dhcps leas
display dhcps pool
show dhcps group
show dhcps lease
show dhcps option
show dhcps pool
```

dhcps vendorclass

Use this command to configure the options according to the vendor class identifier sent by a client. The vendor class can be refined by giving an interface; in this case the options are only applied if both the vendor class identifier and interface match the incoming DHCP request.

Syntax

config dhcps vendorclass *<id>* **vendorclass** *<id>* **interface** [eth0|eth1|none] **optiongroup** *<name>*

Parameters

id	Enter a unique identification for this vendorclass. Enter new for the next sequential ID to be automatically assigned or assign an ID by entering a number. Enter **show dhcps vendorclass** to view all assigned IDs.
vendorclass *id*	Enter the vendor class reported by the client.
interface eth0|eth1|none	Specify the interface.
optiongroup *name*	Enter the name of a group of options to be sent to the client with its IP address. This name is specified in dhcps option.

Example

```
> config dhcps vendorclass new Interface eth1 OptionGroup 1
```

Related commands

```
display dhcps vendorclass
del dhcps vendorclass
show dhcps vendorclass
show dhcps group
show dhcps option
```

Firewall connection timeout command

The firewall dynamically opens and closes ports for data traffic. Some TCP-based applications (such as Telnet, FTP, and HTTP) open connections to external servers, which can be left idle for extended periods. Leaving a port open and idle can create a security risk. Use this command to configure the firewall connection timers:

- firewall TCP

firewall TCP

Setting a timer for firewall connections limits how long a port can remain idle before it is closed. Separate firewall time-outs can be configured for TCP connections and HTTP connections. Use this command to configure the timeout for these connections.

Syntax

config firewall tcp defaulttimeout *<seconds>* **httptimeout** *<seconds>*

Parameters

defaulttimeout *seconds*

Enter the default TCP timeout. The valid range is 60 - 172800 seconds (two days). The default is **7200** seconds (two hours).

httptimeout *seconds*

Enter the HTTP timeout. The valid range is 60-172800 seconds (two days). The default is **300** seconds (5 minutes).

Example

```
> config firewall httptimeout 360
```

Related commands

```
display firewall tcp
show firewall tcp
```

Intrusion detection system commands

The Intrusion Detection System (IDS) defense is designed for protection against attacks that are destined for the BSGX4e or the LAN.

IDS inspects all inbound and outbound network activity and identifies patterns that can indicate system attacks. Table 3 lists the applicable protocols.

IDS identifies the following types of attacks:

- Packet anomaly—Protects the unit from abnormal packets that intend to crash the destination.
- Scan—Protects the unit from useless packets that intend to locate holes in the firewall.
- Flood—Protects the unit from excess incoming packets that can overload the unit.
- Spoof—Protects the LAN network and the unit from intrusion. IDS spoof protection is applicable for all configured untrusted interfaces (see ids spoof on page 47).

Table 3 Protocols for which IDS attack protection applies

Attack	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	

Note: For a secure system, Nortel recommends that IDS protection remains enabled.

Use the following commands to configure IDS:

- ids anomaly
- ids flood activity
- ids flood settings
- ids scan
- ids spoof

ids anomaly

This command enables and disables protection against packet fragments anomalies. Protection can be enabled or disabled for the following anomalies:

- 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 is 800. If it is less than 800, the second fragment overlaps the first fragment. This condition can 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. The following table lists the other anomalies.

Table 4 Packet Anomaly Attacks

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

Syntax

```
config ids anomaly [fragoverlap|fragoverrun|fragtooshort]
active [no|yes]
```

Parameters

attack fragoverlap|fragoverrun|fragtooshort

Specify the packet fragment anomaly to detect.

fragoverlap — The offset of one fragment overlaps the offset of another fragment.

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

	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.
active no|yes	Enable/disable attack detection.

Example

```
> config ids anomaly fragoverlap active yes
```

Related commands

```
show ids anomaly
display ids anomaly
show ids attacks
clear ids attacks
```

ids flood activity

Flood attacks result in denial of service. IDS can detect floods targeted at protocols and services. IDS refers to a threshold value to detect a flood attack. The threshold varies depending on the protocol or service being protected. Use this command to configure IDS flood detection.

Syntax

```
config ids flood activity [udpflood|icmpflood|arpflood|
synflood|espflood|unknowipprotoflood|stpflood|cdpflood|
unknowntypeflood] active [no|yes]
```

Parameters

```
attack udpflood|icmpflood|arpflood|
synflood|espflood|unknowipprotoflood|stpflood|cdpflood|
unknowntypeflood
```

Specify the flood activity to detect.

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.

espflood — Encapsulated Security Payload (ESP) flood. An ESP flood sends bad IPsec traffic. Packets are discarded after the threshold rate limit is reached.

unknowipprotoflood — This flood activity type refers to floods for IP protocols other than those listed specifically.

stpflood — Spanning Tree Protocol (STP) flood. An STP flood sends bad STP packets. Packets are discarded after the threshold rate limit is reached.

cdpflood — 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.

	unknowntypeflood — This flood activity type refers to floods targeting Ethernet activities other than ARP, STP and CDP.
active no|yes	Enable/disable attack detection.

Example

```
> config ids flood activity icmpflood active yes
```

Related commands

```
display ids flood activity
show ids flood activity
show ids attacks
clear ids attacks
```

ids flood settings

This command describes how to change threshold values for IDS flood protection. IDS refers to a threshold value to detect a flood attack. The threshold can be changed for some protocols and services:

- Known protocols: ARP, ICMP, UDP, TCP, ESP
- Any protocol other than the known protocols listed above (unknown_ip_proto).
- Known services: DHCP, DNS, IKE, MGCP, RADIUS, RIP, SIP, SNMP, SNTP, TFTP
- Any service (port) other than the known services listed above (unknown_port).

The following table lists the default threshold values,

Table 5 Default Flood Threshold Values

Protocol or Service	Default Threshold Level	Protocol or Service	Default Threshold Level	Protocol or Service	Default Threshold Level
dhcp	10	radius_1	100	sntp	10
dns	20	radius_2	100	tftp	100
esp	100	rip	20	unknown_IP_proto	500
ike	100	sip	255	unknown_port	500
mgcp	255	snmp	300		

Syntax

config ids flood settings [dhcp|dns|esp|ike| mgcp|radius_1| radius_2|rip|sip|snmp|sntp|tftp|unknown_IP_proto| unknown_port] **threshold** *<pps>*

Parameters

service dhcp|dns|esp|ike| mgcp|radius_1| radius_2|rip|sip|snmp|sntp|tftp|unknown_IP_proto| unknown_port

Specify the Protocol or service with a changed value threshold. See Table 5 for the default values. radius_1 and radius_2 are the ports RADIUS is using.

threshold *pps*

Enter the minimum number of packets/second to be considered an attack.

Example

```
> config ids flood settings dhcp threshold 5
```

Related commands

```
display ids flood settings
show ids flood settings
clear ids attacks
show ids attacks
```

ids scan

IDS scan protection can be activated for ICMP, UDP, 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 (ICMP, UDP, or TCP) for the timeout interval. This command activates a scan time or changes the timeout value.

Syntax

config ids scan [updportscan|tcpportscan|pingsweep] **timeout** *<seconds>* **active** [no|yes]

Parameters

attack updportscan|tcpportscan|pingsweep	Specify the attack type to scan. **udpportscan** — A port scan is a series of messages sent by a potential system intruder to determine which services the system provides. 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 is a means to locate network devices that are active and responding, and so, can be targets for an attack.
timeout *seconds*	Enter the timeout after an attack is detected. The default is 50 seconds for udpportscan and tcpsynscan, and 60 seconds for pingsweep.
active no|yes	Enable/disable attack protection.

Example

```
> config ids scan udpportscan timeout 30 active yes
```

Related commands

```
display ids scan
show ids scan
clear ids attacks
show ids attacks
display ids flood settings
show ids flood settings
clear ids attacks
show ids attacks
```

ids spoof

IDS spoof detection can be activated for all IP interfaces, including eth0, eth1, the PPP interface, vifX (VLAN), and VPN interfaces. IDS spoof detection defines the IP interfaces as trusted or untrusted interfaces.

By default, IDS assumes the trust settings shown in Table 6.

IDS assumes that spoof attacks arrive from the WAN and by default assigns untrusted status to WAN interfaces. This activates spoof detection for these 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.

Table 6 Default Trust Settings for Interfaces

Interface	Trust Setting
eth0	untrusted
eth1	trusted
WAN vif*n*	untrusted
LAN vif*n*	trusted
vpn*n*	trusted
ppp0	untrusted

This command changes IDS spoof detection on an IP interface.

Syntax

```
config ids spoof [eth0|eth1|ppp0] type [trusted|untrusted]
```

Parameters

name eth0|eth1|ppp0

Specify the interface name.

type trusted|untrusted

Specify whether the interface is a trusted or untrusted interface. IDS checks for spoof attacks on untrusted interfaces only.

Example

```
> config ids spoof eth1 type untrusted
```

Related commands

```
display ids spoof
show ids spoof
clear ids attacks
show ids attacks
```

Internet key exchange commands

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. Use the following commands to configure IKE:

- ike parameters
- ike preshared

ike parameters

The IKE SA is re-negotiated when its lifetime expires; the shorter the lifetime, the more frequently the IKE SA is re-negotiated. Thus, a shorter lifetime increases security. Use this command to configures the IKE parameters.

Syntax

config ike parameters lifetime *<seconds>* **maxlifetime** *<seconds>*

Parameters

lifetime *seconds*	Specify the default IKE SA lifetime. This is the initial value used for negotiations with the remote host. The initial setting is **86400** (24 hours).
maxlifetime *seconds*	Specify the maximum IKE SA lifetime. This is the maximum value the BSGX4e accepts during negotiations. The initial setting is **259200** (72 hours).

Example

```
> config ike parameters lifetime 3000 maxlifetime 30000
```

Related commands

```
display ike parameters
show ike parameters
clear protocol ike
show protocol ike
clear ike sa
show ike sa
```

ike preshared

An IKE preshared key record specifies the preshared key used to encrypt ISAKMP messages. An IKE preshared key record defines the key (similar to a password) used to authenticate a remote secure gateway.

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 rule 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.

Syntax

config ike preshared *<hostname|ip address>* **key** *<string>*

Parameters

peer hostname|*ip address*

Enter the peer host name or IP address of the remote gateway.

key *string*

Enter a preshared key (up to 50 characters). The same preshared key must be configured at the remote gateway.

Example

```
> config ike preshared 10.0.1.2 key 1J3W5RE89
```

Related commands

```
del ike preshared
display ike preshared
show ike preshared
clear protocol ike
show protocol ike
clear ike sa
show ike sa
```

Interface commands

This section describes how to configure the interface that connects the BSGX4e to an external network, or WAN. Ethernet WAN interface runs up to 100 Mbps; Ethernet LAN interface runs on 100 Mbps.

The virtual interfaces that can be configured over these interfaces are as follows:

- WAN Ethernet
- PPP over WAN Ethernet
- VLAN over LAN or WAN Ethernet

IP interfaces that can be configured over all these interfaces:

- IP over Ethernet
- IP over PPP
- IP over VLAN

Use these commands to configure the LAN or WAN interfaces of the BSGX4e:

- interface ip
- interface ppp
- interface vlan

interface ip

Use this command to configure the IP settings of the BSGX4e interfaces. The interface ip command also configures the Ethernet settings (speed and mode) for the Ethernet interfaces.

Syntax

config interface ip [eth0|eth1] **ip** *<ip address/mask>* **mtu** *<bytes>* **dhcpclient** [no|yes] **status** [up|down] **speed** [Auto|10Half|10Full|100Half|100Full]

Parameters

if eth0|eth1	Specify the interface type.
ip *ip address/mask*	Specify the IP address and mask of the interface. Specify an address only if DHCP is disabled. The address/mask can be specified with dotted-decimal or CIDR notation (for example, 192.168.15.33/255.255.255.0 or 192.168.15.33/24). The default is 0.0.0.0/0.0.0.0.
dhcpclient no|yes	Enable/disable DHCP for this interface. The default is yes for the WAN and no for the LAN.
status up|down	Enable/disable the interface. The default is up.
speed Auto|10Half|10Full|100Half|100Full	Configure the speed and duplex mode for eth0. For auto-negotiation, specify **auto**; otherwise, specify **10** or **100** Mbps and **half** or **full** duplex.

Example

The following example enables DHCP service for the eth0 interface.

```
> config interface ip eth0 dhcp
```

Example

The following example configures a static IP address for the WAN interface and disables DHCP service.

```
> config interface ip eth0 ip 172.29.19.10/16 dhcp off
```

Related commands

```
display interface ip
del interface ip
display interface ip
show interface ip
stats interface ip
```

interface ppp

Use this command to configure the BSGX4e to use a PPP link as its primary WAN interface. To use a PPP link, PPP parameters must be stored as a PPP profile; when activated, the profile directs the activity of the PPP client in the BSGX4e.

The PPP client supports a single PPP session (ppp0) and is compliant with RFC 2516 (PPPoE).

Note: On the BSGX4e, DHCP service must be disabled for the eth0 interface. (Use the command `config interface ip eth0 dhcp off`). See interface ip on page 52 for more information.

Traffic through the ppp0 interface is controlled by the security policies for the interface. Security policy configuration is described in Security commands on page 111.

Syntax

config interface ppp 0 l2interface [eth0] **active** [no|yes] **authproto** [PAP|CHAP|MSCHAPV1|MSCHAPV2] **selfip** *<ip address>* **mtu** <bytes> **mru** *<bytes>* **restarttime** *<ms>* **servicename** *<string>* **user** <string> **password** <password>

Parameters

l2interface eth0

Specify the layer 2 interface. Use eth0 for the BSGX4e.

active no|yes

Specify yes to activate the profile. Specify no 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 **no**.

authproto PAP|CHAP|MSCHAPV1|MSCHAPV2

Specify an authentication protocol. The default is PAP.

selfip *ip address*

Enter an optional static IP address for the ppp0 interface.

mtu *bytes*

Enter the Maximum Transmission Unit (MTU) of the interface (296-1492 bytes). The default is **1492** bytes.

mru *bytes*

Enter the Maximum Receive Unit (MRU) of the interface (296-1492 bytes). The default is **1492** bytes.

restarttime *ms*

Enter the Time interval before a request is re-sent (in milliseconds). The default is **3000** (3 seconds).

servicename *string*

Enter a service name (up to 30 characters) if required by the Internet Service Provider (ISP). The ISP determines the valid values.

user *string*	Enter a user name (up to 32 characters) as provided by the ISP.
password *string*	Enter a log in password (up to 32 characters) as provided by the ISP.

Example

The following example sets up the PPP link as the WAN interface on the BSGX4e.

- The first command turns off DHCP service on the eth0 interface.
- The second command configures and activates the PPP profile. The profile specifies a static IP address for the PPP interface (**ppp0**); it also specifies values provided by the ISP for logging in to the PPP access concentrator (**servicename, user,** and **password**). The parameter **active yes** activates the profile and automatically creates the WAN interface.
- The next commands configure security policies to allow the same traffic for ppp0 as the default policies for eth0.

```
> config interface ip eth0 dhcp off

> config interface ppp 0

Entering interactive mode: ctrl^z | 'exit', ctrl^c | 'quit"
                            TAB to cycle parameter options
profile-ppp-0#> active yes
profile-ppp-0#> selfip 2.2.2.2
profile-ppp-0#> servicename ip
profile-ppp-0#> user user40
profile-ppp-0#> password pppsecret
profile-ppp-0#> exit

> config security policy new from eth1 to ppp0 action allow

> config security policy new from ppp0 to self dport 22 proto
tcp action allow

> config security policy new from ppp0 to self dport 23 proto
tcp action allow

> config security policy new from ppp0 to self dport 443 proto
tcp action allow

> config security policy new from ppp0 to self dport 80 proto
tcp action allow
```

Related commands

```
clear interface ppp
display interface ppp
del interface ppp
stats interface ppp
show interface ppp
show interface ip
```

interface vlan

Use this command to configure a virtual interface (vif) for a VLAN to assign it an IP address. A virtual interface and IP address assignment enable the BSGX4e to route IP traffic to and from the VLAN. The firewall must be configured to route traffic through the interface.

- **Note:** One or more ports must be assigned to the VLAN before a virtual interface is configured for the VLAN. Up to sixteen virtual interfaces can be configured. Virtual interfaces are referenced as vif*n*, where *n* is 0 through 15. A virtual interface can be configured on whichever Ethernet interface (eth0 or eth1).

Syntax

config interface vlan *<vid>* **interface** [etho|eth1] **status** [up|down] **comment** *<string>*

Parameters

vlan *vid*	Enter the VLAN ID. The valid range is 1-4094. Specify the vid used when the ports of the switch were assigned to the VLAN. To list the VIDs, enter **show switch vlan**.
interface eth0|eth1	Specify the physical ethernet interface on which the virtual interface is configured (eth0 for the WAN interface or eth1 for the LAN interface). (If eth0 is specified, the WAN port is automatically assigned to the VLAN).
status on|off	Enable/disable the virtual interface. The default is **off**.
comment *<string>*	Enter an option comment.

Example

```
> config interface vlan 1 interface eth1
```

Related commands

```
display interface vlan
del interface vlan
show interface vlan
show switch vlan
```

IP security commands

IPsec provides data confidentiality, data integrity, and data authentication between peers.

The Internet Key Exchange protocol (IKE) defines how pairs of secure gateways negotiate IPSec security associations (IPsec SAs).

The IPsec SAs negotiated are determined by the configuration of IPsec policies and IPsec proposals. Use the following commands to configure IPsec:

- ipsec parameters
- ipsec policy
- ipsec proposal

ipsec parameters

Use this command to define the IPsec parameters for maximum lifetimes for an IPsec security association (SA) and the Diffie-Hellman group to use for session key exchange. The default provides for automatic negotiation of the DH group.

Syntax

config ipsec parameters lifetime *<seconds>* **maxlifetime** *<seconds>* **group** [dh1024|dh768|nopfs|auto]

Parameters

lifetime *seconds*

Define the Default IPsec SA lifetime. This is the initial value used for negotiations with the remote host. The default is 28800 (8 hours).

maxlifetime *seconds*

Define the maximum IPsec SA lifetime. This is the maximum value the BSGX4e accepts during negotiations. The default is 86400 (24 hours).

group dh1024|dh768|nopfs|auto

Diffie-Hellman group to use for session key exchange. Use the value **nopfs** to disable perfect forward secrecy. The default is **auto**.

Example

```
> config ipsec parameters lifetime 28000 maxlifetime 86400
group dh1024
```

Related commands

```
display ipsec parameters
show ipsec parameters
display ipsec parameters
show ipsec parameters
clear protocol esp
show protocol esp
clear protocol ike
show protocol ike
display ipsec parameters
show ipsec parameters
```

ipsec policy

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 configuration of an IPsec policy also allows an IP interface to be configured for the policy. The following are required for an IPSec policy to bring up a successful VPN tunnel:

- A preshared key must be defined for the remote secure gateway. The gateway parameter of the policy must match the peer of a preshared key record. The same preshared key value must be configured at the remote secure gateway.
- The VPN interface must be assigned an IP address.
- A route must send traffic to the VPN interface.
- A firewall policy must allow ESP traffic from the remote secure gateway. (IP packets sent from the remote secure network to the local secure network are encrypted as ESP packets.)
- A firewall policy must allow IP packets sent from the local secure network to the remote secure network. Otherwise, ESP packets cannot be routed to the remote secure gateway.

Use this command to configure an IPsec policy between a local subnet and a remote subnet.

Syntax

config ipsec policy *<name>* **gateway** *<hostname|ip address>* **local** *<ip address>* **remote** *<ip address>* **prop** *<proposal>*

Parameters

name	Enter a name for this VPN.
gateway *hostname|ip address*	Enter a Host name or fixed IP address of the remote secure gateway.
local *ip address*	Enter a local IP address secured by the VPN. Valid values include **any** or addresses specified as a range or as a subnet.
remote *ip address*	Enter a remote IP address secured by the VPN. Valid values include **any** or addresses specified as a range or as a subnet.
prop *proposal*	Enter the name of the IPsec proposal. The default value is **vpn-a**.

Example

The following command configures a policy that secures all traffic between the BSGX4e and the gateway 172.28.16.20.

```
> config ipsec policy alltraffic gateway 172.28.16.20 local
any remote any prop VPN-A
```

Related commands

```
del ipsec policy
display ipsec policy
show ipsec policy
clear protocol esp
show protocol esp
```

```
clear ipsec sa
show ipsec sa
```

ipsec proposal

An IPsec proposal is a set of security parameters used when negotiating an IPsec SA with a remote secure gateway. IPsec proposals are used by the IPsec policies that reference them.

The initial BSGX4e configuration provides a predefined IPsec proposal named VPN-A. This predefined IPsec proposal conforms with the recommendations for a standard IPsec cryptographic suite called VPN-A, as described in RFC 4308.

Syntax

config ipsec proposal *<name>* **encrypt** [3DES|AES|AES128|AES192|AES256] **auth** [md5|sha]

Parameters

name	Enter a name for this proposal.
encrypt 3DES|AES|AES128|AES192|AES256	Enter an encryption algorithm. The AES algorithm can be requested with a specific key size (128, 192, or 256 bits) or, if you specify the AES option, IPsec uses the smallest key size supported by both peers. The default is 3DES.
auth md5|sha	Specify an authentication method.

Example

```
> config ipsec proposal prop1 encrypt 3DES auth sha
```

Related commands

```
display ipsec proposal
show ipsec proposal
clear ipsec sa
show ipsec sa
clear protocol esp
show protocol esp
```

Local call routing commands

Local call routing (LCR) mode describes the telephone service that the BSGX4e can provide without the use of a VoIP call server on the WAN. Local call routing is automatically used when VoIP service is interrupted and LAN endpoints cannot receive or place calls using a call server on the WAN.

In LCR mode, LAN VoIP phones can place and receive local calls, that is, calls that do not go out to the WAN. Local calls (between LAN endpoints) are established through the BSGX4e (acting as a VoIP server). In LCR mode, only basic telephone services are supported.

Calls identified as external calls are routed to the PSTN through the FXO interface of the BSGX4e, or through a SIP/PSTN gateway located in the LAN.

When VoIP call service resumes, external calls are automatically received and placed as before.

Use the following commands to configure LCR:

- lcr accounts
- lcr settings

lcr accounts

When the BSGX4e acts as the VoIP server to perform local call routing, it needs to know the telephone numbers of the local endpoints. An LCR account informs the BSGX4e of the telephone number of a local endpoint when the user ID or endpoint ID does not provide that information. For example, when a SIP account is defined by a name string, the LCR account defines the telephone number of that account. Use this command to configure LCR accounts.

Syntax

config lcr accounts <*dn*> **type** [sip|mgcp] **id** <*id*>

Parameters

dn	Enter the x-digit local office phone number.
type sip|mgcp	Enter the signaling protocol used by the endpoint.
id *id*	Enter the ID of the SIP or MGCP endpoint.

Example

```
> config lcr accounts 5555 type SIP id u4ea.five
```

Related commands

```
del lcr accounts
display lcr accounts
show lcr accounts
show lcr settings
```

lcr settings

Use this command to configure local call routing settings, including if a gateway is used for external calls, the emergency call number, and the numbering plan settings that allow the BSGX4e to determine if the call is local or external.

Syntax

config lcr settings lcbmode [int|lgw] **ecpolice** *<value>* **ecfire** *<value>* **ecambulance** *<value>* **ecmisc** *<value>* **obaccess** *<value>* **areacode** *<value>* **coprefix** *<value>* **enlength <value> ectofxo** [yes|no]

NOTE: For this release, the parameters **ecpolice, ecfire, ecambulance**, and **ecmisc** are automatically set by the country code configured using system info on page 160

Parameters

lcbmode int|lgw	Enter the local call backup mode (**int** for the Integrated Gateway or **lgw** for a SIP/PSTN gateway on the LAN). Only one gateway can be configured. The default is **int.**
ecpolice *value*	Enter the emergency call number of the police station. The default is 911.
ecfire *value*	Enter the emergency call number of the fire station. The default is 911.
ecambulance *value*	Enter the emergency call number of the ambulance service. The default is 911.
ecmisc *value*	Enter another emergency call number. The default is 911.
obaccess *value*	Enter the outbound access prefix digit (such as 9 to place an outside call, as in 9-555-1212). Applies only to hosted PBX service. The default is **9**.
areacode *value*	Enter a valid area code, for example, enter 408 for the phone number 408-555-5555.
coprefix *value*	Enter a valid Central Office prefix, for example, enter 555 for the phone number 408-555-5555.
enlength *value*	Enlength is the length of the extensions used to place local calls (not the full phone number). For example the extension of the full phone number 408-555-1234 is 1234 if this parameter is 4. It is 234 if this parameter is 3. The default is 4 digits.
ectofxo yes|no	Specify to force the emergency call (ecnumber) to be routed through the FXO port or gateway in normal mode, for example not in survival mode. The default is **yes**.

Example

Use this command to allow an emergency call for the police station (911) to be routed through the FXO port in a scenario where the BSGX4e is behind a PBX and needs a 9 to dial out.

```
> config lcr settings lcbmode int ecpolice 911 coprefix 9
```

Related commands

```
display lcr settings
show lcr settings
show lcr accounts
show lcr connections
```

Logging commands

The BSGX4e supports both local module logging and remote module logging (udplog and syslog). Local module logging writes entries to an internal buffer. Use the following commands to configure logging:

- logging dest
- logging map
- logging modules

logging dest

If the destination map for a message type is external, a server must be configured. The server destinations are:

- UDP: Messages are sent in raw UDP format to a UDP server.
- syslog: Messages are sent in Syslog format to a Syslog server.

Use this command to configure logging destinations.

Syntax

```
config logging dest udpip <ip address> udpport <port> sysip
<ip address> sysport <port> facility
[local0|local1|local2|local3|local4|local5 |local6|local7]
```

Parameters

udpip *ip address*	Enter the IP address of a standard UDP receiver.
udpport *port*	Enter the port of the receiving UDP logger.
sysip *ip address*	Enter the IP address of a receiving syslog daemon.
sysport *port*	Enter the port of a receiving syslog daemon.
facility local1-7	Enter the syslog facility to use in the form of **localn,** where *n* is **0-7.**

Example

```
> config logging dest udpip 192.168.22.60 udpport 1234
```

Related commands

```
display logging dest
show logging dest
show logging map
```

logging map

Each type of log message is mapped to its own set of destinations. Use this command to configure the logging map.

Note: When the destination is set to file, logs are saved on the compact flash in /cf0usr/log/<date>. They can be read with the command cat. They can be exported using SFTP.

Note: Logging the configuration uses system resources and can cause a difference in system speed.

Syntax

```
config logging map
emerg [all|console+udp+syslog+internal+file|none]
error [all|console+udp+syslog+internal+file|none]
warn [all|console+udp+syslog+internal+file|none]
notice [all|console+udp+syslog+internal+file|none]
inform [all|console+udp+syslog+internal+file|none]
debug [all|console+udp+syslog+internal+file|none]
trace [all|console+udp+syslog+internal+file|none]
```

Parameters

emerg [all|console+udp+syslog+internal+file|none]

Select the destination for critical messages. Select **all** or **none** or a combination of the others.

error [all|console+udp+syslog+internal+file|none]

Select the destination for error messages. Select **all** or **none** or a combination of the others.

warn [all|console+udp+syslog+internal+file|none]

Select the destination for warn messages. Select **all** or **none** or a combination of the others.

notice [all|console+udp+syslog+internal+file|none]

Select the destination for notice messages. Select **all** or **none** or a combination of the others.

inform [all|console+udp+syslog+internal+file|none]

Select the destination for inform messages. Select **all** or **none** or a combination of the others.

debug [all|console+udp+syslog+internal+file|none]

Select the destination for debug messages. Select **all** or **none** or a combination of the others.

trace [all|console+udp+syslog+internal+file|none]

Select the destination for trace messages. Select **all** or **none** or a combination of the others.

Example

```
> config logging map emerg +syslog
```

Related commands

```
display logging map
show logging map
show logging dest
show logging modules
```

logging modules

Specify which message levels can be included or excluded for a system module.

Severity Level	Message Level	Description	Default Destination
0	`emerg`	Emergency operation error	Internal buffer.
1	`alert`	Alert operation error	Internal buffer.
2	`crit`	Critical operation error	Internal buffer.
3	`error`	Low-level operation error	Internal buffer.
4	`warn`	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.

Use this command to configure the logging module.

Syntax

`config logging module` *`<module>`* **`map`** `[all|emergency+alert+critical+error+warning+notice+inform+debug+trace+none]`

Parameters

`module` *`module`*

Specify the name of the system module for which the logging level is specified.

`map` `all|emergency+alert+critical+error+warning+notice+inform+debug+trace+none`

Enter the message levels to be included or excluded. Select **`all`** or **`none`** or a combination of the others.

Example

```
> config logging modules VQM map +debug +trace
```

Related commands

```
show logging modules
show logging dest
show logging map
```

Media setting command

Settings for the Media Bridge (MBR) specify how VoIP media connections are established.

By default, communication streams are established between each party and the BSGX4e that bridges them to establish the end-to-end communications.

The following command configures media connections:

- media settings

media settings

Use this command to set the parameters for VoIP media streams. If the direct media (dm) setting is enabled, communication streams are directly established between parties in a LAN-to-LAN call.

Syntax

config media settings dm [yes|no] **port** *<low#-high#>* **audioqos** *<qg>* **maxconn** *<connections>* **defaultvideobw** *<bps>*

Parameters

dm yes|no	Enable/disable the use of direct media (RTP) connections between two LAN endpoints. The default is **no** (disabled).
port low#-high#	Enter the range of RTP ports to use. The RTP range must contain at least 1000 values and must not overlap ports configured for existing services in the device. Normally, two ports in the range are used for each media connection, one for RTP and the other for RTCP. The default is **13000-14999.**
audioqos *qg*	Quality group used to ensure voice quality. VoIP media streams are sensitive to packet delay and packet loss; if packets are dropped or delayed, voice quality deteriorates. The quality group must be configured before it can be specified here. See QoS (GoS) commands on page 89.
maxconn *connections*	Maximum number of VoIP connections (for both SIP and MGCP) allowed.
defaultvideobw *bps*	Set the default bandwidth the Call Admission Control has to reserve for a given session when the video application uses a codec that is not recognized by the BSGX4e. The default is **640000** bps.

Example

```
> config media settings dm yes rtp 10000-11999 audioqos
VoIPMedia
```

Related commands

```
display media settings
show media settings
stats media status
show qos group
```

Media gateway controller protocol commands

The Media Gateway Control Protocol (MGCP) session controller controls the establishment and termination of VoIP sessions, as requested by endpoint devices. The MGCP gateway, which operates together with the session controller, serves as the VoIP gateway for analog devices.

The BSGX4e controls VoIP sessions for its LAN devices, which can be MGCP phones and PC terminals. It also controls VoIP sessions for analog devices (fax machines or phones) connected to its FXS port. To do so, it requires access through the WAN to one or more MGCP server.

Use the following commands to configure MGCP:

- mgcp sc settings
- mgcp server settings
- mgcp ua port
- mgcp ua settings

mgcp sc settings

All VoIP traffic is directed through the session controller, allowing it to isolate and control all VoIP devices on the internal network (LAN). Use this command to configure the session controller settings.

Syntax

config mgcp sc settings server *<name>* **wanrxport** *<number>* **lanrxport** *<number>* **keepalive** *<seconds>* **eptimeout** *<seconds>* **maxcalls** *<number>* **sigqos** *<name>*

Parameters

name	Enter the name of the MGCP call server profile. To see the configured server profiles, enter **show mgcp server settings**.
wanrxport *number*	Enter the port on which to listen for MGCP signaling messages from the WAN. The default is **2427**.
lanrxport *number*	Enter the port on which to listen for MGCP signaling messages from the LAN. The default is **2427**.
keepalive *seconds*	Interval between keep-alive messages sent to the MGCP server. Specify zero (0) to disable the sending of keep-alive messages. The default is **0**.
eptimeout *seconds*	Endpoint timeout interval. The default is 3600 seconds (one hour).
maxcalls *number*	The maximum number of calls for the BSGX4e is 250.
siqqos *name*	Enter the name of the GoS quality group that specifies the QoS protection for MGCP signaling traffic. To see the configured quality groups, enter **show qos group**.

Example

```
> config mgcp sc settings server Sylantro wanrxport 2427
lanrxport 2427 sigqos VoIP
```

Related commands

```
display mgcp sc settings
show mgcp sc setting
show mgcp sc endpoints
clear mgcp sc calls
show mgcp sc calls
stats mgcp sc calls
clear mgcp sc status
show mgcp sc status
stats mgcp sc status
show qos group
```

mgcp server settings

The following command configures a MGCP server profile. Up to 3 servers can be configured to implement a fail-over mode. If one is unreachable, the other ones are tried.

Syntax

config mgcp server setting *<name>* **mgc1** [fqdn|*<ip address>*] **port1** *<number>* **mgc2** [fqdn|*<ip address>*] **port2** <number> **mgc3** [fqdn|*<ip address>*] **port3** *<number>* **retries** *<number>* **blacklist** *<seconds>*

Parameters

setting *name*	Enter the name of the server profile.
mgc1 fqdn|*ip address*	Enter a fully qualified domain name or IP address of the first media gateway controller.
port1 *number*	Enter the port number for mgc1. The default is 2727.
mgc2 fqdn|*ip address*	Enter a fully qualified domain name or IP address of the second media gateway controller.
port2 *number*	Enter the port number for mgc2. The default is 2727.
mgc3 fqdn|*ip address*	Enter a fully qualified domain name or IP address of the third media gateway controller.
port3 *number*	Enter the port number for mgc3. The default is 2727.
retries *number*	Enter the number of retries before a MGCP call agent is blacklisted. The default is **5** retries. (Specifying **0** disables call server failover.)
blacklist *seconds*	Enter a blacklist timer. The default is **600** seconds (10 minutes).

Example

```
> config mgcp server settings Sylantro mgc1 206.229.26.51
port1 2727
```

Related commands

```
del mgcp server settings
display mgcp server settings
show mgcp server settings
stats mgcp server settings
show mgcp server status
```

mgcp ua port

Syntax

Use this command to configure the MGCP user agent port on a BSGX4e.

config mgcp ua port *<number>* **name** *<name>* **userid** *<id>* **codec1** [PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20| NOTUSED] **codec2** [PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20| NOTUSED] **codec3** [PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20| NOTUSED] **codec4** [PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20| NOTUSED] **rfc2833** [yes|no] **payload** *<type>* **mpt** [on|off] **fax** [on|auto|off] **vad** [yes|no] **up** [yes|no]

Parameters

port *number* — Enter the port number 1.

name *name* — Enter the name for the display.

userid *id* — Enter the User ID of the MGCP account.

codec1 PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20|NOTUSED

Enter the most preferred codec and packet time. The default is **PCMU_20**.

codec2 PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20|NOTUSED

Enter the most preferred codec and packet time. The default is **PCMA_20**.

codec3 PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20|NOTUSED

Enter the most preferred codec and packet time. The default is **G729A_20**.

codec4 PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20|NOTUSED

Enter the most preferred codec and packet time. The default is **notused**.

rfc2833 off|on — Enable/disable RFC 2833 for DTMF. RFC2833 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. The default is **yes**.

payload *type* — If **RFC2833** is enabled, the RTP dynamic payload type can be specified (96-127). The default is **101**.

mpt off|on — Enable/disable modem pass-through and force media to G.711 echo cancellation. Specify **on** (enabled) if a modem is connected to the BSGX4e. The default is **off**.

fax off|CC_ON	Enable/disable fax pass-through and either force media to G.711 echo cancellation (CC_ON). The default is **off**.
vad yes|no	Enable/disable voice activity detection (silence suppression). Enabling VAD allows the BSGX4e to avoid sending RTP packets, conserving resources. VAD can silence very low sounds, lowering voice quality.
up yes|no	Enable/disable the MGCP gateway port. The default is **yes** (enabled).

Example

```
> config mgcp ua port 1 name uap1 userid uap1 rfc2833 yes
payload 96
```

Related commands

```
del mgcp ua port
display mgcp ua port
show mgcp ua port
show mgcp ua status
show mgcp ua settings
```

mgcp ua settings

The MGCP protocol can be modified for interoperability purposes within the MGCP environment on a BSGX4e. Use this command to configure the MGCP user agent settings.

Syntax

config mgcp ua settings domainformat [macaddr] **maxretxnum** *<number>*

Parameters

domainformat macaddr

Enter the domain type used for MGCP endpoint identification userid@domain. Only MAC addresses are supported. For example, macaddr is supported because it is a MAC address.

maxretnum *number*

Enter the maximum number of successive re-transmissions when a request does not get an answer. The default is 5 re-transmissions.

Example

```
> config mgcp ua settings domainformat macaddr maxretxcount 5
```

Related commands

```
display mgcp ua settings
show mgcp ua settings
```

Netflow commands

The BSGX4e implements a Netflow exporter. It monitors incoming traffic and reports it to the Netflow collector. Netflow versions 1, 5, and 9 are supported.

The Netflow exporter must be deployed together with a Netflow collector. The exporter and collector must implement the same Netflow version.

To classify traffic into the flow to be monitored, the Netflow exporter applies filters to the traffic received on the interfaces. The filters can apply to:

- Port (source or destination)
- IP address (source or destination)
- IP ToS tag value
- IP protocol
- Ethernet protocol
- MAC address (source or destination)
- Interface

When more than one filter is specified, a logical AND is applied.

For the monitored traffic flow, the Netflow exporter reports the following information to the Netflow collector:

- Source IP address (IPV4_SRC_ADDR)
- Destination IP address (IPV4_DST_ADDR)
- Protocol (PROTOCOL)
- Source port (L4_SRC_PORT)
- Destination port (L4_DST_PORT)
- Number of packets received (IN_PKTS)
- Number of bytes received (IN_BYTES)
- Time since flow creation (FIRST_SWITCHED)
- Time since last update (LAST_SWITCHED)

Use the following commands to configure Netflow:

- netflow agent
- netflow filter

netflow agent

Use this command to configure the Netflow agent. Netflow is a Cisco-developed system for monitoring network IP traffic from devices that are enabled with the Netflow protocol. This feature is disabled by default. Note that Pmon performs a similar function for all traffic. See PMON commands on page 81 for more information. The BSGX4e uses Netflow on incoming traffic only. The systems consists of an exporter and a collector. The exporter runs on the BSGX4e while the collector is an external server than can be on the WAN or LAN. The BSGX4e supports Netflow versions 1, 5, and 9. Version 9 outputs a template-based flow record that provides extensibility and is the basis for developing the IETF standard.

Note: The exporter and the collector must be running the same version.

Syntax

config netflow agent enabled [yes|no] **ip** *<ip address>* **port** *<number>* **version** [1|5|9] **interval** *<seconds>* **v9template** *<packets>*

Parameters

enabled yes|no	Enable/disable the Netflow exporter.
ip *ip address*	Enter the IP address of the Netflow collector.
port number	Enter the port number of the Netflow collector. The default is 2055.
version 1|5|9	Enter the Netflow version. The default is 9.
interval *seconds*	Enter the interval for which Netflow exports statistics. The default is 10 seconds.
v9template *packets*	Enter the number of Netflow packets sent before a version 9 template is sent. The default is 10 packets sent before a template is sent.

Example

```
> config netflow agent enabled yes ip 192.168.134.167 port
3000 version 9
```

Related commands

```
clear netflow agent
display netflow agent
show netflow agent
stats netflow agent
show netflow filter
```

netflow filter

Use this command to configure the Netflow filter. By default, all traffic is monitored with a default setting of any for all fields.

Syntax

config netflow filter sourceport *<port>* **destport** *<port>* **scrip** *<ip address>* **dstip** *<ip address>* **tos** *<value>* **ipproto** [any|udp|tcp|icmp|esp|gre] **ethproto** [ip|arp|rarp] **srcmac** *<mac address>* **dstmac** *<mac address>* **interface** *<if>*

Parameters

sourceport *port*	Enter the source port to monitor.
destport *port*	Enter the destination port to monitor.
srcip *ip address*	Enter the source IP address to monitor.
dstip *ip address*	Enter the destination IP address to monitor.
tos *value*	Enter the ToS tag value to monitor.
ipproto any|udp|tcp|icmp|esp|gre	Enter the IP protocol to monitor.
ethproto ip|arp|rarp|any	Enter the Ethernet protocol to monitor.
srcmac *mac address*	Enter the source MAC address to monitor.
dstmac *mac address*	Enter the destination MAC address to monitor.
interface *if*	Enter the interface to monitor.

Example

```
> config netflow filter srcip 10.0.1.100 tos 248
```

Related commands

```
display netflow filter
show netflow filter
show netflow agent
```

PMON commands

This section describes how to configure the protocol monitoring (PMON) tool. The PMON tool monitors traffic coming into the BSGX4e. PMON can record one or more traces of the incoming traffic. Only incoming traffic is monitored. The following statistics are reported by each trace:

- Number of packets (received)
- Number of bytes (received)
- Packet rate
- Bit rate

PMON creates traces by applying filters to the traffic received on the interfaces. When more than one filter is specified, a logical AND is applied. The filters can apply to:

- Port (source or destination)
- IP address (source or destination)
- IP ToS tag value
- VLAN ID
- IP protocol
- MAC address (source or destination)
- Interface

Use the following commands to configure PMON:

- pmon agent
- pmon trace

pmon agent

This command enables and disables protocol monitoring.

Syntax

config pmon agent enabled [yes|no]

Parameters

enabled yes|no	Enable and disable protocol monitoring. The default is **no**.

Example

```
> config pmon agent enabled yes
```

Related commands

```
del pmon agent
show pmon agent
display pmon trace
show pmon trace
```

pmon trace

Use this command to configure monitor traces. All protocol monitoring traces are synchronized. This allows easy comparison of the traffic types received over a given period of time.

Syntax

config pmon trace *<tracename>* **sourceport** [port] **destport** [port] **srcip** *<ip address>* **dstip** *<ip address>* **tos** *<value>* **vlanid** *<value>* **ipproto** [any|udp|tcp|icmp|esp|gre] **srcmac** *<mac address>* **dstmac** *<mac address>* **interface** *<if>*

Parameters

tracename *tracename*	Enter the name of the trace to add or change.
sourceport *port*	Enter the source port to monitor.
destport *port*	Enter the destination port to monitor.
srcip *ip address*	Enter the source IP address to monitor.
dstip *ip address*	Enter the destination IP address to monitor.
tos *value*	Enter the ToS tag value to monitor.
vlanid *value*	Enter the VLAN ID value to monitor.
ipproto any|udp|tcp|icmp|esp|gre	Enter the IP protocol to monitor.
srcmac *mac address*	Enter the source MAC address to monitor.
dstmac *mac address*	Enter the destination MAC address to monitor.
interface *if*	Enter the interface to monitor.

Example

```
> config pmon trace VoIP srcip 10.0.1.100 tos 248
```

Related commands

```
clear pmon trace
display pmon trace
del pmon trace
show pmon trace
stats pmon trace
```

Protocol commands

This section describes how to configure ARP and PPP protocols to be protected by QoS:

- protocol arp
- protocol ppp

protocol arp

Address Resolution Protocol (ARP) is a network layer protocol that automatically maps IP addresses to hardware Media Access Control (MAC) addresses. When a network node sends data to an IP address on its segment, it broadcasts an ARP request to resolve the IP address to an Ethernet MAC address.

ARP protocol must be protected to be able to forward traffic, especially the high priority flows including VoIP flows. Protecting ARP ensures ARP resolutions to succeed so the critical flows are correctly forwarded.

When QoS is turned on, always protect ARP. See arp table.

Syntax

config protocol arp qq *<class>*

Parameters

qq *class*	Enter the quality group class.

Example

The following command creates the quality group arp_protect then assigns it.

```
> config qos group arp_protect qg A3 type policed committed
100000
> config protocol arp qg arp_protect
```

Related commands

```
display protocol arp
show protocol arp
show arp table
```

protocol ppp

Use this command to configure PPP control traffic to be protected by QoS.

Protecting PPP control protocol ensures the PPPoE interface goes up and is maintained up over time. Not protecting PPP control protocol can lead to the PPPoE interface going down in case of congestion.

When GoS is configured for a PPPoE interface, always protect PPP control protocol. PPP control protocol concerns the LCP phase, NCP phase and PPP keep-alive. LCP and NCP (see RFC 1661) are to negotiate and bring up a PPP link. PPP keep-alive are PPP control packets periodically exchanged to control if the link is still UP.

Syntax

config protocol ppp qq *<class>*

Parameters

qg *class*	Enter the quality group class.

Example

The following command creates the quality group ppp_protect then assigns it.

```
> config qos group ppp_protect qg A3 type policed committed
100000
> config protocol ppp qg ppp_protect
```

Related commands

```
display protocol ppp
show protocol ppp
show interface ppp
```

Proxy ARP commands

Proxy ARP is used in the BSGX4e to connect hosts that belong to different subnets transparently, that is, without those hosts having to know that the communication is across different subnets, eliminating the need to configure default gateways, routes, and so on, on those hosts.

This section describes how to configure Proxy Arp:

- proxy arp

proxy arp

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. When a host on a network accessible to the WAN port of the BSGX4e sends an ARP request through the BSGX4e to a host on its LAN switch, it responds to the request by supplying its own MAC address (the MAC of the WAN port). The sending host caches the MAC address of the BSGX4e. A similar process occurs in the reverse direction. When a host on BSGX4e LAN sends an ARP request to a host on a remote network, BSGX4e responds with the BSGX4e LAN MAC address. All subsequent traffic between the hosts, sent as normal (as if on the same subnet), are then be routed by the BSGX4e.

Proxy ARP has the following characteristics:

- It is applicable to both LAN and WAN interfaces. It can be enabled and disabled on interfaces that use ARP: Ethernet and VLANs
- The proxy is configured for a specific IP address
- The unit must have static IP addresses on all affected interfaces, for example DHCP must be disabled
- It automatically creates dynamic ARP route table entries and firewall security policies as needed. Deleting or disabling a proxy ARP removes the corresponding route and security policy
- Proxy ARP can configure a maximum of 32 proxies

Syntax

config proxy arp [new|<*id*>] **from** [eth0|eth1] **to** [eth0|eth1] **ip** <*ip address*> **enable** [yes|no]

Parameters

id	Enter new for a new proxy or an exiting ID for reconfiguring.
from eth0|eth1	Enter the interface from which proxied traffic is routed.
to eth0|eth1	Enter the interface to which proxied traffic is to be routed.
ip *ip address*	Enter the destination address for which this proxy is being created.
enable yes|no	Enable/disable proxy ARP.

Example

```
> config proxy arp new from eth0 to eth1 ip 192.168.1.0/24
enable yes
```

Related commands

```
del proxy arp
display proxy arp
show proxy arp
show arp table
```

QoS (GoS) commands

Attention:

Downstream QoS is not yet supported.

This section describes how to configure the following Guarantee of Service (GoS) commands:

- qos downstream link
- qos group
- qos link

qos downstream link

Downstream QoS manages WAN link bandwidth to provide quality protection for specified incoming data streams. This is intended primarily to ensure adequate bandwidth for incoming VoIP streams.

It designates an (upstream) QoS quality group to protect the corresponding downstream traffic. The bandwidth and prioritizing functions that the quality group provides does not, however, apply to Downstream QoS. Rather, Downstream QoS implements a dedicated mechanism to protect the high priority traffic by rate limiting the low priority TCP based traffic. See qos group on page 91 for more information on QoS group configurations.

Note: Do not add protect TCP traffic using downstream QoS.

Syntax

config qos downstream link linerate *<rate>* **encapsulation** [ethernet|vlan|pppoe|pppoa_vcmux|pppoa_llc|pppohdlc|fr]

Parameters

linerate *rate* Enter the WAN interface line rate.

encapsulation ethernet|vlan|pppoe|pppoa_vcmux|pppoa_llc

Enter the type of WAN interface. The rate associated corresponds to the WAN access technology. The service provider includes bandwidth with the overhead of the WAN access technology used. For example, a 2 Mbps PPP over ATM VCMUX, the 2 Mbps normally includes ATM VCMUX + PPP overheads. With a 2 Mbps PPP over Ethernet, the 2 Mbps normally includes the Ethernet + PPP overheads. Because the overheads are not the same for ATM VCMUX and Ethernet, the 2 Mbps of ATM VCMUX + PPP are not the same as the 2 Mbps of Ethernet + PPP.

Example

```
> conf qos downstream linerate 2000000 encapsulation Ethernet
```

Related commands

```
show qos group
display qos downstream link
show qos downstream link
show qos downstream status
stats qos downstream
clear qos downstream
```

qos group

Use this command to configure a quality group. A quality group is the definition of a Guarantee of Service (GoS) treatment, including bandwidth, policing, and GoS class.

Note:

- The GoS link must be configured before the quality groups that reference that link.
- Ten percent of link capacity is always reserved for Best Effort traffic. Thus, no more than 90% of the link rate can be explicitly committed to other quality groups. In other words the sum of the committed rates for all other quality groups must not be greater than 90% of the link rate.

Consider the following when configuring GoS quality groups:

- When a quality group specifies committed access rate (CAR) policing, traffic can be downgraded and discarded, as follows:
  - Traffic received below the committed rate is entirely protected.
  - Traffic received between the committed rate and the burst rate is downgraded; it becomes best effort (BE) traffic. Traffic assigned to BE is forwarded only if bandwidth is available. If bandwidth is not available, the traffic is discarded; thus, the forwarding of downgraded traffic is not guaranteed.
  - Traffic received above the burst rate is discarded (traffic is out of contract).

When a quality group specifies strict policing (POLICED), traffic is managed as follows:

  - Traffic received below the committed rate is entirely protected.
  - Traffic received above the committed rate is discarded (traffic is out of contract).

- Traffic can be discarded even when the average theoretical throughput of the flow is within contract. This can happen when the traffic source is bursting and packets are being deterministically dropped.
- Packet loss is typically due to peak traffic; however, it can also occur if an incorrect load estimate was made.

  For example, suppose up to fifteen VoIP calls can be set up simultaneously, but the quality group to protect VoIP traffic is sized to protect only ten calls. Calls are then dropped because of configuration error, not because of extraordinarily high traffic. So, to avoid dropped calls, sufficient bandwidth must be protected by the quality group to accommodate the total number of possible calls.

When a GoS link is created, a default quality group assigned to BE (Best Effort) is automatically created. This default quality group does not prioritize traffic, and it is not shown when you enter **`show quality group`**. However, this BE quality group exists to serve as default traffic manager for the traffic flows which are not assigned to any other quality group.

You can configure a quality group explicitly defined as best effort (BE). The defined BE quality group replaces the hidden, default BE group. Unlike the default BE group, a defined BE quality group does appear in the quality group list.

Downstream QoS functions differently than the upstream QoS described in the preceding sections. Downstream QoS controls the WAN link by dynamically limiting the bandwidth available to TCP (non-quality) traffic when quality traffic such as VoIP (using UDP) is present. By limiting bandwidth for non-quality traffic, which is mostly Web pages and email, quality traffic experiences only minimal packet loss and delay.

Syntax

config qos group *<name>* **link** [eth0|eth1] **qg** [A1|A2|A3|B1|B2|B3|C1|C2|C3|BE] **type** [car|policed|bestefford] **committed** *<rate>* **burst** *<rate>* **iptos** [*<value>*|no] **cos** [*<value>*|no] **downstreamgos** [yes|no]

Parameters

name

The name of the quality group to be created or edited. Assign the QoS group video to protect video traffic. Assign the QoS group appqos to protect multimedia traffic other than audio and video.

link eth0|eth1

Enter the interface to which this link applies.

qg A1|A2|A3|B1|B2|B3|C1|C2|C3|BE

Enter the GoS class. Up to 10 quality groups can be assigned to the same GoS class. The default is **A1**.

type car|policed|besteffort

Enter a quality group type. The default is **policed**.

committed *rate*

Enter the committed rate for the quality group (in bps). Specify a value if **qg** is *not* **BE**. The minimum rate is 64000. The maximum rate is 90 percent of the total link rate (as specified in qos link on page 94).

burst *rate*

Enter the burst rate for the quality group (in bps). Specify a value if **qg** is **CAR**. The burst rate must be greater than the committed rate and less than or equal to the maximum link rate (as specified in qos link on page 94).

iptos *value*|no

Enter an IP ToS value to be written into each packet assigned to this quality group (decimal, **0-255**). Specify **no** 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.

cos *value*|no	Enter a CoS value to be written into each packet assigned to this quality group (decimal, **0–7**). Specify **no** 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).
downstreamgos yes|no	Enable/disable downstream QoS for this group. This feature reserves incoming bandwidth for non-TCP traffic (such as VoIP).

Example

This example configures a quality group for handling high-priority VoIP traffic.

```
> config qos group VoIP link eth0 qg A1 type policed committed
500000
```

Example

This example sets a downstream QoS group.

```
> conf qos group gold link eth0 qg A1 committed 100000
DownstreamQoS yes
```

Related commands

```
del qos group
display qos group
show qos group
clear qos link
stats qos link
clear qos counters
stats qos counters
display qos downstream link
show qos downstream link
clear qos downstream
show qos downstream
stats qos group
```

qos link

Use this command to configure a GoS link. A GoS link specifies the outgoing interface whose traffic is to be managed and the size of the bandwidth to be managed, that is, the maximum speed of that link.

The GoS link is configured on the physical WAN interface, eth0 on the BSGX4e. It cannot be configured on a virtual interface (vif, vpn or ppp).

Syntax

config qos link [eth0] **max** <bps> **comment** <"comment">

Parameters

if eth0	Enter the interface to which this link applies.
max *<bps>*	Enter the maximum speed of the link in bps. For an Ethernet interface, eth0, the full Ethernet overhead is 38 bytes per packet (14 of Ethernet header, 4 of Ethernet FCS, 8 of Ethernet Preambule and 12 of Ethernet Inter Frame Gap). For example, a stream of 64-byte IP packets is calculated for 102-byte packets by QoS. The maximum speed for an Ethernet output interface is 100,000,000 bps.
comment "comment"	Enter an optional comment describing this link.

Example

```
> config qos link eth0 max 1500000 comment "Office link"
```

Related commands

```
clear qos link
del qos link
display qos link
show qos link
stats qos link
show qos group
```

Radius commands

This section describes how to configure the RADIUS authentication when you log into BSGX4e 2.1.1:

- radius client

radius client

External authentication of passwords can be configured, providing additional security for user log ins to the BSGX4e. When a password is externally authenticated, the radius client in the BSGX4e sends the log in password to an external server for authentication.

When external authentication is used for a user account, the external server defines the password required for log in using the account. The **password** command can change the internal password stored for the account, but the internal password is not used for authentication, thus the effective password is not changed.

The RADIUS client is compatible with standard RADIUS servers. The client maps RADIUS authentication records to users by their user account name. Up to twenty RADIUS authentication records are supported.

Note: Disabling its authentication record suspends RADIUS authentication for a user account. This prevents log ins by the user account until either its authentication record is re-enabled or its authentication method (**auth** value) is changed.

After a user account is configured to use RADIUS authentication, a RADIUS authentication record must be configured for that user account. Every user account that uses RADIUS password authentication must have *its own* RADIUS authentication record.

Note: The user account must be configured before the corresponding RADIUS authentication record is configured. See user accounts on page 169 for details on user accounts. Deleting the user account also deletes its authentication record.

The following command configures the RADIUS authentication record.

Syntax

```
config radius client <name> enabled [yes|no] auto
[yes|no] authserver <ip address|fqdn> secret <string>
binadaddr <ip address> interface [eth0|eth1|none]
```

Parameters

user *name*	Enter the name of the user account to which the authentication record applies. The user account must specify `radius` authentication.
enabled `yes|no`	Enable/disable the RADIUS client for the user. The default is **no.**
auto `yes|no`	Automatically bind the client to the interface specified by the interface parameter if DHCP is in use. Specify **yes** if DHCP is in use. The default is **no.**
authserver *ip address|fqdn*	Enter a FQDN or IP address of the RADIUS authorization server that the client references.
secret *string*	Enter a shared secret for the client as determined by the server.
bindaddr *ip address*	

Enter the binding IP address for the client. It is the IP address of the interface that the server references (typically, the IP address of the WAN interface.) Specify this value only if DHCP is *not* in use.

interface eth0|eth1|none

Select the physical interface through which RADIUS communicates if the **auto** parameter is **yes**. This is typically the WAN interface. To clear the parameter, specify **none**.

Example

```
> config radius client RadiusUser
Entering interactive mode: ctrl^z | 'exit', ctrl^c | 'quit'
                           TAB to cycle parameter options
radius-cl-Radi#> enabled yes
radius-cl-Radi#> auto yes
radius-cl-Radi#> authserver radius.wan.com
radius-cl-Radi#> secret Radsecret
radius-cl-Radi#> interface eth0
radius-cl-Radi#> exit
```

Related commands

```
del radius client
display radius client
show radius client
show user accounts
```

Relay commands

This section describes how to configure the following relay commands:

- relay dhcp settings
- relay dns settings
- relay sntp settings
- relay tftp cache
- relay tftp files
- relay tftp settings

relay dhcp settings

The DHCP relay function relays DHCP messages between clients located on the LAN and a single server located on the WAN. From the viewpoint of the clients on the LAN, the BSGX4e appears to be the server. From the viewpoint of the server on the WAN, the BSGX4e appears to be the client.

Before enabling DHCP relay, the following tasks must be performed:

- Disable the DHCP server on the LAN interface. See dhcps pool on page 35.
- Disable NAT on the WAN interface. See security nat interface on page 113.
- Create a security policy allowing the traffic from the DHCP server to the DHCP relay agent. See security policy on page 116.

Note: DHCP relay can not be enabled while the DHCP server is running.

Use this command to configure DHCP relay.

Syntax

config relay dhcp settings enabled [yes|no] **server** *<ip address>*

Parameters

enabled yes|no	Enable/disable DHCP relay. The default is **no** (disabled).
server *ip address*	Enter the IP address of the DHCP server on the WAN to which the LAN DHCP messages are relayed. The DHCP server can only be configured with an address on the interface subnet.

Example

```
> config security nat interface eth0 status off

> config security policy from eth0 to self sip 192.168.134.200
sport 67 dport 67 proto udp action allow

> config relay dhcp settings enabled yes server
192.168.134.200
```

Related commands

```
display relay dhcp settings
show relay dhcp settings
```

relay dns settings

The DNS relay function relays DNS messages between clients located on LAN and a DNS server located on the WAN. The DNS relay function sets up the BSGX4e as a proxy for clients on the LAN that must make DNS requests (such as those required for Web browsing and email). From the viewpoint of the clients on the LAN, the BSGX4e appears to be the server. From the viewpoint of the server on the WAN, the BSGX4e appears to be the client.

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

The following table displays DNS relay provisioning.

Table 1 Possible sources for the DNS relay configuration

DNS Relay *source* parameter	DNS Client *source* parameter	Does DHCP or PPP client provide DNS configuration?	Does user provide DNS Client configuration ?	Source of DNS relay configuration
user	any			User-provided for DNS Relay
auto	**dhcp or ppp**	yes		DHCP or PPP
auto	**dhcp or ppp**	no		User-provided for DNS Relay
auto	**user**		yes	User-provided for DNS Client
auto	**user**		no	User-provided for DNS Relay
auto	**auto**	yes		DHCP or PPP
auto	**auto**	no	yes	User-provided for DNS Cli-ent
auto	**auto**	no	no	User-provided for DNS Relay

Use this command to configure DNS relay.

Syntax

`config relay dns settings enabled` `[yes|no]` **`dns1`** *`<ip address>`* **`dns2`** *`<ip address>`* **`source`** `[user|auto]`

Parameters

`enabled` `yes|no`	Enable/disable DNS relay. The default is **no** (disabled).
`dns1` *`ip address`*	Enter the IP address of the primary external DNS server.
`dns2` *`ip address`*	Enter the IP address of an optional second external DNS server.

source user|auto	Enter the source of the DNS relay configuration. The default is **auto**. For **user**, use the latest user-provided configuration, that is, the DNS servers last specified by the **dns1** and **dns2** parameters. For **auto**, use the DNS server configuration provided for the DNS client (see system dns on page 156). If the server configuration for the DNS client is null, use the user-provided configuration for the DNS relay (dns1 and dns2). The DNS client configuration is null if it requested its server configuration from DHCP/PPP, but it did not receive one and/or it requested the user-provided configuration, but no DNS servers had been specified.

Example

The following example enables the DNS relay function, specifies the configuration source as user, and specifies one DNS server at IP address 192.168.134.201.

```
> config relay dns settings enabled yes source user dns1
192.168.134.201
```

Example

The following example re-configures the DNS relay function so that it uses the server configuration provided for the DNS client. The relay DNS is initially enabled.

```
> config relay dns settings no enabled
> config relay dns settings source auto
> config relay dns settings enabled
```

Related commands

```
display relay dns settings
show relay dns settings
show relay dns cache
show system dns
```

relay sntp settings

The SNTP relay function relays the SNTP messages between clients located on the LAN and a server located on the WAN. From the viewpoint of the clients on the LAN, the BSGX4e appears to be the server. From the viewpoint of the server on the WAN, the BSGX4e appears to be the client.

Note: Configure devices on the LAN, either through DHCP (option 42) or manually, to use the BSGX4e 2.1.1 as the SNTP server. When the configuration source for the SNTP relay is auto, the SNTP relay attempts to use the configuration provided for the SNTP client, even if the SNTP client is disabled. To see the current server configuration for the SNTP client, enter the command **`show system sntp.`**

The following table displays SNTP relay provisioning.

Table 2 *Possible Sources for the SNTP Relay Configuration*

SNTP Relay *source* parameter	SNTP Client *source* parameter	Does DHCP or PPP client provide SNTP configuration?	Does user provide DNS Client configuration?	Source of SNTP relay configuration
user	any			User-provided for SNTP Relay
auto	**dhcp**	yes		DHCP
auto	**dhcp**	no		User-provided for SNTP Relay
auto	**user**		yes	User-provided for SNTP Client
auto	**user**		no	User-provided for SNTP Relay
auto	**auto**	yes		DHCP
auto	**auto**	no	yes	User-provided for DNS Client
auto	**auto**	no	no	User-provided for DNS Relay

Use this command to configure SNTP relay.

Syntax

`config relay settings enabled` `[yes|no]` **`server`** *`<ip address|fqdn>`* **`source`** `[user|auto]` **`gmt`** *`<+|-offset>`*

Parameters

`enabled` `yes|no` — Enable/disable SNTP relay. The default is **`no`** (disabled).

`server` *`ip address|fqdn`*

Enter the IP address or FQDN of an external SNTP server.

`source` `user|auto` — Enter the source of the SNTP relay configuration. The default is **`auto`**. For **`user`**, use the SNTP server last specified by the server parameter. For **`auto`**, use the SNTP server provided for the SNTP client (see system sntp on page 161). If the server configuration for the SNTP client is null, use the user-provided server for the SNTP relay (the SNTP server last specified by the server parameter). The SNTP

	client configuration is null if it requested its server from DHCP, but it did not receive one and/or it requested the user-provided server, but no SNTP server had been specified.
gmt *+|-offset*	Enter the GMT time zone offset in hours. The default is **0**. Specify this offset only if the client devices cannot provide their offset. If the appropriate offset is supplied by the clients, set this parameter to 0.

Example

The following example enables the SNTP relay function. By default, the configuration source is **auto**; the SNTP relay uses the same SNTP server configuration provided for the SNTP client. Also by default, the **gmt** parameter is set to **0**; the BSGX4e does not provide a time offset to the LAN clients.

```
> config relay sntp settings enabled
```

Example

The following example re-configures the SNTP relay function to use the SNTP server at IP address 192.168.134.160. Relay SNTP is initially enabled.

```
> config relay sntp settings no enabled
> config relay sntp settings source user server
192.168.134.160
> config relay sntp settings enabled
```

Related commands

```
display relay sntp settings
show relay sntp settings
show relay sntp sessions
show system sntp
```

relay tftp cache

The TFTP cache feature allows copies of frequently requested files to be temporarily stored on the BSGX4e in memory. If a file requested by a LAN device is found in the cache, it can be immediately sent to the client. Use this command to configure TFTP cache.

Syntax

config relay tftp cache enabled [on|off] **size** *<MB>* **refresh** *<minutes>* **download** *<method>* **server** [fqdn|*<ip address>*] **user** *<string>* **password** *<string>*

Parameters

enabled on|off	Enable/disable TFTP file caching. The default is off.
size *MB*	Specify the size of the file cache. The valid range is 1-16. The default is **6** MB.
refresh *minutes*	Enter the cache refresh interval. The default is **240** minutes (4 hours).
download *method*	Method for downloading files into the cache: **auto** files are saved to the cache while being downloaded by the TFTP relay function. **tftp** files are downloaded into the cache using an internal TFTP client. **ftp** files are downloaded into the cache using an internal FTP client. The default is **auto.**
server *fqdn|ip address*	Enter the IP address or FQDN of the TFTP or FTP server.
user *string*	Enter the user name if downloading files by FTP.
password *string*	Enter the password if downloading files by FTP.

Example

```
> config relay tftp cache enabled yes size 16 refresh 960
download auto
```

Related commands

```
display relay tftp cache
show relay tftp cache
show relay tftp files
show relay tftp settings
```

relay tftp files

Use this command to configure a file to be stored in the TFTP file cache.

Syntax

config relay tftp files <*index*|new> **name** <*string*>

Parameters

index|new	Specify new or an existing index number.
name *string*	Specify the name of the file to cache.

Example

```
> config relay tftp files 1 name SIPDefault.cnf
```

Related commands

```
del  relay tftp files
display relay tftp files
show relay tftp files
show relay tftp cache
show relay tftp settings
```

relay tftp settings

TFTP relay function relays the TFTP messages between clients located on the LAN and a single server located on the WAN. From the viewpoint of the clients on the LAN, the BSGX4e appears to be the server. From the viewpoint of the server on the WAN, the BSGX4e appears to be the client.

The BSGX4e maintains a cache filled with the successful downloaded files. If a TFTP request is already in the cache, the BSGX4e can reply to the TFTP request without referencing a TFTP server.

Note: Configure devices on the LAN, either through DHCP (option 66, for example) or manually, to use the BSGX4e 2.1.1 as the TFTP server.

Syntax

config relay tftp settings enabled [yes|no] **server** <*ip address|fqdn*> **dhcp** [on|off] **allow** [get|all] **sessions** <*max sessions*>

Parameters

enabled on|off	Enable/disable TFTP relay. The default is **no** (disabled).
server *ip address|fqdn*	Enter an IP address or FQDN of the external TFTP server.
dhcp on|off	Indicate whether the TFTP server address is provided by the DHCP client on the WAN interface of the BSGX4e. The default is **off**.
allow get|all	Indicate **get** to allow the LAN devices to get files only. Indicate **all** to allow the LAN devices to get and put files.
sessions *max sessions*	Enter the maximum number of concurrent TFTP sessions. This ensures that the CPU is not monopolized by TFTP packet relays. The default is **50**.

Example

```
> config relay tftp settings enabled yes server
tftpserver.wan.com
```

Related commands

```
display relay tftp settings
show relay tftp settings
show relay tftp files
show relay tftp cache
```

RIP command

This section describes how to enable dynamic routing using RIP (Routing Information Protocol). The BSGX4e supports RIP versions 1 and 2.

- rip daemon

rip daemon

Use this command to configure the RIP daemon to start then listen for RIP messages on the WAN interface and uses that information to store routes in a table.

For RIP to be effective, all routers in the network must support RIP version 1 or version 2. RIP 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; it does not support RIP on its LAN interface.

Note: Use of a RIP daemon on the WAN interface can be a security risk.

Syntax

```
config rip daemon started [no|yes] version [v1|v2]
```

Parameters

started yes|no	Enable/disable the RIP daemon. The default value is **no**.
version v1|v2	Select the version of the RIP protocol to run (v1 | v2). The default value is v2.

Example

```
> config rip daemon started version v2
```

Related commands

```
display rip daemon
show rip daemon
show route table
```

Route commands

This section describes how to configure BSGX4e static IP routes:

- route table

route table

This command adds a static IP route to the routing table in the BSGX4e. Each route in the table specifies the following:

- The destination. Each packet contains a destination IP address. If the destination address is within the *destination address range* specified for the 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 IP address of the gateway to which packets have to be forwarded to.
- The interface through which the packets have to be forwarded to.

Syntax

config route table *<dest>* **gw** *<ip address>* **if** [none|eth0|eth1]

Parameters

dest	Enter the range of destination IP addresses to which the route applies. To add a default route to the table, specify **default.**
gw *ip address*	Enter the IP address of the gateway. The gateway must be reachable from the BSGX4e.
if none|eth0|eth1	Enter an optional interface for the route. If no interface is specified, the route interface is determined from the gateway address.

Example

This example adds a default route to send traffic to gateway 66.206.164.193.

```
> config route table default gw 66.206.164.193
```

Example

This example adds a route that sends all packets destined for subnetwork 192.168.134.0/24 to gateway 66.206.164.194.

```
> config route table 192.168.134.0/24 gw 66.206.164.194
```

Related commands

```
del route table
display route table
show route table
```

Security commands

This section describes how to configure the BSGX4e security features: Firewall, NAT and ALG. The following security types are available:

- security alg
- security nat policy
- Security NAT public
- security policy

security alg

The Application Layer Gateway (ALG) enables the transfer of FTP, PPTP, and TFTP traffic through the firewall policies and NAT. This is done by creating dynamic holes in the firewall and changing IP addresses in application protocol headers.

FTP 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.

Point-to-Point-Tunneling Protocol (PPTP) is a networking technology that supports multiprotocol virtual private networks (VPN), enabling remote users to access corporate networks securely across the Microsoft Windows operating systems and other point-to-point protocol (PPP)-enabled systems.

Syntax

config security alg ftp [yes|no] **pptp** [yes|no] **tftp** [yes|no]

Parameters

ftp yes|no	Enable/disable ALG for FTP traffic.
pptp yes|no	Enable/disable ALG for PPTP traffic.
tftp yes|no	Enable/disable ALG for TFTP traffic.

Example

```
> config security alg ftp yes
```

Related commands

```
display security alg
show security alg
```

security nat interface

Network Address Translation (NAT) provides security by hiding the internal addresses of the private network from the Internet: addresses and/or ports are translated from private IP addresses to public IP addresses, and vice versa.

The BSGX4e processes both standard and reverse NAT:

- Standard NAT translates the source IP address of the LAN to the public WAN IP address. It also changes the port numbers (for UDP and TCP protocols) or the ICMP identifier. These translations allow several LAN devices to be connected to the WAN through a single public IP address.
- Reverse NAT (redirection) forwards traffic from the public network to a private network. This allows a device in the LAN to be accessed from the Internet (using address forwarding or port forwarding).

Use this command to configure the NAT interface.

Syntax

```
config security nat interface [eth1|eth0] status [on|off]
```

Parameter

interface eth1|eth0	Select the WAN interface to apply NAT on.
status on|off	Enable/disable the interface. The default is **off**.

Enable

```
> config security nat interface eth0 status on
```

Related commands

```
del security nat interface
display security nat interface
show security nat interface
```

security nat policy

When translating addresses, Network Address Translation (NAT) references policies that map addresses and ports. These policies enable static NAT, port forwarding, and address forwarding. Use this command to configure a NAT policy.

Syntax

config security nat policy [new |*<id>*] **type** [static|rport|raddr] **address** *<ip address>* **port** *<number>*

Parameters

id	Enter a policy ID number. Specify new when creating a new policy.
type static|rport|raddr	Enter the type of policy. Specify **rport** for port forwarding or **raddr** for address forwarding, or **static** for static NAT.
address *ip address*	Enter the IP address to be translated (a public address for a static NAT policy; a private address for a redirect NAT policy). A public address must have been specified for a static NAT policy. See Security NAT public on page 115.
port *number*	If policy Type rport was selected, enter the port number for the address that was entered into the Address field. Otherwise, leave blank.

Example

This following example configures the BSGX4e to forward traffic arriving on UDP port 9000 to LAN IP address 10.0.1.130, destination port 2600. This configuration requires a rport policy (port forwarding).

```
> config security nat policy new type rport address 10.0.1.130
port 2600
```

Related commands

```
del security nat policy
display security nat policy
show security nat policy
```

Security NAT public

A public IP address must be configured for static NAT and also for address forwarding. This command adds public IP addresses to NAT. Up to 16 addresses can be configured. NAT addresses can be configured outside the subnet of the WAN.

Syntax

config security nat public *<address>* **interface** *<type>*

Parameters

address	Enter the public IP address. This can be a single IP address or a range of address using the xx.xx.xx.xx—xx.xx.xx.xx format.
interface *type*	Select the interface type. The BSGX4e BG supports eth0 and none. The default is none. Select none if the public address you entered is within the subnet range of the WAN. If you are creating a public address outside of the existing WAN subnet, select the WAN interface to which it applies.

Example

```
> config security nat public 192.168.134.199
```

Related commands

```
del security nat public
display security nat public
show security nat public
```

security policy

This command defines firewall security policies to accept desired incoming traffic. The firewall is closed by default.

Firewall security is based on policies. A policy is created to accept or deny a traffic flow based on the current rule sequence.

Security policies are also used to classify traffic for Network Address Translation (NAT) and for layer 3 Quality of Service (QoS) treatment (Guarantee of Service [GoS]). See security alg on page 112.

Syntax

config security policy [new|*<index>*] **from** [self|eth0|eth1] **to** [self|eth0|eth1] **sip** *<ip address(es)>* **dip** *<ip address(es)>* **sport** *<port(s)>* **dport** *<port(s)>* **proto** [udp|tcp|icmp|esp|gre|any] **nat** *<id>* **qosqg** *<name>* **iptos** *<decimal>* **seq** [begin|end|position] **action** [allow|deny]

Parameters

index	Specify **new** to create a new policy.
from self|eth0|eth1	Specify the interface where the packet originated. Specify **self** for packets originating at the device.
to self|eth0|eth1	Specify where the packet is destined. Specify **self** for packets destined for the device.
sip *ip address(es)*	Enter the source IP address or range of IP addresses.
dip *ip address(es)*	Enter the destination IP address or range of IP addresses.
sport *port(s)*	Enter the source port number or range of port numbers.
dport *port(s)*	Enter the destination port number or range of port numbers.
proto udp|tcp|icmp|esp|gre|any	Enter the protocol specified in the packet.
nat *id*	Enter the ID of the NAT policy to be referenced. See security nat policy on page 114.)
qosqg *name*	Enter the name of a GoS quality group. See qos group on page 91.)
iptos *decimal*	Enter an IP ToS tag value (decimal byte). It has to be used only by GoS policies, that is, only when the qosqg parameter is specified. See qos group on page 91.)
seq begin|end|position	Enter the position of the new policy within the policy sequence. If **Position** is specified, it specifies where the policy is inserted in the sequence. An incoming packet can match more than one security policy. Its treatment

	(acceptance or rejection) is determined by the first policy that the packet matches. Therefore, the sequential order of firewall policies is important.
action *allow|end*	Indicate whether a packet matching the policy is accepted or rejected.

Example

The following example configures a security policy that allows all TCP traffic from the eth1 interface, destined for port 9000, and going out the eth0 interface.

```
> config security policy new from eth1 to eth0 proto tcp dport
9000 action allow
```

Example

The following example makes all traffic originated by the BSGX4e itself (like management traffic) destined to the WAN interface eth0 protected by the QoS group 'management'.

```
> config security policy new from self to eth0 dip
192.168.1.10 qos management
```

Related commands

```
del security policies
display security policies
show security policies
show security nat policies
show qos group
```

Service commands

This section describes how to configure BSGX4e access types. The following services are available:

- service ssh
- service telnet
- service web

service ssh

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

SSH use requires the following:

- The workstation on the WAN or LAN must provide an SSH client, for example PuTTY, and SSH secure shell.
- The SSH server in the unit must be enabled and the firewall must allow SSH access.

Syntax

config service ssh enabled [yes|no] **port** <*number*> **hostkeys** [none|640bit] **authmethods** [all|keyboard|password|publickey|none] **services** [all|ssh|sftp|none]

Parameters

enabled yes|no	Enable/disable the SSH server. The default is **enabled**.
port *number*	Enter a SSH server port number. The default is **22**.
hostkeys none|640bit	Enter the host keys the SSH server uses to authenticate itself. The default is **640bit**. To regenerate the SSH keys, HostKeys must first be set to none, and then to 640bit.
authmethods all|keyboard|password|publickey|none	Enter the permitted authentication method. The default is **all**.
services all|ssh|sftp|none	Enter the permitted SSH services. The default is **all**.

Example

The following example disables the SSH server:

```
> config service ssh enabled no
```

Related commands

```
display service ssh
show service ssh
whoison
```

service telnet

Telnet allows access to the BSGX4e over a remote terminal session. Telnet access requires the following:

- The workstation on the WAN or LAN must provide a Telnet client, for example Tera Term Pro, Windows telnet client, and Linux telnet client.
- The Telnet server in the unit must be enabled and the firewall must allow Telnet access.

Syntax

config service telnet enabled [yes|no] **port** <*number*>

Parameters

enabled yes|no	Enable/disable the Telnet server. The default is **enabled**.
port *number*	Enter a Telnet server port number. The default is **23**.

Example

The following example disables the Telnet server:

```
> config service telnet enabled no
```

Related commands

```
display service telnet
show service telnet
whoison
```

service web

The Web server enables remote administration of the BSGX4e using the Web User Interface.

The Web server supports access over HTTP and HTTPS (HTTP over SSL). For more information, see SSL commands on page 138.

Web server use requires the following:

- The workstation on the WAN or LAN must provide a Web browser (Microsoft® Internet Explorer® or Mozilla® Firefox®).
- The Web server in the unit must be enabled and the firewall must allow HTTP or HTTPS traffic from the WAN.

Syntax

config service web enabled [yes|no] **httpport** *<number>* **httpsport** *<number>*

Parameters

enabled yes|no	Enable/disable the web server. The default is **enabled**.
httpport *number*	Enter an HTTP port number for the Web server. The default is **80**.
httpsport *number*	Enter an HTTPs port number for the Web server. The default is **443**.

Example

The following example disables the Web server:

```
> config service web enabled no
```

Related commands

```
clear service web
stats service web
display service web
show service web
```

Shell terminal command

This section describes how to configure shell terminal settings:

- shell terminal

shell terminal

Use this command to configure the shell terminal settings.

Syntax

config shell terminal <*width size***> prompt** *<string>* **timeout** *<minutes>*

Parameters

width size	Enter the number of characters in a terminal line. The default is 80 characters.
prompt	Enter a string to define the command prompt.
timeout	Enter the number of minutes before the terminal logs out.

Example

The following example changes the command prompt from the BSGX4e to U4EA and the timeout value to 2 hours:

```
> config shell
Entering interactive mode: ctrl^z | 'exit', ctrl^c | 'quit'
                           TAB to cycle parameter options
*sh-term#*> prompt u4ea
*sh-term#*> timeout 120
*sh-term#*> exit
*u4ea*>
```

Related commands

```
display shell terminal
show shell terminal
```

SIP commands

The following section describes how to configure Session Initiation Protocol (SIP) commands. The SIP session controller controls the establishment and termination of VoIP sessions, as requested by endpoint devices. The integrated SIP gateway, which operates together with the session controller, serves as a VoIP gateway for analog devices. The SIP server determines how the session controller accesses SIP proxy servers to provide VoIP service.

sip gateway settings

Use this command to configure a SIP FxO gateway on the LAN side of the BSGX4e to provide the ability to call over the PSTN. An optional domain name can also be provided.

Note: Before the gateway is configured, the SIP session controller must be configured, and the gateway settings for the Local Call Routing must be configured. See sip sc settings on page 126 and lcr settings on page 63 more information.

Syntax

config sip gateway settings [domain *<domainname>*] **ip** *<ip address>* **port** *<number|range>*

Parameters

domain *fqdn*	Enter an optional domain name for the SIP gateway.
ip *ip address*	Enter an IP address for the SIP gateway.
port *number*	Enter the signaling RX port for the SIP gateway. The default is **5060**.

Example

```
> config sip gateway settings ip 192.168.1.1 port 5060
```

Related commands

```
display sip gateway settings
show sip gateway settings
show sip sc settings
show lcr setting
```

sip sc settings

The SIP session controller (SC) relays SIP messages between SIP endpoints and SIP servers, controls how VoIP media traffic is established, controls which LAN endpoints can place and receive calls and reports the quality of calls.

Syntax

config sip sc settings server *<name>* **lcdomain** *<domain>* **wanrxport** *<number>* **lanrxport** *<number>* **timert1** *<ms>* **timert2** *<ms>* **timerb** *<sec>* **timerf** *<sec>* **timerc** *<sec>* **maxcalls** *<number>* **sigqos** *<name>* **contpass** [yes|no] **switchtype** [BROADSOFT|NORTEL_CS2K|SIEMENS|SYLANTRO|OTHER] **forkingenable** [yes|no]

Parameters

server *name*	Enter the name of the SIP call server profile. To see the configured server profiles, enter **show sip server settings**.
lcdomain *domain*	Enter the local domain for LAN endpoints. SIP messages that do not match the domain are discarded. This parameter is optional.
wanrxport *number*	Enter the port on which to listen for SIP signaling messages from the WAN. The default is **5060**.
lanrxport *number*	Enter the port on which to listen for SIP signaling messages from the LAN. The default is **5060**.
timert1 *ms*	Enter the minimum retransmission time interval (in milliseconds). The default is **500** milliseconds.
timert2 *ms*	Enter the maximum retransmission time interval (in milliseconds). The default is **4000** milliseconds.
timerb *sec*	Enter the timeout interval for INVITE transactions (in seconds). The default is **16** seconds.
timerf *sec*	Enter the timeout interval for non-INVITE transactions (in seconds). The default is **32** seconds.
timerc *sec*	Enter the timeout interval for proxy INVITE transactions (in seconds). The default is **180** seconds (3 minutes).
maxcalls *number*	Enter the maximum number of SIP calls allowed simultaneously. Maximum number of SIP calls allowed simultaneously. The default is 50.
siqqos *name*	Enter the name of the GoS quality group that specifies the QoS protection for SIP signaling traffic. To see the configured quality groups, enter **show qos group**.

contpass yes|no — Enable/disable unknown content types to be relayed. The default is **yes**.

switchtype BROADSOFT|NORTEL_CS2K|SIEMENS|SYLANTRO|OTHER

BSGX4e interoperates with various softswitches that offer multi-line (forking) capabilities. These switches require special handling by the session controller. Selecting a vendor here instructs the session controller to format call ID codes to operate with the switch multi-line feature. This version of BSGX4e supports the following softswitches:

Broadsoft

Sylantro

Nortel CS2K (selected LG-Nortel phone models 6812 and 6830)

Future versions may support Siemens and Other (manual configuration) interoperability. In this release, forking is disabled by default when either of these is selected.

forkingenable yes|no

This parameter enables/disables SIP forking support. Sylantro is the only switch that requires this parameter to be enabled. If you selected Sylantro in the Switch Type field, set this field to enabled (yes). For all other vendors switches, set this field to disabled (no).

Example

```
> config sip sc settings server Sylantro_Automatic wanrxport
5060 lanrxport 5060 sigqos VoIP contpass yes
```

Related commands

```
display sip sc settings
show sip sc settings
show sip sc calls
show sip sc endpoints
clear sip sc calls
stats sip sc calls
clear sip sc status
stats sip sc status
show sip server settings
show qos group
```

sip server settings

Use this command to configure a server profile, which determines how the session controller accesses SIP proxy servers to provide VoIP services.

One of the session controller settings specifies the call server profile that the session controller is to use. A server profile can explicitly specify up to three SIP proxy servers or it can specify no. If no proxy server is specified, the session controller uses DNS to find its proxy servers. If no proxy server is specified in proxy1, proxy2, and proxy3, then the session controller uses DNS SVR to find its proxy servers. The SIP session controller can accept inbound messages from additional SIP servers if those servers are explicitly specified in the server profile currently in use. The firewall is automatically updated to accept SIP messages from the additional inbound servers. When configuring additional SIP servers, a single IP address or a range of addresses can be specified through the inbound server (ibserver) parameters. The DNS SRV feature automatically finds the SIP server.

Syntax

config sip server settings *<name>* **domain** *<domainname|ip address>* **proxy1** *<fqdn |ip address>* **port1** *<number>* **proxy2** *<fqdn|ip address>* **port2** *<number>* **proxy3** *<fqdn|ip address>* **port3** *<number>* [**ibserver1** *<ip address|range>* **ibserver2** *<ip address|range>* **ibserver2** *<ip address|range>*] **retries** *<number>* **blacklist** *<minutes>* **heartbeat** [yes|no] **hbtimer1** *<seconds>* **hbtimer2** *<seconds>*

Parameters

name
Enter the name of the server profile to be created or edited.

domain *domainname|ip address*
Enter the registrar domain for registering SIP phones.

proxy1 *fqdn|ip address*
Enter the first SIP proxy server (either a fully qualified domain name [FQDN] or an IP address).

port1 *number*
Enter the port number of the first proxy server. The default is **5060**.

proxy2 *fqdn|ip address*
Enter the second SIP proxy server (either a fully qualified domain name [FQDN] or an IP address).

port2 *number*
Enter the port number of the second proxy server. The default is **5060**.

proxy3 *fqdn|ip address*
Enter the third SIP proxy server (either a fully qualified domain name [FQDN] or an IP address).

port3 *number*
Enter the port number of the third proxy server. The default is **5060**.

ibserver1 *ip address|range*

Enter an optional additional inbound servers (IP address or range).

ibserver2 *ip address|range*

Enter an optional additional inbound servers (IP address or range).

ibserver3 *ip address|range*

Enter an optional additional inbound servers (IP address or range).

retries *number* — Enter the number of retries before a SIP proxy server is blacklisted. The default is **4** retries. (Specifying **0** disables call server failover.)

blacklist *seconds* — Enter a blacklist timer. The default is **600** seconds (ten minutes).

heartbeat no|yes — Enable/disable the SIP heartbeat. The default is **yes** (enabled). Enabled is recommended.

hbtimer1 *seconds* — Enter the timer between HeartBeat packets for active servers. The valid range is 10-100. The default is 30.

hbtimer2 *seconds* — Enter the timer between HeartBeat packets for temporary unavailable servers. The valid range is 5-25. The default is 15.

Example

The following example configures a single SIP server:

```
> config sip server settings Sylantro_Manual domain
sip.live.sylantro.net proxy1 server1.sip.live.sylantro.net
port1 6666
```

Example

Up to three SIP proxy servers can be explicitly specified in a setting. The second server is used only if the first server is unavailable; the third server is used only if the first and second servers are unavailable. This example configures a setting for failover mode:

```
> config sip server settings Sylantro_FailOverMode domain
sip.live.sylantro.net proxy1 primary.sip.live.sylantro.net
port1 6666 proxy2 secondary.sip.live.sylantro.net port2 6666
retries 4 blacklist 300
```

Example

The following example configures an additional inbound SIP server:

```
> config sip server settings Sylantro_AdditionalServer domain
sip.live.sylantro.net proxy1 server1.sip.live.sylantro.net
port1 6666 ibserver1 192.168.134.100
```

Related commands

```
del sip server settings
display sip server settings
show sip server settings
show sip server status
show sip sc settings
```

sip ua port

The SIP user agent (UA) allows an analog device to use VoIP connections to place and receive calls on a BSGX4e. The analog device must be connected to the BSGX4e port as described in the installation guide. The device can be a single analog device such as a telephone or fax machine or a gateway device which connects to multiple analog devices.

Use this command to configure the SIP user agent port. For more information on SIP user agent settings including session expiration timers and hold timers, see SIP UA settings on page 132.

Syntax

config sip ua port *<number>* **name** *<name>* **userid** *<id>* **authid** *<id>* **password** *<password>* **codec1** [PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20| NOTUSED] **codec2** [PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20| NOTUSED] **codec3** [PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20| NOTUSED] **codec4** [PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20| NOTUSED] **rfc2833** [yes|no] **payload** *<type>* **mls** [off|RFC3264|RFC2976] **mpt** [on|off] **fax** [on|auto|off] **vad** [yes|no] **up** [yes|no]

Parameters

port *number* — Enter 1 for the port.

name *name* — Enter the name for the display.

userid *id* — Enter the User ID of the SIP account.

authid *id* — Enter the authentication ID of the SIP account.

password *password* — Enter the password of the SIP account.

codec1 PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20|NOTUSED

Enter the most preferred codec and packet time. The default is **PCMU_20**.

codec2 PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20|NOTUSED

Enter the second most preferred codec and packet time. The default is **PCMA_20**.

codec3 PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20|NOTUSED

Enter the third most preferred codec and packet time. The default is **G729A_20**.

codec4 PCMU_10|PCMU_20|PCMA_10|PCMA_20|G729A_10|G729A_20|NOTUSED

Enter the fourth most preferred codec and packet time. The default is **NOTUSED**.

rfc2833 off|on	Enable/disable RFC 2833 for DTMF. **RFC2833** 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. The default is **yes**.
payload *type*	If **RFC2833** is enabled, the RTP dynamic payload type can be specified (96-127). The default is **101**.
mls Off|RFC3264|RFC2976	Enable/disable multi-line support. **RFC2976** uses out-band DTMF signals (using the SIP Signalling INFO method). The default is **off**.
mpt off|on	Enable/disable modem pass-through and force media to G.711 echo cancellation. Specify **on** (enabled) if a modem is connected to the BSGX4e. The default is **off**.
fax on|off|auto	Enable/disable fax pass-through and either force media to G.711 echo cancellation (**on**) or enable re-negotiation of the CODEC with the remote party to G.711 Echo Cancellation when a fax tone is detected (**auto**). The default is **off**.
vad yes|no	Enable/disable voice activity detection (silence suppression). Enabling VAD allows the BSGX4e to avoid sending silent RTP packets, conserving resources. 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. The default is **no** (disabled).
up yes|no	Enable/disable the SIP gateway port. The default is **no** (disabled).

Example

```
> config sip ua port 1 name uap1 userid uap1 authid uap1
password mysecret rfc2833 yes payload 96
```

Related commands

```
del sip ua port
display sip ua port
show sip ua port
show sip ua status
show sip ua settings
```

SIP UA settings

Use this command to configure the SIP protocol settings on a BSGX4e that apply to the SIP user agent. The SIP settings for the gateway do not apply to the SIP session controller.

The SIP protocol can be modified for interoperability purposes within the SIP environment.

Syntax

config sip ua settings timert1 *<ms>* **timert2** *<ms>* **timerb** *<ms>* **regexpire** *<seconds>* **seenable** [yes|no] **setimer** *<seconds>* **minsetimer** *<seconds>* **onholdtimer** *<seconds>* **noanstimer** *<seconds>* **endofdial** [yes|no] **interdigittimeout** *<seconds>*

Parameters

timert1 *ms*	Set the SIP retransmission T1 interval. The default is **500** milliseconds.
timert2 *ms*	Set the SIP retransmission T2 interval. The default is **4000** milliseconds.
timerb *ms*	Set the SIP retransmission B interval. The default is **32000** milliseconds.
regexpire *seconds*	Set the timeout interval for expiration of the endpoint registration. The default is **3600** seconds (1 hour).
seenable yes|no	Enable/disable session-expires support (see **setimer** and **minsetimer**). The default is **no** (disabled).
setimer *seconds*	Enter the maximum session interval if no session refresh requests are received. If the timer expires, the session ends. The default is **1800** seconds (30 minutes). This parameter is valid only if **seenable** is **yes**.
minsetimer *seconds*	Enter the minimum session interval that the User Agent can accept. The default is **90** seconds. This parameter is valid only if **seenable** is **yes**.
onholdtimer *seconds*	Enter the maximum interval of time in seconds that the User Agent can be put on hold with no audio or music-on-hold. If the on hold timer expires, the call is disconnected. The default is **180** seconds (3 minutes).
noanstimer *seconds*	

Enter the maximum interval of time in seconds that User Agent can ring without being answered. 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 that feature is enabled). The default is **60** seconds.

endofdial *yes|no*

Enable/disable the hash (**#**) character at the end of the dialed digit string; if enabled (yes), the **#** character is stripped from the digit string. The default is **yes**.

interdigittimeout *seconds*

Enter the maximum time allowed in seconds between the dialing of digits. The default is **3** 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 (for example, 911), the call is placed immediately.

Example

```
> config sip ua settings seenable yes setimer 600 minsetimer
500
```

Related commands

```
display sip ua settings
show sip ua settings
show sip ua port
```

SNMP commands

The following section describes how to configure SNMP commands. Use the following commands to configure SNMP on the BSGX4e.

- snmp agent
- snmp community
- snmp traps

snmp agent

Use this command to configure an SNMP agent. The SNMP agent MIBs are described in IETF RFC 1213.

The SNMP agent replies only to SNMP version 2c requests. Apart from the system group, all MIBs are in read-only mode in this version.

Note: The BSGX4e cannot be configured through SNMP. The port used by the SNMP agent must be opened in the Firewall, allowing SNMP clients to reach it.

Syntax

config snmp agent enabled [yes|no] **port** *<number>* **sysloc** *<location>* **syscon** *<contact>* **sysname** *<name>*

Parameters

enabled yes|no	Enable or disable the agent. The default is **enabled**.
port *number*	Enter the port or range of ports on which the agent listens. The default port is **161**.
sysloc *location*	Enter the SNMP system location (sysLocation MIB); physical location of the hardware.
syscon *contact*	Enter the SNMP system contact (sysContact MIB); contact person for this hardware.
sysname *name*	Enter the SNMP system name (sysName MIB); administrator assigned to this hardware.

Example

```
> config snmp agent enabled yes port 161
```

Related commands

```
clear snmp agent
display snmp agent
show snmp agent
stats snmp agent
show snmp community
```

snmp community

Use this command to configure SNMP communities including the IP address and access rights.

Syntax

config snmp community *<community name>* **ip** *<address>* **access** [read|read-write]

Parameters

community community-name

Enter the name for the community.

ip *ip address*

Enter the IP address of the management station.

access read|read-write

Enter the access rights for this community string.

Example

```
> config snmp community public ip 192.168.134.160 access read
```

Related commands

```
display snmp community
show snmp community
```

snmp traps

Use this command to configure SNMP traps. The following traps are supported:

- **ColdStart**: indicates the BSGX4e has restarted.
- **WarmStart**: indicates the SNMP agent has restarted.
- **LinkUp**: indicates an interface has come up.
- **LinkDown**: indicates an interface has gone down.
- **AuthenticationFail**: indicates SNMP authentication has failed (such as when the wrong community name is used).

Syntax

config snmp traps enabled [yes|no] **comm** <*community*> **ip** <*ip address*>

Parameters

enabled yes|no	Enable or disable the SNMP traps.
comm *community*	Enter the traps community
ip *ip address*	Enter the IP address of the management station receiving the traps.

Example

```
> config snmp traps enabled yes comm public ip 192.168.134.161
```

Related commands

```
display snmp traps
show snmp traps
clear snmp agent
stats snmp agent
```

SSL commands

This section describes how to configure the Secure Socket Layer (SSL). Use the following commands to enable SSL to secure remote access to the BSGX4e over an insecure network.

- ssl certificate
- ssl csr
- ssl key

ssl certificate

The SSL certificate allows a system administrator to configure an X509 certificate used by the SSL server. There are two methods to generate the X509 certificate: either it is generated from a self signed SSL CSR or the SSL CSR is signed by an external certificate authority and a certificate is imported.

A single X509 certificate can be generated. When self-signed, the certificate is derived from the current CSR record and key record. Thus, a self-signed certificate can be generated only if an SSL key record and an SSL CSR record exist.

Alternately, an SSL CSR can be imported using a file containing a certificate signed by an external certificate authority (CA). The certificate must be in PEM format with no header before the ----- BEGIN CERTIFICATE ----- text. When a CA-signed certificate is imported, it is checked that the certificate is in the correct PEM format. If the format is incorrect, the certificate is not imported.

Syntax

config ssl certificate *<type>* **signed** [self|null] **import** *<pem format>*

Parameters

type	Enter the certificate type **x509**.
signed self|null	Self-sign the current CSR. See ssl csr on page 140.
import *pem format*	Enter the PEM format file from which to import the certificate.

Example

This example generates an RSA key of 768 bits. It then generates an SSL CSR for the Sells unit of the company EiffelGroup in Paris, France and, finally, generates a self-signed SSL certificate. See ssl csr on page 140 and ssl key on page 142 for more information on assigning an SSL CSR and key.

```
> config ssl key rsa bits 768

> config ssl csr x509 country FR no state locality Paris
orgname EiffelGroup orgunit Sells commonname
www.eiffelgroup.com email contact@eiffelgroup.com

> config ssl certificate x509 signed self
```

Related commands

```
del ssl certificate
display ssl certificate
show ssl certificate
show ssl csr
show ssl key
```

ssl csr

The SSL Certificate Signing Request (CSR) allows a system administrator to generate an X509 certificate, which can be self-signed by the SSL module or signed by an external certificate authority (CA).

A single X509 CSR can be generated. Generating a CSR requires an SSL key. To see the status of the SSL key, enter **show ssl key**.

Note: If the SSL CSR is deleted, new SSL connections cannot be created.

Syntax

config ssl csr *<certificate>* **country** *<code>* **state** *<name>* **locality** *<name>* **orgname** *<name>* **orgunit** *<name>* **commonname** *<domain>* **email** *<address>*

Parameters

type *certificate*	Enter the certificate type **x509**.
country *code*	Enter a two-letter country code. The default is US for the United States. Go to www.iso.org for the most recent list.
state *name*	Enter a full name of a state or province, for example, california.
locality *name*	Enter a locality or city name, for example, fremont.
orgname *name*	Enter a company name, for example, U4EA.
orgunit *name*	Enter the organizational unit of the company, for example, engineering.
commonname *domain*	Enter a domain name, for example, www.example.com
email *address*	Enter an email address, for example, guest@example.com

Example

This example imports an SSL CSR. SFTP must be used. The recommended directory for the uploaded CSR file is /cf0sys/ssl. An example follows.

1. Connect the BSGX4e unit:

```
fred@cygnus ~ $ sftp admin@192.168.134.217

Connecting to 192.168.134.217...
The authenticity of host '192.168.134.217 (192.168.134.217)'
can't be established.
DSA key fingerprint is
9a:1f:34:52:f1:78:d7:6c:56:5b:9d:73:f0:da:1f:c0.


Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.134.217' (DSA) to the list
of known hosts.
User: admin
Password:
```

2. Set the current directory and store the CSR file in it:

```
sftp> cd /cf0sys/ssl
sftp> put csr.pem
```

```
Uploading csr.pem to /cf0sys/ssl/csr.pem
```

3. Check that the CSR file is in the current directory:

```
sftp> ls
rsakey.dat          csr.pem
sftp> exit
```

4. The following imported CSR can be used to generate the SSL certificate as described in the ssl certificate on page 139:

```
> config ssl certificate x509 import /cf0sys/ssl/csr.pem
```

Related commands

```
del ssl csr
display ssl csr
show ssl csr
show ssl certificate
show ssl key
```

ssl key

The SSL key allows the system administrator to manage a private RSA key, which is needed by the SSL server to encrypt data. The first time the BSGX4e is started, a randomly-seeded, 1024-bit RSA key is generated and saved. Normally, a new private key does not need to be generated unless it is suspected that the security of the private key had been compromised. The RSA key is stored in the file /cf0sys/ssl/rsakey.dat.

Note: If the SSL key is deleted, new SSL connections cannot be created. To see the status of the SSL key, enter **show ssl key**.

A new SSL key can be generated. The number of bits is constrained to 512, 768, 1024 or 2048. When the SSL key record is created or modified, a key generation task is started. Key generation can take several minutes depending on the size of the key. When key generation starts, the key used by the SSL server is deleted; new SSL connections cannot be created until a new key is available. When key generation completes, the RSA key used by the SSL server is set to the newly generated key; new SSL connections can then be created.

Syntax

config ssl key *<type>* **bits** [512|768|1024|2048]

Parameters

type	Enter the encryption key type **rsa**.
bits 512|768|1024|2048	Enter the number of bit in the key.

Example

```
> config ssl key rsa bits 768
```

Related commands

```
del ssl key
display ssl key
show ssl key
show ssl certificate
show ssl csr
```

Switch commands

This section describes how to configure the LAN switch:

qos

The LAN switch in the BSGX4e provides a layer 2 Quality of Service (QoS) feature. This feature enables prioritization of network traffic, which is essential for the protection of time-sensitive traffic such as VoIP phone calls.

Because it has multiple LAN ports to send traffic to the WAN and only one WAN interface to send that traffic, the BSGX4e must prioritize the traffic it routes. Layer 2 QoS is provided to guarantee that higher priority traffic is routed while lower priority traffic can be delayed or discarded. Layer 2 QoS is most effective for traffic switched from the LAN to the IP host to be routed to the WAN.

For a full QoS solution to manage LAN to WAN traffic, configuration of layer 3 QoS is also recommended. For information about the layer 3 QoS implementation, see QoS (GoS) commands on page 89.

Layer 2 QoS provides four queues to classify and prioritize network traffic: LOWESTQ, LOWQ, HIGHQ and HIGHESTQ. LOWESTQ is the lowest priority queue; HIGHESTQ is the highest priority queue. The four queues are assigned weights (8:4:2:1) that determine the time and number of packets serviced from the queue. (The queue weighting cannot be changed.)

Two scheduling methods are available; the default method is WFQ:

- Weighted Fair Queuing (WFQ)

  All queues are serviced depending on the weight assigned to the queue. No starvation occurs, that is, even the lowest priority queue receives service periodically.

- Fixed

  All priority packets are serviced from a queue until that queue is empty, and then the next lower-priority queue is serviced, and so on. Starvation can occur, that is, the traffic load for a higher-priority queue can prevent lower-priority queues from being serviced.

Packets are classified and then assigned to one of the four priority queues. Layer 2 QoS can classify traffic using any one of the following criteria:

- Port number (the default classification has all ports mapped to LOWESTQ)
- IEEE 802.1p tag
- DiffServ/ToS tag

The table below lists the default priority queues depending on the criteria used for classification.

Table 7 Default Priority Queues

Priority Queue	Port Number	IEEE 802.1p or ToS Tag	Tos/DiffServ Tag
LOWESTQ	All ports	1, 2	0 - 15
LOWQ		0, 3	16 - 31
HIGHQ		4, 5	32 - 47
HIGHESTQ		6, 7	48 - 63

switch qos ieee

This command maps IEEE 802.1p values to priority queues. This command is valid only if **8021p** is selected as the layer 2 QoS type. See switch qos setting on page 148 for more information on selecting a layer 2 QoS type.

Syntax

config switch qos ieee *<value>* **priority** [lowestq|lowq|highq|highestq]

Parameters

ieee *value*

Enter the IEEE 802.1p tag value to map to the priority queue. Valid range is 0-7.

priority lowestq|lowq|highq|highestq

Enter the priority queue. The default is lowq.

Example

The following example selects IEEE 802.1p tag mapping and then maps tags 4 and 5 to the highest-priority queue.

```
> config switch qos setting type 8021p
> config switch qos ieee 4 priority highestq
> config switch qos ieee 5 priority highestq
```

Related commands

```
display switch qos ieee
show switch qos ieee
show switch qos settings
```

switch qos port

This command maps port numbers to priority queues. This command is valid only if port is selected as the layer 2 QoS type. See switch qos setting on page 148 for more information on selecting a layer 2 QoS type.

Syntax

config switch qos port *<value>* **priority** [lowestq|lowq|highq|highestq]

Parameters

port *value*	Enter the specific port number to map to a priority queue. Valid range is 1-4. Entering range of ports is not valid.
priority lowestq|lowq|highq|highestq	Enter the priority queue.

Example

```
> config switch qos port 1 priority highestq
```

Related commands

```
display switch qos port
show switch qos port
show switch qos settings
```

switch qos setting

Use this command to configure layer 2 QoS settings.

Syntax

config switch qos setting type [port|TOSDiff|8021p] **scheduling** [wfq|fixed]

Parameters

type port|TOSDiff|8021p

Enter the criterion that layer 2 QoS uses to classify traffic. The default is **port**.

scheduling wfq|fixed

Enter the method of QoS scheduling. The default is **wfq**.

Example

```
> config switch qos setting type 8021p scheduling wfq
```

Related commands

```
show switch qos settings
display switch qos settings
show switch qos port
show switch qos ieee
show switch qos tos
clear switch port
show switch port
```

switch qos tos

This command maps IP ToS/DiffServ values to priority queues. This command is valid only if **tosdiff** is selected as the layer 2 QoS type. See switch qos setting on page 148 for more information on selecting a layer 2 QoS type.

Syntax

config switch qos tos *<value>* **priority** [lowestq|lowq|highq|highestq]

Parameters

tosdiff *value* Enter the port number to map to the highest priority queue. Valid range is 0-63.

priority lowestq|lowq|highq|highestq

Enter the priority queue.

Example

The following example selects **TOSDiff** mapping as the setting type, and then maps tag 45 to the highest-priority queue.

```
> config switch qos setting type TOSDiff
> config switch qos tos 45 priority highestq
```

Related commands

```
display switch qos tos
show switch qos tos
show switch qos settings
```

switch arl

Address Resolution Logic (ARL) maps MAC addresses to specific LAN ports. This enables switching packets between ports based on the destination MAC address in the packet. ARL provides these features:

- Dynamic Entries

  A MAC address learning process automatically builds the ARL table as a forwarding database. The entries it creates are dynamic entries, that is, entries that are flushed regularly from the table.

- 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 flushed.

- Prioritizing Traffic by MAC Address

  By defining static ARL entries, you can prioritize traffic by the destination MAC address in the packet. Each static entry can be assigned to a priority queue. Packets that match the entry are assigned to the specified priority queue. Four priority queues are available: LOWESTQ, LOWQ, HIGHQ, and HIGHESTQ.

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

Syntax

config switch arl state {dynamic|static] **mac** *<mac address>* **age** *<seconds>* **priority** [lowestq|lowq|highq|highestq] **ports** *<number>*

Parameters

state dynamic|static

Enter the type of ARL. The default is **dynamic**.

mac *mac address*

Enter the MAC address in format xx.xx.xx.xx.xx.xx.

age *seconds*

Enter the aging interval that determines when dynamic entries are flushed from the table. The valid range is 16-4080 seconds. The value is rounded to the next multiple of 16. The default aging interval is 304 seconds.

priority lowestq|lowq|highq|highestq

Enter the priority queue.

ports *number*

Enter the LAN port(s) associated with this MAC address (**0**(MII) to 4).

Example

The following example adds a static ARL entry to the forwarding database. It maps a MAC address to port 3 and assigns its traffic to the highest priority queue.

```
> config switch arl state static mac 00:80:2E:11:11:11
priority highestq ports 3
```

Example

The following example increases the aging interval for the ARL table to 320 seconds:

```
> config switch arl age 320
```

Related commands

```
clear switch arl
show switch arl
```

switch mirror

Use this command to configure port mirroring. Port mirroring duplicates traffic from one or several source ports to a destination port. The following port traffic can be mirrored:

- Outgoing traffic only
- Both incoming and outgoing traffic.

Port mirroring is intended for troubleshooting only. After its use is complete, remove the port mirroring configuration immediately so that unit performance is not degraded.

Port mirroring applies to LAN ports only. Also, the mirroring port and the port being mirrored have the same speed.

Syntax

```
config switch mirror port [0 [MII]|1|2|3|4] mirror [1|2|3|4]
dir [both|out|none]
```

Parameters

port 0 MII|1|2|3|4	Enter the port number for which traffic is mirrored.
mirror 1|2|3|4	Enter the destination port for the mirrored traffic. If mirroring is currently taking place, the default is the current destination port.
dir both|out|none	Enter the direction of traffic to mirror.

Example

This example configures mirroring so that both incoming and outgoing traffic for port 2 is mirrored to port 3.

```
> config switch mirror 2 mirror 3 dir both
```

Related commands

```
del switch mirror
display switch mirror
show switch mirror
```

switch port

Use this command to configure the BSGX4e LAN ports.

There is an uplink port (port 0 or MII) and 4 LAN ports. Network traffic from the switch is sent through port 0 to the host for routing. The uplink port cannot be configured. It always operates at 100 Mbps, full duplex mode, flow control disabled.

Each front port can be configured to automatically negotiate the appropriate speed and duplex mode or for a speed of 10Base-T or 100Base-T and either half or full duplex mode. The initial configuration for each LAN port specifies **auto-negotiation** for speed and duplex mode.

Flow control for a port can be disabled or configured to provide either back pressure (forced collision) for half duplex mode or pause frames for full duplex mode. The initial configuration for each LAN port disables flow control.

Syntax

config switch port *<number>* **speed** [auto|10half|10full|100half|100full] **flow** [yes|no] **enabled** [yes|no]

Parameters

port *number*	Configure a LAN port. The valid range is 1-4.
speed auto|10half|10full|100half|100full	Specify a speed and duplex mode. The default is auto.
flow yes|no	Enable flow control for half duplex mode or for full duplex mode. The default is **no**.
enabled yes|no	Select whether or not the port is enabled. The default is yes.

Example

This example enables port 2 and changes its speed setting to auto-negotiation.

```
> config switch port 2 speed auto enabled yes
```

Example

This example enables port 3 and changes its configuration to 100 Mbps full duplex with flow control enabled and the port is enabled:

```
> config switch port 3 speed 100full flow yes enabled yes
```

Related commands

```
display switch port
show switch port
clear switch port
stats switch port
```

switch vlan

This command assigns ports as members of a Virtual LAN (VLAN). The ports can be any of the LAN switch ports. The ports can be the WAN port or any of the LAN switch ports. Switching is confined to the members of VLANs.

Packets can be transmitted tagged with the VLAN ID for VLAN trunking or untagged as follow:

- Tagged ports transmit tagged packets. A port can belong to multiple VLANs as tagged.
- Untagged ports transmit untagged packets. A port can belong to only one VLAN as untagged.

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.

Tagged packets arriving at a port, including a VLAN identifier different than the one of the port, are dropped.

IEEE 802.1p packets are considered untagged packets.

Syntax

config switch vlan *<vid>* **name** *<name>* **p1|p2|p3|p4** [*|u|t]

Parameters

vid	Enter the VLAN identification number. Valid range is 1-4094.
name *<name>*	Enter a name or description of the VLAN. Up to 32 characters are allowed.
p1|p2|p3|p4 *|u|t	Enter the VLAN state of the port. * is not member, U is member and untagged, T is member and tagged.

Example

The following example assigns port 1 to VLAN 3 as an untagged port.

```
> config switch vlan 3 name v3 p1 u
```

Related commands

```
display switch vlan
show switch vlan
show interface vlan
```

System commands

This section describes how to configure the following system parameters:

- system dns
- system dyndns
- system images
- system info
- system sntp
- system startup
- system watchdog

system dns

The Domain Name Service (DNS) client in the unit sends requests to a DNS server on the WAN. A DNS request is used to get an IP address required by the BSGX4e, such as the IP address of a server that was specified by a fully-qualified domain name (FQDN). Two DNS servers can be configured: one as the primary server; the other as a secondary, backup server.

This command specifies the source of the DNS configuration the client is to use (auto, dhcp, ppp, or user). The default is auto. If specifying a user-provided DNS configuration, the configuration can be used only when either the source parameter value is set to user, or the source parameter value is auto and a DNS server configuration is not provided by the DHCP or PPP server. An optional domain name can be specified.

Syntax

config system dns [**dsn1** *<ip address>*|**dns2** *<ip address>*] **domain** *<FQDN>* **source** [auto|dhcp|ppp|user]

Definitions

dns1|2 *ip address*	Enter the IP address of the primary and secondary DNS servers.
domain *FQDN*	Enter the domain name for the BSGX4e. The DNS client adds the domain to the host before querying the DNS server. For example, if the specified name is host and the specified domain is domain.com, the query is for host.domain.com
source auto|dhcp|ppp|user	Sets the configuration of the user. Use the configuration provided by the DHCP or PPP server or use the latest user-provided configuration. If the DHCP or PPP server cannot provide a configuration, the server address is set to 0.0.0.0. The default is **auto**.

Example

```
> config system dns dns1 192.168.1.2
```

Related commands

```
display system dns
show system dns
show relay dns cache
```

system dyndns

Attention:

Dynamic DNS is not yet supported.

The dynamic DNS service allows a remote host on the Internet to stay connected to the BSGX4e when it is configured with DHCP or PPP on the WAN interface. When the BSGX4e is configured with a dynamic IP address on its WAN port, remote hosts can not stay connected as the BSGX4e's address 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.

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 and no-ip.com. Dynamic DNS is disabled by default.

Syntax

config system dyndns service [dyndns@dyndns.org|default@no-ip.com] **enabled** [yes|no] **user** *<name|email address>* **password** *<string>* **hostname** *<alias hostname>* **period** *<minutes>* **forceupdateperiod** *<days>* **wildcard** [nochg|on|off]

Parameters

service dyndns@dyndns.org|default@no-ip.com

Enter the service name.

enabled yes|no

Enable the DynDNS client. The default is no.

user *name|email address*

Enter the user name of the dynamic DNS account.

password *string*

Enter the password of the dynamic DNS account.

hostname *alias hostname*

Enter a hostname alias. This is the user name + domain of the dynamic DNS account.

period *minutes*

Specify the refresh period. The valid range is 10-1440 minutes. The default is 60.

forceupdateperiod *days*

Enter the number of days to prevent hostname from being deleted. The valid range is 20-35 days. The default is 30.

wildcard nochg|on|off

Specify whether or not *.yourdomain.ext is to be resolved to the same IP address than yourdomain.ext. The default is **nochg**.

Example

```
config system dyndns service dyndns@dyndns.org enabled yes
user test password **** hostname test.dyndns.org period 60
forceupdateperiod 30 wildcard nochg
```

Related commands

```
display system dyndns
show system dyndns
```

system images

This configures the default boot application.

Syntax

config system images [1|2] **default** [yes|no]

Parameters

slot 1|2	Designate the slot number to which the application image is assigned.
default yes|no	Designate yes to assign this slot as the default. No indicates this slot is not the default.

Example

```
> config system images 1 default yes
```

Related commands

```
display system images
show system images
```

system info

Use this command to configure the name and country code of the BSGX4e. Selecting a country code makes the appropriate configuration changes to the FxS telephony interfaces, for voice tone configurations (see voice tones on page 183) and to the session controller, for emergency call numbers configuration (see lcr settings on page 63).

NOTE: After changing the country code, save the change and reboot the system to implement the change.

Syntax

config system info unit *<name>* **country** [code]

Parameters

unit *name*	Designate a name for the BSGX4e.
country code	Designate a country code for the BSGX4e. The country codes are as follows: Certified Countries — AT BE BG CA CY CZ DE DK EE ES FI FR GB GR HU IE IT LT LU LV MT NL PL PT RO SE SI SK US Non-Certified Countries (to be used in trials and for demonstration only) — AD AE AF AG AI AL AM AN AO AQ AR AS AU AW AZ BA BB BD BF BH BI BJ BM BN BO BR BS BT BU BV BW BY BZ CC CF CG CH CI CK CL CM CN CO CR CS CU CV CX DD DJ DM DO DZ EC EG EH ER ET FJ FK FM FO FX GA GD GE GF GH GI GL GM GN GP GQ GS GT GU GW GY HK HM HN HR HT ID IL IN IO IQ IR IS JM JO JP KE KG KH KI KM KN KP KR KW KY KZ LA LB LC LI LK LR LS LY MA MC MD MG MH ML MN MM MO MP MQ MR MS MU MV MW MX MY MZ NA NC NE NF NG NI NO NP NR NT NU NZ OM PA PE PF PG PH PK PM PN PR PW PY QA RE RU RW SA SB SC SD SG SH SJ SL SM SN SO SR ST SU SV SY SZ TC TD TF TG TH TJ TK TM TN TO TP TR TT TV TW TZ UA UG UM UY UZ VA VC VE VG VI VN VU WF WS YD YE YT YU ZA ZM ZR ZW ZZ See the following link to identify the country codes: www.iso.org/iso/country_codes/iso_3166_code_lists/english_country_names_and_code_elements.htm

Example

```
> config system info unit BSGX4e country ca
```

Related commands

```
display system info
show system info
show system country
```

system sntp

Use this command to configure the SNTP client.

Syntax

config system sntp enabled [yes|no] **source** [user|dhcp|auto] **server**[**1|2|3|4**] *<ip address|FQDN>* **gmtoffset** [+/-]*<hh:mm>* **sync** *<days>*

Parameters

enabled yes|no — Enable/disable the SNTP client. The default is enabled.

source user|dhcp|auto

Sets the configuration of the user, the DHCP or allows the client to choose the source. The SNTP client can get SNTP server configuration automatically. The configuration from comes from the DHCP server if possible; otherwise, it uses the user-provided configuration. If the DHCP server cannot provide a configuration, the server address is set to 0.0.0.0. The default is **auto**.

server1|2|3|4 *ip address|FQDN*

Enter the IP address or a fully qualified domain name of a NTP server.

gmtoffset
+/-*hh:mm* — Set the time zone offset from GMT in hour:minute format. The default is 00:00.

sync *days* — Set the synchronization interval in number of days (1-31). The default is **7**.

Example

This example enables the SNTP client, specifies the configuration source as the user, and specifies the name of a NTP server and the time zone offset. The FQDN of the NTP server is ntpserver.wan.com. The GMT offset is one hour forward (+1).

```
> config system sntp enabled source user server1
ntpserver.wan.com gmtoffset +1

> save

> show system sntp
SNTP:
Enabled  on
Source   user
Server 1 ntpserver.wan.com
Server 2 0.0.0.0
Server 3 0.0.0.0
Server 4 0.0.0.0
Gmt Offset+01:00
Sync Interval7 days
Last SyncFRI FEB 17 15:53:25 2007
Next SyncFRI FEB 24 15:53:25 2007
```

Example

The following example changes the configuration source to auto. Assuming the DHCP server provides an NTP server configuration, the **show** command lists the DHCP-provided configuration currently in use. The **display** command lists the previously-saved, user-provided configuration that is available.

```
> config system sntp source auto

> save

> show system sntp

SNTP:
Enabled  on
Source   auto (dhcp)
Server 1 172.29.167.101
Server 2 172.29.0.1
Server 3 172.29.221.2
Server 4 172.29.0.75
Gmt Offset+01:00
Sync Interval7 days
Last SyncFRI FEB 17 15:53:25 2007
Next SyncFRI FEB 24 15:53:25 2007

> display system sntp

# SNTP client settings
Enabled  yes
Source   auto
Server1  ntpserver.wan.com
Server2  0.0.0.0
Server3  0.0.0.0
Server4  0.0.0.0
gmtOffset+01:00
Sync     7
```

Related commands

```
display system sntp
show system sntp
```

system startup

Use this command to configure the BSGX4e to run a command automatically after each restart.

Syntax **config system startup** <*index*> **command** "<*command name*>"

Parameters:

index	Designate the number of the command index. The first command has the index of 0.
command "*command name*"	Designate a command to run after each restart. Enclose the command in double-quotes.

Example

```
> config system startup 0 command "show system info"
```

Related commands

```
display system startup
show system startup
```

system watchdog

Use this command to configure the watchdog timer. The watchdog reset timer allows the BSGX4e to automatically restart after a software failure. Such a failure can disrupt normal traffic flow through the BSGX4e. The automatic reset allows restoring the BSGX4e to normal operation.

Note: It is recommended that the initial watchdog configuration remain unchanged. The initial configuration enables the reset timer and sets its value to 7 seconds.

Syntax

config system watchdog enabled [yes|no] **refresh** <*seconds*>

Parameters

enabled yes|no	Enable/disable the watchdog timer.
refresh *seconds*	Enter the refresh interval for the timer in seconds. Default is **7**.

Example

```
> config system watchdog enabled yes refresh 5
```

Related commands

```
display system watchdog
show system watchdog
```

Tacplus command

This section describes how to configure the TACACS+ client of the BSGX4e.

tacplus client

This command provides additional security when logging in to the BSGX4e. When a log in is externally authenticated, a client in the device sends the log in information to an external server for authentication.

Note: When external authentication is used for a user account, the external server defines the password required for log in using the account. The password command can change the internal password stored for the account, but this password is not used for authentication and so the effective password is not changed.

One external authentication method uses the TACACS+ protocol to provide authentication services. Normal operation fully encrypts the body of the packet for secure communication. It uses TCP port 49.

The TACACS+ client in the BSGX4e is compatible with standard TACACS+ servers, maps TACACS+ authentication records to users by their user account name, can reference up to twenty TACACS+ authentication records, and provides ASCII log in authentication.

Syntax

config tacplus client [admin|user] **enabled** [yes|no] **server** *<ip address|fqdn>* **key** *"<command name>"*

Parameters

admin|user	Enter the name of the user account to which the authentication record applies.
enabled yes|no	Enable/disable TACACS+ for the user. The default is **no**.
server *ip address|fqdn*	Enter the IP address or FQDN of the TACACS+ server.
key *"command name"*	Enter a shared key for the client as determined by the server. If the key includes a space character, enclose the key value in double-quote characters (" ").

Example

The following example creates an authentication record for user account TACuser. It assumes that the user account TACuser has been configured and TACACS+ has been specified as its authentication method. See user accounts on page 169 for more information on configuring user accounts.

```
> config tacplus client tacuser

Entering interactive mode: ctrl^z | 'exit', ctrl^c | 'quit'
                           TAB to cycle parameter options
tacplus-cl-TACu#> enabled yes
tacplus-cl-TACu#> server 172.29.19.56
tacplus-cl-TACu#> key "tacacskey"
tacplus-cl-TACu#> exit
```

Related commands

```
del tacplus client
display tacplus client
show tacplus client
show user accounts
```

User commands

This section describes how to configure user accounts, groups and rights.

- user accounts
- user groups
- user rights

user accounts

This command defines user access to a BSGX4e. There are two types of users, administrators (admins) and regular users (users). Administrators are granted all access modes and all access rights; regular users are granted only Web and CLI access. Regular user rights are restricted. A maximum of 20 user accounts can be defined for the BSGX4e.

Syntax

config user accounts *<name>* **access** [all|ssh+web+cli+telnet+ftp|none] **auth** [sha|radius|tacacs] **group1** [admins|users|none] [group2|3|4|5 [admins|users|none]] **password** *<password>* **inherit** [yes|no] **enabled** [yes|no]

Parameters

name Enter the name of the existing account to be changed or a new account to be added. This parameter is required. If an existing account is specified, only the specified parameter values are changed; all other existing values remain unchanged.

access all|ssh+web+cli+telnet+ftp|none
Select an access method. Choose all or none or a combination of the others.

auth sha|radius|tacacs

Internal or external password authentication. The default is internal Strong Password Hashing (SHA). To require external authentication, specify RADIUS or TACACS+ and configure an authentication record for this user account.

group1 admins|users|none

The pre-defined user groups are admins and users. If another user group has been configured, the user account can be assigned to it. To remove the user from a group, specify the group parameter with the value none.

group2|3|4|5 Optional additional user groups to which the user account is assigned

password *password* Enter the password for the user account if internal authentication is used. (If external authentication is used, the password entered at log in must be the password defined by the external server.) The default is admin.

inherit yes|no Define whether the user account inherits access rights from the groups it belongs to. The default is **yes**.

enable yes|no Enable/disable the user account. The default value is **yes**.

Example

This example assumes that the user is given read and write access to the unit, but only while connected directly to its console port or to the Web interface. Remote access is disallowed. The name of user is user1, the access methods are web + cli, the group membership is admins and the password is test123.

```
> config user account user1

Entering interactive mode: ctrl^z | 'exit', ctrl^c | 'quit'
TAB to cycle parameter options
user-accounts-user#> access web + cli
user-accounts-user#> group1 admins
user-accounts-user#> password test123
user-accounts-user#> exit
```

Related commands

```
del user accounts
display user accounts
show user accounts
show user groups
show user rights
```

user groups

This command defines user access to a BSGX4e as managed by user accounts, and user rights settings. There are two user groups, one for administrators (admins) and one for all other users (users). The admins user group is granted all access modes. The users user group is granted only Web and CLI access.

Syntax

config user groups *<name>* **access** [all|ssh+web+cli+telnet+ftp|none] **auth** [sha|radius|tacacs] **all** [yes|no]

Parameters

name
Enter the name of the existing group to be changed or the new group to be added. This parameter is required. If an existing group is specified, only the specified parameter values are changed; all other existing values remain unchanged.

access all|ssh+web+cli+telnet+ftp|none
Select an access method. Choose all or none or a combination of the others.

auth sha|radius|tacacs
Enter the internal or external password authentication. The default is internal Strong Password Hashing (SHA). To require external authentication, specify RADIUS or TACACS and configure an authentication record for this user group.

all yes|no
Specify whether or not **access** is to be allowed. The default is **no**, meaning that enforcement is in place. If yes is specified for a group (such as for the admins group), checks are not enforced.

Example

This example adds a new user group named dev giving it all access rights and no authentication enforcement:

```
> config user group dev access all all yes
```

Related commands

```
display user groups
show user groups
show user accounts
show user rights
```

user rights

There are three rights settings — one for the Administrators (admins) user group and the other two for the users user group. All rights are granted to admins; the two rights settings for the users user group grant read-only access to some objects and read and write access to other objects. The available access rights are read, write, and execute. Read allows the viewing of data; write allows the writing of data; execute is not currently used.

Note: You must configure the user group before you can configure a rights record for it. For more information, see the command user groups on page 171.

Syntax

```
config user rights <id> access [all|read + write + execute
|none] gname <name> object [admins|users]
```

Parameters

id

Enter the identifier of the new or existing rights record. This parameter is required. If you edit an existing rights record, only the values specified on this command are changed; all other values in the record remain unchanged.

access all|read + write + execute |none

Select an access method. Choose all or none or a combination of the others.

gname *name*

Enter group name for this rights record.

objects admins|users

Enter the objects to which this record applies. A group can have more than one rights record defined for it. For example, the predefined rights records **useradv** and **userbasic** are both defined for the same user group called users. In this case, two rights records are defined so that the user group can be granted different access to different objects in the system, as follows:

The **useradv** record applies to objects that belong to Admins; it grants only read access.

The **userbasic** record applies to objects that belong to Users; it grants both read and write access.

Example

```
> config user rights user access read gname users object Users
```

Related commands

```
display user rights
show user rights
config user accounts
show user accounts
config user groups
show user groups
```

Voice Commands

This section describes how to configure the following voice features:

- voice acl
- voice fxo gain
- voice fxo hw impedance
- voice fxs gain
- voice fxs hw impedance
- voice fxs ring pattern
- voice jitterbuffer
- voice np
- voice tones

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. 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).

Syntax

config voice acl <id> **mac** *<mac address>* **epid** *<id>* **softversion** *<version>* **platform** *<type>* **deviceid** *<id>* **seq** [begin|end|position] **ip** *<ip address(es)>* **type** [any|mgcp|sip] **action** [deny|allow]

Parameters

id	Enter a numeric identifier of the policy. Specify **new** to create a new policy.
mac *mac address*	Enter the MAC address of the endpoint in xx:xx:xx:xx:xx format.
epid *id*	Enter the endpoint identifier in alphanumeric format.
softversion *version*	Enter the software version of the endpoint.
platform *type*	Enter the platform type of the endpoint.
deviceid *id*	Enter the device ID of the endpoint.
seq beg|end|position	Enter the sequence number of the policy.
ip ip address(es)	Enter the IP address or range of address for the endpoints in a.b.c.d format. Use a.b.c.d-a.b.c.d format for a range of IP addresses.
any|mgcp|sip	Enter the signaling type of the endpoint. The default is **sip**.
deny|allow	Indicate the access given by this entry. The default is **allow**.

Example

This example configures a new ACL policy. The entry denies access to the SIP LAN endpoint identified by SIP000F8F073088.

```
> config voice acl new deviceid SIP000F8F073088 type sip
action deny
```

Related commands

```
display voice acl
show voice acl
show cdp entry
show cdp neighbors
show cdp traffic
```

voice fxo gain

This command sets the DSP gain values for the FXO port(s).

Syntax

config voice fxo gain tx *<value>* **rx** *<value>*

Parameters

tx *value*	Enter the transmit (tx) gain (digital to analog conversion) in decibels. Specify a minus (-) before a negative value. The default is **-0** dB.
rx *value*	Enter the receive (rx) gain (analog to digital conversion) in decibels. Specify a minus (-) before a negative value. The default is **0** dB.

Example

```
> config voice fxo gain tx -6 rx -6
```

Related commands

```
show voice fxo gain
display voice fxo gain
```

voice fxo hw impedance

This command sets a line impedance value for the FXO port(s).

Syntax

config voice fxo hw impedance [automatic 600|900|270+750_150nF|220+820_120nF|370+620_310nF|320+1150_230nF|370+820_110nF|275+780_115nF|120+820_110nF|350+1000_210nF|200+680_100nF|600_2.16uF|900_1uF|900_2.16uF|600_1uF] **acim** *<value>* **hyb1-8** *<filter>*

Parameters

impedance automatic|600|900|600_1uF|900_2.16uF|270+750_150nF|220+820_120nF|370+620_310nF|320+1150_230nF|370+820_110nF|275+780_115nF|120+820_110nF|350+1000_210nF|200+680_100nF|600_2.16uF|900_1uF|900_2.16uF|600_1uF

Enter the impedance. It overrides the settings of the line(s). The default is automatic.

acim *value*

Specify an AC impedance register (customizing impedance only). The value refers to an AC line termination. The default value is **11** (600 W + 2.16 mF).

hyb1-8 *filter*

Specify a hybrid filter. Eight hybrid filters are provided (for customizing impedance only). Valid values are 0 - 255. The default value for each filter is **0**.

Example

```
> config voice fxo hw impedance automatic
```

Related commands

```
show voice fxo hw impedance
display voice fxo hw impedance
```

voice fxs gain

This command sets the DSP gain values for the FXS port on a BSGX4e.

Syntax

config voice fxs gain tx *<value>* **rx** *<value>*

Parameters

tx *value*	Enter the transmit (tx) gain (digital to analog conversion) in decibels. Specify a minus (-) before a negative value. The default is **-6** dB.
rx *value*	Enter the receive (rx) gain (analog to digital conversion) in decibels. Specify a minus (-) before a negative value. The default is **-6** dB.

Example

```
> config voice fxs gain tx -6 rx -6
```

Related commands

```
show voice fxo gain
display voice fxo gain
```

voice fxs hw impedance

This command sets a line impedance value for the FXS port on a BSGX4e.

Syntax

config voice fxs hw impedance
[automatic|600|900|600_1uF|900_2.16uF|270+750_150nF|220+820_120nF|220+820_115nF|200+680_100nF]

Parameters

impedance automatic|600|900|600_1uF|900_2.16uF|270+750_150nF|220+820_120nF|220+820_115nF|200+680_100nF

Enter the impedance. It overrides the settings of the line. The default is **automatic**.

Example

```
> config voice fxs hw impedance automatic
```

Related commands

show voice fxs hw impedance
display voice fxs hw impedance

voice fxs ring pattern

This command modifies ring cadences for the FxS port based on eight patterns. The ring pattern is defined by series of cadences, in pairs, over a certain length of time. Each pair is configured in milliseconds with a ring-on and ring-off value. A single ring cadence can have up to four different sets of on/off periods, constituting the full pattern. Each pattern repeats until the phone goes off-hook or the call is cancelled.

The pattern ID is based on the country code configured in system info on page 160.

Syntax

config voice fxs ring pattern <*id*> **cad1** on1-off1 **cad2** on2-off2 **cad3** on3-off3 **cad4** on4-off4

Parameters

pattern *id*	Enter a pattern identification number based upon a specified country. The valid range is 1-8.
cad1 on1-off1	Enter the number of millisecond for ringing and silence. On1 represents ringing. Off1 represents silence.
cad2 on2-off2	Enter the number of millisecond for ringing and silence. On2 represents ringing. Off2 represents silence.
cad3 on3-off3	Enter the number of millisecond for ringing and silence. On3 represents ringing. Off3 represents silence.
cad4 on4-off4	Enter the number of millisecond for ringing and silence. On4 represents ringing. Off4 represents silence.

Example

The following example configures a pattern of ringing for 1000ms and silence for 2000ms.

```
> config voice fxs ring pattern 1 cad1 1000-2000
```

Example

The following example configures a pattern of ringing for 1000 ms followed by silence for 2000 ms, ringing for 900 ms then silence for 700 ms, ringing for 600 ms then silence for 500 ms, ringing for 800 ms then silence for 100 ms.

```
> config voice fxs ring pattern 1 cad1 1000-2000 cad2 900-700
cad3 600-500 cad4 800-100
```

Related commands

```
del voice fxs ring pattern
display voice fxs ring pattern
show voice fxs ring pattern
```

voice jitterbuffer

Use this command to configure voice playout jitter buffer setting for the SIP or MGCP gateway (User Agent).

Syntax

config voice jitterbuffer mode [fixed|adaptive] **maximum** <ms> **nominal** <ms> **minimum** <ms>

Parameters

mode fixed|adaptive

Enter the jitter buffer type. The default is **adaptive**.

maximum *ms*

Enter the maximum delay introduced by the jitter buffer, in milliseconds. This value is used only if the mode is **adaptive**. The default value is **120** ms.

nominal *ms*

Enter the nominal delay introduced by the jitter buffer, in milliseconds. The default is **40** ms.

minimum *ms*

Enter the minimum delay introduced by the jitter buffer, in milliseconds. This value is used only if the mode is **adaptive**. The default value is **20** ms.

Example

```
> config voice jitterbuffer mode fixed nominal 60
```

Related commands

```
show voice jitterbuffer
display voice jitterbuffer
stats voice jitterbuffer
```

voice np

When an analog device, such as a phone, is connected to the FxS port on the BSGX4e, a numbering plan can be needed to make full use of the features of the device. The SIP integrated gateway uses a numbering plan to interpret any string entered.

The plan is a series of entries, each defining how a specific string is to be interpreted. When the gateway receives a string from the analog device, it compares the string to the entries in the numbering plan and translates it as needed before the string is sent to the server.

For service codes, the digits dialed are sent without modification.

Every service request entry must end with a hash character [#] to activate the service. For example, if the Do Not Disturb code is set to *78, then an entry to activate Do Not Disturb for a phone is *78#.

For phone numbers, the string of digits can be translated as follows:

- A number of digits can be stripped from the beginning of the number.
- A string of digits can be prepended to the beginning of the number.

Note: Before the numbering plan is configured, the SIP gateway must be configured.

This command is applicable to the SIP UA only.

Syntax

config voice np *<number>* **type** [number|service] **feature** [None|SDND|CDND|SFWA|CFWA|SFWB|CFWB|SFWNA|CFWNA|BXFER] **length** *<number>* **stripcount** *<digits>* **prepend** *<digits>*

Parameters

number	Enter a string translated by the entry.
type number|service	Indicate whether the entry type is for a number or a service code.
Feature	
none	No feature type.
SDND	Set Do Not Disturb. Applicable only if type parameter is set to service.
CDND	Clear Do Not Disturb. Applicable only if type parameter is set to service.
SFWA	Set Forward All. Applicable only if type parameter is set to service.
CFWA	Clear Forward All. Applicable only if type parameter is set to service.
SFWB	Set Forward on Busy. Applicable only if type parameter is set to service.
CFWB	Clear Forward on Busy. Applicable only if type parameter is set to service.
SFWNA	Set Forward No Answer. Applicable only if type parameter is set to service.

CFWNA	Clear Forward No Answer. Applicable only if type parameter is set to service.
BXFER	Blind Transfer. Transfers a call and disconnects your line. Applicable only if type parameter is set to service.
length *number*	Enter the expected length of the phone numbers. Applicable only if type parameter is set to number.
stripcount *digits*	Enter the number of digits to strip from the beginning of the numbers. Applicable only if type parameter is set to number.
prepend *digits*	Enter the numbers of digits to prepend to the beginning of the numbers. Applicable only if type parameter is set to number.

Example

```
> config voice np 90 type service feature BXFER
```

Related commands

```
delete voice np
display voice np
show voice np
```

voice tones

Use this command to configure tone types for the FxS port. Each tone type is assigned cadence, frequency, and level values. Available tones are:

- dial tone
- call waiting tone 1
- ringback tone
- call waiting tone 2
- busy tone
- reorder tone
- congestion tone
- stutter dial tone
- test tone
- off hook warning tone

Syntax

config voice tone [dial|ringback|busy|congestion|callwait1|callwait2|reorder|stutter|offhookwarn|test] **on1** <cadence> **off1** *<cadence>* **on2** *<cadence>* **off2** <cadence> **freq1** <freq> **level1** <level> **freq2** <freq> **level2** <level>

Parameters

tone dial|ringback|busy|congestion|callwait1|callwait2|reorder|stutter|offhookwarn|test

Enter the tone type to be reconfigured. This parameter is mandatory.

on1 *cadence*
off1 *cadence*

Define the first ringing cadence (in ms).

on2 *cadence*
off2 *cadence*

Define the second ringing cadence (in ms).

freq1 *freq*
level1 *level*

Define the first frequency (in Hz) and level (in db). Level is defined in db.

freq2 *freq*
level2 *level*

Define the second frequency (in Hz) and level (in db). Level is defined in db.

Examples

Use the following commands to re-define various tone types, frequency and level values for the call progress tones:

```
> config voice tones dial on1 500 off1 0 on2 0 off2 0 freq1
425 level1 -10 freq2 0 level2 0

> config voice tones ringback on1 1000 off1 4000 on2 0 off2 0
freq1 425 level1 -10 freq2 0 level2 0

> config voice tones busy on1 330 off1 330 on2 0 off2 0 freq1
425 level1 -10 freq2 0 level2 0
```

```
> config voice tones congestion on1 150 off1 150 on2 0 off2 0
freq1 425 level1 -10 freq2 0 level2 0

> config voice tones callwait1 on1 200 off1 5000 on2 0 off2 0
freq1 425 level1 -10 freq2 0 level2 0

> config voice tones callwait2 on1 100 off1 1000 on2 0 off2 0
freq1 425 level1 -10 freq2 0 level2 0

> config voice tones reorder on1 250 off1 250 on2 0 off2 0
freq1 425 level1 -10 freq2 0 level2 0

> config voice tones stutter on1 400 off1 40 on2 0 off2 0
freq1 425 level1 -10 freq2 0 level2 0

> config voice tones test on1 500 off1 0 on2 0 off2 0 freq1
1000 level1 -10 freq2 0 level2 0
```

Related commands

```
delete voice tones
display voice tones
show voice tones
show sip ua port
```