Release 1.2
Release Bulletin

BSGX4e
Business Services Gateway

NN47928-401
Software Release 2.1.1

BSGX4e 1.2
Business Services Gateway

Document Status: **Standard**

Document Version: **01.01**

Document Number: **NN47928-401**

Date: **July 2008**

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

Trademarks

Contents

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:

http://www.nortel.com/support

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

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

Getting help over the phone from a Nortel Solutions Center

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

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

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

http://www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

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

http://www.nortel.com/erc

Getting help through a Nortel distributor or reseller

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

INTRODUCTION

This document makes recommendations about the deployment of the Business Services Gateway X4e (BSGX4e), release 1.2, GA Candidate build 2.1.1-02. This document provides the following information:

WARNING: Before working on this equipment, be aware of good safety practices and the hazards involved with electrical circuits.

WARNING: To reduce risk of injury, fire hazard, and electric shock, do not install the unit near a damp location.

CAUTION: Do not connect the PHONE port to the central office line.

CAUTION: To reduce the risk of fire, use only number 26 AWG or larger UL Listed or CSA Certified telecommunication line cord for all network and telecommunication connections.

INTEROPERABILITY

The BSGX4e is designed to interoperate with all standards-compliant SIP, MGCP, and VPN devices.

SIP Softswitch

- Nortel CS2000 (vSN09U)

SIP Terminals

- LG 6812 (v1.2.41sc)
- LG 6804 (v1.2.41sc)
- LG 6830 (v1.2.41sc)
- Multi-media PC Client Softphone (v4.1.665 (20071028))

SIP Servers

- Ericsson IMT (v3.0)
- Sylantro SIP Application Server (v3.2.1)
- Sylantro SIP Application Server (v4.0)
- Broadsoft (v13)
- Broadsoft (v14)
- CS2K SIP Application Server (SN09FF)

SIP Clients

- Cisco 7940/7960 SIP phones (P0S3-07-5-00 and P0S3-08-8-00)
- Cisco ATA 186 (v3.02.01)
- Polycom IP600 (v 2.1.2.0078)
- EyeBeam soft phone (v1.5)
- Nortel/LG LIP-6812 and LIP-6830 phones (v1.2.17s and v1.2.41sc)
- Snom 320/360 (v6.5.12)
- Linksys SPA 941/942 (v5.1.15(a))
- Aastra 480i (v1.4.0.1048)
- Mediatrix 110x (v5)
- Mediatrix 1204 (v5)
- Audiocode MP-114 (v5)
- GrandStream video phone (v1.0.1.20)
- Innomedia video phone (v2.3.7bGEN)

MGCP Servers

- Sylantro MGCP Call Agent (v3.2.1)
- Sylantro MGCP Call Agent (v4.0)

MGCP Clients

- Cisco 7940/7960 MGCP phones (P0M3-07-5-00 and P0M3-07-6-00)
- Cisco ATA 186 (v3.1.1)
- SwissVoice IP10S (v104b3)

VPN Devices

- Cisco 3845 IOS 12.4
- Cisco ASA5510 v7.2(2)

New Features and Functionality

The following changes are included in software release R2.1.1-02.

Table 1 Summary of changes

Type	Defect number	Description
New feature	N/A	Routing: Proxy ARP
	N/A	QoS: Downstream QoS
	N/A	Security: PPTP ALG
	N/A	Session controller: SIP trunking (SIP Connect) SIP forking SIP Shared Line Appearance (SLA) Full support for SIP based video calls Relaying of SIP messages with unknown content type Emergency calls via FxO in connected mode (not in survival mode, SIP only) Heartbeat mode to monitor the connection to the VoIP server (SIP only)
	N/A	User agent: Multi-line support (SIP only) Voice Activation Detection
	N/A	Services: Dynamic DNS Enhanced DHCP server to provide more flexibility for deployments
	N/A	Management: Initial Configuration Wizard
	N/A	User Agent and Session Controller: Localization settings per country (ring tones, ring cadences, and emergency numbers)
Enhancements	N/A	PPPoE: PPPoE user name now supports up to 64 characters.

Table 1 Summary of changes

Type	Defect number	Description
	N/A	NAT: You can configure public IP addresses out of the IP subnets of the WAN interfaces of the BSGX4e.
	N/A	DHCP server: DHCP option 66 now supports provisioning with FQDN addresses. DHCP options 150, 151, 160, and 161 now support provisioning with FQDN addresses and URLs.
	N/A	QoS: You can protect SIP based multimedia traffic other than voice and video.
	N/A	Session Controller: You can configure the softswitch type (“Sylantro”, “Broadsoft”, “Siemens”, or “other”) with which the Session Controller interoperates. You can configure the SIP forking support of the Session Controller to be activated or deactivated.
Bug fixes	Q01594121	Unknown Error pops up when configuring VPN IKE preshared key .

Table 1 Summary of changes

Type	Defect number	Description
	Q01595084	Cannot clear specified IKE SAs currently negotiated from CLI.
	Q01595089	Cannot clear specified IPSec SAs currently negotiated by CLI.
	Q01595880-01	SNMP traps "Linkup" and "LinkDown" are not sent by BSGX4e.
	Q01596505	BSGX4e: PPP and Eth0 with DHCP set to YES.
	Q01597647	Upgrade a wrong format FW load cannot be prevented in WebUI.
	Q01597676	Cannot create multiple PPP profiles by using WebUI. Note: the “new” button has been replaced by a “refresh” button.
	Q01597755	Modifying SNTP Parameters on Web UI results in message "Error Deleting Server 1".
	Q01611233	In WebUI, ESP Statistics is wrong.
	Q01611291	BSG cannot stick to Survival mode.
	Q01611316	Web/ CLI Display for Redirect Port (rport) NAT Policy is truncated to 16 characters.
	Q01611380	VAMP Test Failures.
	Q01611386	Web UI allows incorrect configuration for redirect Port NAT Security Policy.

Table 1 Summary of changes

Type	Defect number	Description
	Q01612478	Shouldn't allow select "any" for local and remote networks in Wizard VPN config.
	Q01612667	2nd phone registered with the same user kicks out the first phone. Note: this has been solved by introducing the new SIP forking support of the SIP SC.
	Q01614495	Active Sip Server is removed under SIP Control when unused SIP Server is deleted.
	Q01616011	Link Status of PPPoE cannot be updated automatically in WebUI.
	Q01618790	BSG filter out Video information in SDP. Note: this problem has been solved by introducing the new Video support of the SIP SC.
	Q01622434	TFTP and Filename Fields cannot be deleted from DHCP Pool.
	Q01622766	GoS Link Drop Down List incorrectly displays PPPoE interface.
	Q01622784	DHCP Server Options 150, 152, 160, 161 on BSGX4e do not get sent to DHCP client.
	Q01640144	Polycom DHCP Clients do not receive SNTP Parameter from BSGx4e DHCP Server Pool.
	Q01641317	SIP server profile is accepted without mandatory parameter.
	Q01641411	Cannot delete user account in WebUI.
	Q01644727	BSGX4e: two phones call forwarded from Call server only ring one phone.
	Q01658119	Screen width limited on some versions of Internet Explorer.
	Q01658122	Timed Log-out Made After Changes Implemented.
	Q01667997	BSGX4e - Citel interop - wrong contact in registration response.
	Q01668127	Incorrect Instructions on DHCP Server Web Page.
	Q01668131	Operation of DHCP Server Sensitive to Change Order.
	Q01668136	SIP User Agent Password Case Changes Don't Work.

Table 1 Summary of changes

Type	Defect number	Description
	Q01668201	Simplify PPPoE configuration. Note: this problem has been solved by introducing the new Initial Configuration Wizard. It has to be used to simply configure PPPoE.
	Q01668204	Simplify LAN subnet change. Note: this problem has been solved by introducing the new Initial Configuration Wizard. It has to be used to simply change the LAN subnet.
	Q01668621	BSGx4e: web server not visible from LAN side of router. Note: to support this scenario work the following security policy has to be created: from <LAN interface> to <WAN interface> dip <public IP address> dport <public port> proto <Protocol> nat <NAT id> The NAT policy must be: type rport address <private IP address> port <private port>
	Q01671421	Unit Crashes Under Complex Stress Conditions.
	Q01672352	Corrupted Firmware Version Displayed.
	Q01674220	Cannot select an IPSEC Proposal in WebUI to configure a VPN tunnel.
	Q01676241	Ridiculous security policies to support IPSec protocol are generated.
	Q01676250	DHCP Server and LAN DHCP Client must not be On at same time.
	Q01680036	CDND on BSG doesn't work with analog phone.
	Q01721368	FXS Call pickup failure with Broadsoft Server - FXS returns Busy Tone.
	Q01729902	Non-Basic features With MCS Client.
	Q01800388	Accept A String For DHCP Option Values 150, 151, 160, and 161.
	Q01851672	Intermittently no speech path on LAN-To-LAN call with LG set.
	Q01868829	BSG4: BSG4 to BSG8 IM fails when using different domain names.
	Q01870791	BSG4: BSG4 denies RTP media to be external for intra BSG calls; causes LI failure.

Table 1 Summary of changes

Type	Defect number	Description
	Q01878295	BSGX4e-The call which is established bw WAN phone and FXS is 1 way after 4s.
	Q01879311	BSG4: PCC behind BSG not logged out when new PCC logs in using same ID.
	Q01891749	BSG4 crashes when DTMF tones played from LG or PCC to FXS SIP UA.

USER NOTES

Table 2 User notes

Area	Description
Switching	When the switch is configured with VLAN (config switch vlan), use Vifx interfaces instead of the eth1 interface.
	It is not possible to configure the Ethernet parameters (speed, mode, flow control) of the LAN interface eth1. It is forced to 100FULL/no flow control because it internally interfaces the 4 ports switch. The ports of the switch are configured by default to be in auto-negotiation mode. All 10/100 Mbps, half/full duplex mode, flow control on/off combinations are supported.
	When configured on WAN, a VLAN interface is forced to transmit and receive VLAN-tagged frames.
PPP	To configure the BSG4e for PPPoE operation using the GUI, do the following: • In Data>WAN>PPP, create a new interface. Set Active to yes and fill in the account information. • In Data>Interfaces>IP, modify eth0, and set DHCP to off. • In Data>WAN>PPP, confirm that the link status is Up. • Add firewall and NAT Entries • In Security>Policy, add a new static policy • Enter a policy from eth1 to ppp0, with all other all values as default • In Security>NAT, add a new NAT Interface. Set the interface to ppp0 and the status to on.
	In order to enable PPPoE, DHCP must be turned off on the WAN (eth0) interface. This is configured under Data>Interfaces>IP in the GUI.
Routing	Eth0 and virtual interfaces (VLAN, VPN, PPP) defined on top of eth0 must always be WAN interfaces. Eth1 and virtual interfaces (VLAN) defined on top of eth1 must always be LAN interfaces.

Table 2 User notes

Area	**Description**
	To change the LAN subnet using the GUI: • Under Data>Interfaces>IP, modify the LAN interface (eth1), and change IP address mask to a value that encompasses both current and new subnets, but doesn't overlap the WAN subnet. • For example, if you are changing from 192.168.1.x to 192.168.4.x, change the subnet mask to 255.255.0.0. • Under System>DHCP Server, modify the LAN interface, and change the DHCP server address range and subnet mask to the desired subnet. • Under Data>Interfaces>IP, modify the LAN interface, change the IP address mask to the proper value (255.255.255.0). • Unplug, and reconnect the PC to get a new address in the new subnet.
	When Proxy ARP is configured, VoIP endpoints must not be located in the LAN side of the router for which Proxy ARP has been enabled. They have to be directly attached to the LAN side of the BSGX4e. A typical deployment is to set-up two VLANs over eth1, one for the VoIP endpoints, one for the router.
	If devices in the LAN side of the BSGX4e and devices in the LAN side of the router for which Proxy ARP has been enabled have to communicate, appropriate routes have to be set-up. The first ones must have the LAN IP address of the BSGX4e as gateway. The latter ones must be directed to the WAN IP address of the BSGX4e.
	Disabling the detection of IP fragment too short may be required to interoperate with equipment sending the last fragments (which are likely short) before the first ones (which are likely large). This is done with “config ids anomaly fragtooshort active no”.
Security	Firewall is always enabled. It cannot be disabled. By default, the Firewall rejects traffic. When a VLAN or PPPoE interface is created, Firewall policies must be added to allow traffic.
	The BSGX4e is mainly intended to be deployed with NAT enabled. WAN interface(s) must be set as “untrusted” for spoofing.
	LAN interface(s) should be set as “trusted” for spoofing.

Table 2 User notes

Area	Description
VPN	When setting up a Branch Office Tunnel, the firewall must be set up to allow IKE negotiation, ESP packets, and tunnelling of traffic. This is done automatically if the Branch Office Tunnel is established using the Wizard. For manually configured tunnels, configure the following in the firewall: • Create a policy allowing all traffic from eth1 to vpn0. • Create a policy allowing UDP traffic on port 500 from 'eth0' or 'ppp0' (in the case of PPPoE connections) to 'self'. • Create a policy allowing ESP traffic 'eth0' or 'ppp0' to 'self'.
	Negotiation capabilities of the Branch Office Tunnels are summarized as follows: • IKE encryptions for phase 2 negotiation can be DES (56), 3DES (168), AES (128, 192 and 256) or BLOWFISH (128). They are all offered during the IKE negotiation. • IKE authentications for phase 2 negotiation can be SHA (96) or MD5 (96). They are all offered during the IKE negotiation. • IPSec encryptions supported are 3DES (168) or AES (128, 192 and 256). • IPSec authentications supported are SHA (96) or MD5 (96).
	Routing to the tunnel is based on the routing table and not on IPSec policies. IPSec policies are only used for IKE phase 2 negotiations. Traffic is decrypted based on the ingress interface (it must be a VPN interface) and not on IPSec policies. IPSec policies are only used for IKE phase 2 negotiations.
Session controller	The Session Controllers are supposed to work with a single server (SIP proxy or MGCP call agent) at a time. They don't support redirection to other servers.
	In topology 3, Direct Media must be enabled on the main site to avoid calls between remote sites from being routed by the main site. In topology 3, to avoid remote sites from switching to LCR mode when the SIP server goes down, the "retries" parameter in the "SIP server setting" should be set to a higher value on the remote site than on the main site. By default, this value is set to 4; it should be set to a higher value (6 for example) on the remote site.

Table 2 User notes

Area	**Description**
	The CAC (Call Admission Control) algorithm of the SC is the following: • During the starting of a call, the maximum possible bandwidth is allocated, that is the one for G.711 10ms. • After negotiation of the CODEC type (SDP protocol), the allocation is adjusted to the maximum possible bandwidth for this CODEC. • When the RTP stream starts, the bandwidth allocation is adjusted based on the packet time observed. Example: SIP call over WAN Ethernet: • When an INVITE message is received the SC allocates 126400 bps (100 pps x 158 bytes x 8 bits), corresponding to a G.711 10ms CODEC. • When the 200 OK is received, say to use G.729a CODEC, the SC adjusts the bandwidth to G.729a 10 ms, 70400 bps (100 pps x 88 bytes x 8 bits). • When the media is started, say it is G.729a 20ms, the SC adjusts the bandwidth to 39200 bps (50 pps x 98 bytes x 8 bits). To use as much bandwidth as there is, when the remaining bandwidth doesn't allow to make a G.711 10ms call (the CAC would reject it if we strictly follow the algorithm above), the G.711 CODEC, if present, is removed from the SDP body before relaying the SDP offers (so to prevent the call to be established with it) and the CAC allocates the maximum bandwidth that could be used by the remaining CODECs. The limitations of this algorithm are: • Endpoints must not change the payload type without renegotiating it through signalling. • Since every call requires to initially reserving the maximum possible bandwidth (126400 bps), calls cannot be established at a too high rate since it takes time for the CAC to adjust the bandwidth allocations (i.e. it has to wait for the end of the SDP negotiation).
	If the SIP VoIP server is reachable through a VPN tunnel, you should enable heartbeat mode to rapidly detect the server is up after the tunnel is up (during the negotiation of a VPN tunnel, which can take a while, the Session Controller could state the VoIP server is down).
	Mechanisms such as STUN (Session Traversal Utilities for NAT) or ICE (Interactive Connectivity Establishment) for crossing NAT/Firewall devices must be disabled on VoIP terminals located on the LAN side of the BSGX4e.

Table 2 User notes

Area	**Description**
Legacy telephony & User Agent	When a CODEC is configured as not used, it indicates the end of the preferred CODEC list. Subsequent CODEC(s) will be ignored. If CODEC1 is set to 'Not Used', no CODEC is included in SDP offers.
	To use the User Agent for Fax only, you should set the FAX parameter to "On".
SIP	SIP signalling is supported over UDP only.
	In order to enable or disable SIP forking support or to change the softswitch type, ensure that no SIP endpoints are registered through the SIP SC (they can be listed by using the command "show sip sc endpoints"). If SIP endpoints are registered they have to be de-registered prior to make the change.
	Forwarding features (all, no answer, on busy) invoked through BSGX4e User Agent's dial plan do not work with some back-to-back user agents (such as Sylantro 4.0). This is because they remove the contact header required by the caller to initiate a new call.
MGCP	MGCP phones and gateways located in LAN (including the MGCP User Agent) must be identified by MAC address (i.e. the right side of their identifier must be their MAC address).

Table 2 User notes

Area	Description
QoS	Layer 2 QoS is mainly intended to be used to manage the bandwidth of the LAN switch uplink port, which operates at 100 Mbps while the offered load can be 400 Mbps (4 x 100 Mbps) from the four FE LAN ports. Layer 3 QoS (GoS) is mainly intended to be used to manage the bandwidth of the physical WAN interface.
	To set up QoS for Voice using the GUI: • Determine your upstream bandwidth using a third-party web site. Examples are http://myvoipspeed.visualware.com/ and http://www.speakeasy.net/speedtest/. Take multiple readings and average results. • Enable QoS for the WAN interface. In Quality>Link, add a new interface. Select the interface (eth0) and enter the upstream bandwidth. • Define a QoS group for voice traffic. In Quality>Group, add a new interface for VoIP. Enter the required bandwidth based on the number of consecutive calls, codec, and delay.
	To set up QoS for other traffic using the GUI: • Determine upstream bandwidth and configure the WAN link as per 'QoS for Voice' above. • Define the guaranteed and maximum bandwidth. In Quality>Group, add a new interface. Enter the guaranteed and maximum bandwidths, with type 'car'. • Define the user/service that the bandwidth is reserved for. In Security>Policy, add a new interface. Enter a descriptive name, a source of eth1, and a destination of eth0. Enter the criteria to recognize the traffic (address, port, protocol). Select the QoS profile defined above.

Table 2 User notes

Area	Description
	To assure low delay and packet loss for VoIP traffic: • Layer 2 QoS should be configured with a strict priority queuing mechanism (rather than a weighted round robin queuing mechanism). • Layer 3 QoS Quality Groups should be of type POLICED (rather than type CAR).
	Layer 3 QoS rates should account for the 14 bytes Ethernet overhead of the WAN interface. It doesn't need to account for the Ethernet FCS (4 bytes), preamble (8 bytes) or inter frame (12 bytes). Layer 3 QoS should account for the VLAN overhead if traffic is VLAN encapsulated, the PPP overhead if traffic is PPP encapsulated, and the VPN overhead if traffic is tunnelled.
	You should protect ARP traffic when QoS is deployed using the command "config protocol arp". You should protect PPP traffic when QoS is deployed over PPP using the command "config protocol ppp". Video traffic must be protected using a Quality Group named "video" (lower case).
	Multimedia traffic other than voice and video must be protected using a Quality Group named "appqos" (lower case).
	If traffic is coming into the WAN and is intended to be routed to a router in the LAN for which Proxy ARP is enabled, it has to be protected by Downstream QoS. A security policy has to be manually configured as follows (even if this traffic is already protected for the upstream direction through a Quality Group set with the downstream option to yes): "from <WAN interface> to <LAN interface> dip <IP address of the router> action allow qos <QoS group>" where <QoS group> is set with the downstream option to yes.

Table 2 User notes

Area	Description
Services	The DHCP server is mainly intended to be used to manage IP addresses on LAN.
	By default the DHCP server is enabled on eth1 for IP range 192.168.1.2-192.168.1.127.
	The DHCP client is mainly intended to be used to automatically configure the WAN interface(s) of the BSGX4e.
	You should separately configure the firewall to allow access for the desired services: • If a Telnet client wants to reach the BSGX4e from the WAN, a policy must be correctly configured in the Firewall to allow it. • If a SSH/SFTP client wants to reach the BSGX4e from the WAN, a policy must be correctly configured in the Firewall to allow it. • If a traceroute needs to be originated from the BSGX4e to the WAN, you must configure a policy in the Firewall to allow ICMP traffic coming from WAN to be processed.
	The SSH/SFTP server of the BSGX4e works with SSHv2 clients only.
	For the relay functions, it is assumed that the servers (DHCP, TFTP, DNS, NTP) are located on the WAN and the clients are located on the LAN (typically VoIP phones).
	The SNTP Client needs to be disabled before the SNTP Server address can be changed.
Monitoring	The rates reported by PMON and Netflow take into account the IP header and payload only.
	The Tcpdump feature should be used for troubleshooting purposes only since it significantly impacts the performances of the BSGX4e.
	Only SNMP v2c is supported.
	In order for an SNMP client to reach the SNMP agent of the BSGX4e from the WAN, a policy must be correctly configured in the Firewall to allow it.
Management	In order for a Web client (HTTP or HTTPS) to reach the BSGX4e from the WAN, a policy must be correctly configured in the Firewall to allow it.
	Audit logs can theoretically fill the entire compact flash (although this would require a long time). If it happens the user should remove the older logs located in /cf0usr/Audit.

Recommendations for Deployment

Table 3 Recommendations for Deployment

<table>
<tr><th>Area</th><th>Description</th></tr>
<tr><td>Switching</td><td>You cannot configure the Ethernet parameters (speed, mode, and flow control) of the LAN interface eth1. It is forced to 100FULL/no flow control because it internally interfaces with the 4 ports switch. The default setting of the ports of the switch is auto-negotiation mode. All 10/100 Mbps, half/full duplex mode, and flow control on/off combinations are supported.</td></tr>
<tr><td></td><td>When configured on the WAN, a VLAN interface is forced to transmit and receive VLAN-tagged frames.</td></tr>
<tr><td>PPP</td><td>On the BSGX4e, eth0 must be configured with DHCP turned off in order to create a PPP over Ethernet interface.</td></tr>
<tr><td></td><td>The format of IP over PPPoHDLC packets is described in RFC 1662, chapter 3.1 (Protocol and FCS are of 2 bytes):
+----------+----------+----------+
| Flag | Address | Control |
| 01111110 | 11111111 | 00000011 |
+----------+----------+----------+
+----------+-------------+---------+
| Protocol | Information | Padding |
| 16 bits | * | * |
+----------+-------------+---------+
+----------+----------+------------------+
| FCS | Flag | Inter-frame Fill |
| 16 bits | 01111110 | or next Address |
+----------+----------+------------------+</td></tr>
</table>

Table 3 Recommendations for Deployment (continued)

Area	Description
Routing	On the BSGX4e, eth0 and virtual interfaces (VLAN, VPN, PPP) defined over eth0 must be WAN interfaces. Eth1 and virtual interfaces (VLAN) defined on top of eth1 must be LAN interfaces.
	If devices on the LAN side of the BSGX4e and devices on the LAN side of the router (for which Proxy ARP is enabled) need to communicate, you must set up appropriate routes. The first routes must have the LAN IP address of the BSGX4e as the gateway. The latter routes must be directed to the WAN IP address of the BSGX4e.
	On the BSGX4e, when the Proxy ARP is configured, VoIP endpoints must not be located on the LAN side of the router for which Proxy ARP is enabled. They have to be directly attached to the LAN side of the BSGX4e. A typical deployment is to set up two VLANs over eth1 - one for the VoIP endpoints, and the other for the router.
	Disabling the detection of IP fragment too short may be required to interoperate with equipment sending the last fragments (which are likely short) before the first ones (which are likely large). This is done with the following command: config ids anomaly fragtooshort active no.
Security	Firewall is always enabled. It cannot be disabled. By default the Firewall rejects traffic.
	When a VLAN interface is created on the LAN, no Firewall policies are automatically set up to allow traffic. By default all traffic is rejected. Firewall policies must be manually configured.
	When a VLAN, PPP, FR, or VPN interface is created on WAN, no Firewall policies are automatically set up to allow traffic. By default all traffic is rejected. Firewall policies need to be manually configured. NAT must be manually enabled, if required.
	The BSGX4e should be deployed with NAT enabled on the WAN interface.
	WAN interfaces, except VPN interfaces, must be set as untrusted, for IDS spoofing.
	LAN interfaces and VPN interfaces should be set as trusted for IDS spoofing.

Table 3 Recommendations for Deployment (continued)

Area	Description
VPN	IKE negotiation is done on UDP port 500. Main mode and preshared keys should be deployed.
	By default, all IKE packets coming in the BSGX4e are discarded by the Firewall. You must configure the Firewall to accept IKE packets.
	IKE encryptions for phase 2 negotiation can be DES (56), 3DES (168), AES (128, 192, and 256), or BLOWFISH (128). They are all offered during the IKE negotiation.
	IKE authentications for phase 2 negotiation can be SHA (96) or MD5 (96). They are both offered during the IKE negotiation.
	By default, all ESP packets coming in the BSGX4e are discarded by the Firewall. You must configure the Firewall to accept the packets.
	IPSec encryptions supported are 3DES (168) or AES (128, 192, and 256).
	IPSec authentications supported are SHA (96) or MD5 (96).
	Traffic is encrypted based on the routing table and not on IPSec policies. IPSec policies are only used for IKE phase 2 negotiations.
	Traffic is decrypted based on the ingress interface (must be a VPN interface) and not on IPSec policies. IPSec policies are only deployed.

Table 3 Recommendations for Deployment (continued)

Area	Description
QoS	Layer 2 QoS is used to manage the bandwidth of the LAN switch uplink port to CPU, which operates at 100 Mbps.
	Layer 2 QoS must be configured with a strict priority queuing mechanism (rather than a weighted round robin queuing mechanism) to protect VoIP traffic (to get the lowest delay and packet loss).
	Layer 3 QoS (GoS) is used to manage the bandwidth of the physical WAN interface (eth0 for the BSGX4e).
	On the BSGX4e, Layer 3 QoS rates take into account the full Ethernet overhead of 38 bytes (14 of header, 4 of FCS, 8 of preamble, and 12 of inter frame).
	Layer 3 QoS rates take into account the VLAN overhead if traffic is VLAN encapsulated.
	Layer 3 QoS rates take into account the PPP overhead if traffic is PPP encapsulated.
	Layer 3 QoS rates take into account the VPN overhead if traffic is tunneled.
	Layer 3 QoS Quality Groups must be of type POLICED (rather than type CAR) to protect VoIP traffic (to get the lowest delay and packet loss).
	On the BSGX4e, Nortel recommends that you protect ARP traffic when Layer 3 QoS is deployed using the command config protocol arp.
	You should protect PPP control traffic when Layer 3 QoS is deployed along with PPP (PPPoE or PPPoHDLC) using the command config protocol ppp.
	You should protect Video traffic by using a Quality Group named video (lower case).
	You should protect Multimedia traffic (other than voice and video) by using a Quality Group named appqos (lower case).
	If traffic coming into the WAN is routed to a router in the LAN for which Proxy ARP is enabled, and that traffic must be protected by Downstream QoS, a security policy must be manually configured as follows: from <WAN interface> to <LAN interface> dip <IP address of the router> action allow qos <QoS group>. The security policy must be configured even if the traffic is already protected for the upstream direction through a Quality Group set with the downstream option to yes.

Table 3 Recommendations for Deployment (continued)

Area	Description
Session Controller (SC)	The Session Controllers are always enabled. They cannot be disabled.
	The Session Controllers should work with a single server (SIP proxy or MGCP call agent) at a time. They do not support redirection to other servers.
	The CAC (Call Admission Control) algorithm of the SC is the following: - During the start of a call, the maximum possible bandwidth for G.711 10ms is allocated. - After negotiation of the CODEC type (SDP protocol), the allocation is adjusted to the maximum possible bandwidth for this CODEC. - When the RTP stream starts, the bandwidth allocation is adjusted based on the packet time observed. For example, a SIP call over WAN Ethernet: -When an INVITE message is received, the SC allocates 126400 bps (100 pps x 158 bytes x 8 bits), corresponding to a G.711 10ms CODEC. - When the 200 OK is received (for example, to use G.729a CODEC), the SC adjusts the bandwidth to G.729a 10 ms, 70400 bps (100 pps x 88 bytes x 8 bits). - When the media is started (for example, G.729a 20ms), the SC adjusts the bandwidth to 39200 bps (50 pps x 98 bytes x 8 bits). If there is not enough bandwidth left to make a G.711 10 ms call (the CAC rejects the call if the above algorithm is strictly observed), then the G.711 CODEC, if present, is removed from the SDP body before relaying the SDP offers (to prevent the call from using it) and the CAC allocates the maximum remaining bandwidth. The limitations of this algorithm are: - Endpoints must not change the payload type without renegotiating it through signalling. - Since every call initially requires the reserving of the maximum possible bandwidth (126400 bps), calls cannot be established at too high a rate since it takes time for the CAC to adjust the bandwidth allocations. For example, the CAC must wait for the end of the SDP negotiation.
	In main/branch office topologies where branch offices make VoIP calls through the main office (main office acting as VoIP server for remote offices), Direct Media (config media settings dm yes/no) should be enabled on the main site to avoid calls between remote sites being routed by the main site (to save bandwidth between branch and main offices).

Table 3 Recommendations for Deployment (continued)

Area	Description
	In main/branch office topologies where branch offices make VoIP calls through the main office (main office acting as VoIP server for remote offices), to avoid remote sites switching to survival mode when the SIP server goes down, the retries parameter in the SIP/MGCP server setting should be set to a higher value on the remote sites than on the main site. By default, this value is set to 4; it should be set to a higher value (6, for example) on the remote sites. Another solution, for the SIP SC only, is to configure heartbeat mode on the remote sites.
	If the SIP VoIP server is reachable through a VPN tunnel, you should enable heartbeat mode to rapidly detect that the server is up after the tunnel is up. (During negotiation of a VPN tunnel, which can take a while, the Session Controller could state the VoIP server is down).
	Mechanisms such as STUN (Session Traversal Utilities for NAT) or ICE (Interactive Connectivity Establishment) for crossing NAT/Firewall devices must be disabled on VoIP terminals located on the LAN side of the BSGX4e.
Legacy Telephone and User Agent (UA)	A CODEC configured as NOTUSED indicates the end of the preferred CODEC list. Subsequent CODEC or CODECs are ignored. If CODEC1 is set to NOTUSED, no CODEC is included in SDP offers.
	To use the UA for fax only, you should set the FAX parameter to On (SIP), CC_ON (MGCP).
SIP	SIP signaling is supported over UDP only.
	Prior to enabling or disabling SIP forking or to changing the softswitch type, you must ensure that no SIP endpoints are registered through the SIP SC. (You can list them by using the command show sip sc endpoints). If there are registered SIP endpoints, they have to be un-registered.
	On the BSGX4e, when deployed with Ericsson IMT 3.0, the SIP UA must be set to IAD/Gateway (SIP generic Std) through the portal, if MLS is set to RFC 2976. You must set the SIP US to IP phone, if MLS is set to RFC 3264.
	On the BSGX4e, forwarding features (all, no answer, and on busy) invoked through BSGX4e UA dial plan, do not work with some Back to Back UAs (such as Sylantro 4.0) when they remove the contact header required by the caller to initiate a new call with the desired party.

Table 3 Recommendations for Deployment (continued)

Area	Description
MGCP	MGCP phones and gateways located in LAN (including the MGCP UA on BSGX4e) must be identified by MAC address. For example, the right side of the identifier must be the MAC address.
Services	You should use the DHCP server to manage IP addresses on LAN side.
	By default, the DHCP server is enabled on eth1 for IP range 192.168.1.2-192.168.1.127.
	You should use the DHCP client to automatically configure the WAN interface or interfaces of the BSGX4e.
	If a Telnet client must reach the BSGX4e from the WAN, you must configure a policy in the Firewall to allow it.
	The SSH/SFTP server of the BSGX4e works with SSHv2 clients only.
	If an SSH/SFTP client must reach the BSGX4e from the WAN, you must configure a policy in the Firewall to allow it.
	For the relay functions, the servers (DHCP, TFTP, DNS, NTP) should be located on the WAN and the clients should be located on the LAN (typically VoIP phones).
	If a traceroute must originate from the BSGX4e to the WAN, you must configure a policy in the Firewall to allow the firewall to process ICMP traffic coming in from the WAN.
Monitoring	Tcpdump must be used for troubleshooting purposes only since it significantly impacts the performances of the BSGX4e.
	Only SNMP v2c is supported.
	If a SNMP client must reach the SNMP agent of the BSGX4e from the WAN, you must configure a policy in the Firewall to allow it.
	Netflow versions 1, 5, and 9 are supported.
Management	If a Web client (HTTP or HTTPS) must reach the BSGX4e from the WAN, you must configure a policy in the Firewall to allow it.
	It is possible for Audit logs to fill the entire compact flash (although this would occur over a long period of time). If this happens, the user must remove the older logs located in /cf0usr/Audit.

Notable Limitations

Table 4 Notable Limitations

Area	Description
Switching	It is not possible to mirror only the ingress direction of a port.
	The maximum number of MAC addresses that can be learned by the LAN switch is 1024.
	It is not possible to individually remove static MAC entries from the forwarding table of the switch. The entire table can be flushed.
	The maximum number of VLANs supported is 64.
	It is not possible to mirror the traffic of a port belonging to a VLAN to another port belonging to another VLAN.
PPP	A single PPP interface is supported.
	A PPP interface cannot be created on top of VLAN interfaces.
	UDP over PPP packets that are larger than the PPP interface MTU size are not correctly fragmented. They are discarded instead.
	The command stats interface ppp only reports statistics about the PPP control traffic. It does not report statistics about the PPP data traffic.
Routing	The maximum number of flows that can be routed at the same time is 2000.
	The maximum number of ARP entries is 1400.
	The maximum number of IP routes (static and dynamic) is 198.
	The maximum number of router interfaces is 16.
	All VLAN interfaces defined on the LAN side of the BSGX4e use the MAC address of eth1. All VLAN interfaces defined on the WAN side of the BSGX4e use the MAC address of eth0.
	The routing table does not support metrics.
	Multi-subnetting (for example, assigning more than one IP address to an interface) is not supported.

Table 4 Notable Limitations (continued)

Area	Description
Security	Firewall policies can't be modified. They have to be removed and re-configured.
	No statistics are available for individual Firewall policies. Statistics are available for the overall Firewall policies.
	The maximum number of Firewall policies is 128.
	Classification of traffic based on IP ToS field only works for QoS purposes. This means the parameter "iptos" of the command "config security policy" only works when the parameter "qosgp" is specified.
	The statistics concerning the IDS attacks may not appear accurate ("show ids attacks"), because only a limited number of attacks (64 per second at most) are reported to not overload the CPU.
	The maximum number of packets of size 64 bytes (including Ethernet FCS - G.729 like packets) verified by IDS is: • 90 000 pps for traffic from LAN to WAN (about 70%) • 127 000 pps for traffic from WAN to LAN (about 100%) Note GoS is enabled for LAN to WAN traffic. Over these limits, the IDS process discards packets.
	The maximum number of NAT public IP addresses is 16.
	Static NAT is not supported over a PPP interface.
	The maximum number of concurrent PPTP sessions supported by the PPTP ALG is 50.
VPN	The maximum number of VPN tunnels is 10.
	The maximum bi-directional performances for Ethernet 64 bytes packets (including FCS) for VPN, for both encryption and authentication types, and having layer 3 QoS enabled for LAN to WAN traffic, is: -30 percent of Ethernet wire speed LAN to WAN -30 percent of Ethernet wire speed for WAN to LAN Over these limits, the VPN process discards packets.
	IKE negotiation is done on port 500. It cannot be configured.
	IKE uses pre-shared keys only. CA certificates are not supported.
	IKE supports main mode only. Aggressive mode is not supported.

Table 4 Notable Limitations (continued)

Area	Description
	IKE encryptions and authentications for phase 2 negotiation cannot be configured. You cannot change the content of the offer, nor the order of the offer. It is set to: Priority Encryption Hash Group -------------------------------------- 1 3DES SHA DH1024 2 3DES SHA DH768 3 3DES MD5 DH1024 4 3DES MD5 DH768 5 AES SHA DH1024 6 AES SHA DH768 7 AES MD5 DH1024 8 AES MD5 DH768 9 DES SHA DH1024 10 DES SHA DH768 11 DES MD5 DH1024 12 DES MD5 DH768 13 BLOWFISH SHA DH1024 14 BLOWFISH SHA DH768 15 BLOWFISH MD5 DH1024 16 BLOWFISH MD5 DH768
	Only VPN tunnel mode is supported.
	Interoperability is checked with VPN capable devices such as Cisco 3845 IOS 12.4 and Cisco ASA5510 v7.2(2).
QoS	The maximum number of Quality Groups is 10.
	The maximum bi-directional performance for 64 bytes packets (including FCS), for a QoS link of 100 Mbps, is: • 70 percent of Ethernet wire speed LAN to WAN • 100 percent of Ethernet wire speed for WAN to LAN Over these limits, the Layer 3 QoS process discards packets.
	When the QoS feature is enabled for a specified interface, the burstiness of the offered load must not be higher than 35 packets sent at Ethernet wire-speed; otherwise, packets are dropped.
	Downstream QoS is designed for WAN links of 1.5 Mbps and above. Below this rate, activating downstream QoS can lead to degradation of the downstream rate.
Session Controller (SC)	The Session Controller is always enabled. It cannot be disabled.
	The maximum number of calls over one second that the unit is able to handle is 10 for SIP and 5 for MGCP.
	The Session Controllers don’t keep the states of ongoing calls in persistent memory so if the BSGX4e has to be restarted they will be lost.

Table 4 Notable Limitations (continued)

Area	Description
	The Session Controllers don’t maintain the ToS byte of signalling packets received to be relayed. They are relayed with a ToS of 0. Note for LAN to WAN traffic, QoS ToS re-writing can be used to maintain it. It cannot be maintained from WAN to LAN.
	Calls cannot be established through the Session Controllers in the case signaling and media IP addresses of LAN endpoints are different.
	CAC (Call Admission Control) for video calls, unlike CAC for voice calls and layer 3 QoS, doesn’t take into account the Ethernet, IP, UDP and RTP headers. This could lead for the CAC to accept few more voice/video calls than what’s possible to manage through the “video” quality group, so to slightly impact voice/video quality.
	The commands “show call current” and “show call history” may not report call party identifiers and numbers depending on the LAN endpoint types.
	Load balancing based on DNS-SRV weights is currently not supported.
	Only basic calls are supported in survival mode. Features such as Transfer and Conference are not supported.
	Video calls are not supported in survival mode.
	Emergency calls don’t take precedence over non emergency calls in survival mode, when they are established through the FxO interface or a local FxO gateway.

Table 4 Notable Limitations (continued)

Area	Description
SIP	Interoperability has been checked with the following servers: • Ericsson IMT (v3.0) • Sylantro SIP Application Server (v3.2.1) • Sylantro SIP Application Server (v4.0) • Broadsoft (v13) • Broadsoft (v14) • CS2K SIP Application Server (SN09U)
	Interoperability has been checked with the following clients: • Cisco 7940/7960 SIP phones (P0S3-07-5-00 and P0S3-08-8-00) • Cisco ATA 186 (v3.02.01) • Polycom IP600 (v 2.1.2.0078) • EyeBeam soft phone (v1.5) • Nortel/LG LIP-6812 & LIP-6830 phones (v1.2.17s and v1.2.41sc) • Multimedia PC Client soft phones version 4.1.665 (20071028) • Snom 320/360 (v6.5.12) • Linksys SPA 941/942 (v5.1.15(a)) • Aastra 480i (v1.4.0.1048) • Mediatrix 110x (v5) • Mediatrix 1204 (v5) • Audiocode MP-114 (v5) • GrandStream video phone (v1.0.1.20) • Innomedia video phone (v2.3.7bGEN)
	Bodies of SIP messages of unknown types can be relayed by the SIP Session Controller but without changes (i.e. especially IP addresses and FQDN addresses are not translated). It is the responsibility of the user to ensure this won't lead to any problems.
	SIP REGISTER messages including more than one "Contact" fields are relayed by the SIP Session Controller. However only the first "Contact" field is considered, the other ones are ignored.
	SIP forking does not work for LAN endpoints having the same IP address.
	SIP forking and SIP SLA are not supported in survival mode.
	SIP trunking is not supported in survival mode.
	SIP SC does not support TEL URL in Request URI.
	Multi-Line Support for the SIP UA is not supported in survival mode.
	PRACK is not supported by the SIP User Agent.

Table 4 Notable Limitations (continued)

Area	Description
Legacy Telephone and User Agent (UA)	UA services (for example, call forwarding always and do not disturb) are de-activated after reboot. You must re-register these services each time the unit is restarted.
	GR-909 metallic loop tests can be launched while the FxS port is in use. As a consequence, they disrupt the voice quality while they run. The execution time, however, is usually short.
	The UA does not send ptime parameter in SDP offers.
	Fax T.38 is not supported.
	Packet Loss Concealment (PLC) is not supported.
	Media Activity Detection (MAD) is not supported.
	Message Waiting Indicator (MWI) is not supported.
	Visual Waiting Message Indicator (VWMI) is not supported.
	Distinctive Ringing is not supported.
	The User Agent doesn’t send the ptime parameter in SDP offers.
	UA does not support different CODEC types for transmission and reception.
	VAD is not supported during three-way conference calls when media is bridged by the UA.
	It is not possible to configure the User Agent of the FxO interface of the BSGX4e. Calls can be established with G.711 or G.729 CODECs only.
	The “Hazardous Potential” and “Foreign voltage” GR-909 functions work correctly. However they can damage the FXS line interface in the case a too high voltage is injected as there is no internal over-current limitation on the FXS line interface.

Table 4 Notable Limitations (continued)

Area	Description
MGCP	Interoperability is checked with the following servers: -Sylantro MGCP Call Agent (v3.2.1) -Sylantro MGCP Call Agent (v4.0)
	Interoperability is checked with the following clients: -Cisco 7940/7960 MGCP phones (P0M3-07-5-00 and P0M3-07-6-00) -Cisco ATA 186 (v3.1.1) -SwissVoice IP10S (v104b3)
	If a sequence partially matches a Digit Map, the MGCP UA sends the sequence in a NTFY message after 4s instead of 16s as recommended in RFC 3660. This has no impact on the operations of the MGCP UA.
	Forcing emergency calls to be established through the FxO interface or interfaces in normal mode is not supported by the MGCP SC.
Services	The BSGX4e can manage a maximum of 500 leases.
	You can configure up to 4 DHCP servers.
	You can configure up to 32 groups of DHCP options.
	The DHCP server does not check if an IP address is already in use before assigning it.
	A maximum of 50 TFTP transfers can be simultaneously relayed.
	Wildcards cannot be used to identify files to be downloaded by the TFTP relay cache function.
	The DNS relay cache can contain up to 200 entries.
	A maximum of 256 DNS requests can be simultaneously relayed.
	A maximum of 256 SNTP requests can be simultaneously relayed.
	You must disable the DHCP relay before you configure it.
	The file system commands do not support wildcards.

Table 4 Notable Limitations (continued)

Area	Description
Monitoring	PMON and Netflow only monitor incoming traffic. Outgoing traffic is not monitored.
	The maximum number of flows that Netflow can monitor is 4000.
	Tcpdump monitors traffic in non-promiscuous mode only.
	Tcpdump monitors traffic of a single interface at a time.
	Tcpdump does not capture IEEE 802.1Q headers for traffic coming from LAN. As a consequence, you cannot configure tcpdump to filter traffic based on VLAN identifier for traffic coming from the LAN.
	Tcpdump does not support DNS name resolution nor does it resolve IP addresses to domain names.
	While tcpdump monitors VoIP signaling traffic, it does not monitor VoIP media traffic. For example, in RTP streams, it does not impact their quality.
	Tcpdump does not capture all packets when the offered load is too high. If the offered load is too high, the CPU can be busy preventing the user from stopping tcpdump. The CLI can appear blocked. If this occurs, the traffic should be lowered to free the CPU so it can use the CLI to stop the capture.
	All SNMP MIBs are in read-only mode, except the system group MIBs.
	The SNMP counter ipInUnknownProtos (IP group) cannot be incremented. Such packets are discarded by IDS before they reach the IP stack.
	The SNMP counter ipInAddrErrors (IP group) cannot be incremented. Such packets are discarded by IDS before they reach the IP stack.
	While the counters provided by CLI/Web (show protocol ip/icmp/udp/tcp) and SNMP (ip/icmp/udp/tcp groups) are not exactly the same, clearing one of them clears both of them.
	Video call quality is not monitored as closely as voice call quality.

Table 4 Notable Limitations (continued)

Area	Description
Management	The BSGX4e supports a maximum of 20 users and 11 groups.
	The BSGX4e supports a maximum of 98 right records.
	TACACS+ and RADIUS client implementations on the BSGX4e includes authentication for ASCII log in requests only.
	TACACS+/RADIUS authorization and TACACS+/RADIUS accounting are not implemented.
	When TACACS+ or RADIUS server are not available, no backup method of authentication (SHA) is provided. You should create a separate backup user account with SHA authentication.
	You cannot configure the parameters of the serial interface.
	The maximum CLI command length is 256 characters.
	The Web browsers supported are Microsoft Explorer v6 and Mozilla FireFox v1.5/v2.0 for Windows.
	HTTPS redirection is not supported. Either HTTP or HTTPS should be used.
	Up to five simultaneous sessions (terminal, web, telnet, or SSH) are possible.
	The user can establish a maximum of three simultaneous connections to the Telnet servers.
	The user can establish a maximum of three simultaneous connections to the SSH servers.
	The CLI and Web interfaces do not ask for confirmation when a user deletes objects (for example, interfaces, qos links, and a protocol monitoring trace).
	Level of logging per module cannot be saved.

Known Problems

Table 5 Known Problems

Area	Number	Description
Switching	5423	Connections to LAN equipment may fail in auto-negotiation mode. For example, a cable is plugged in but there is no link. When LAN equipment fails, unplug the cable or disable auto-negotiation.
Routing	1073	Under very high load with a mixture of large and small packets, up to 0.01 percent of packets can be dropped.
	3922	Packets of size superior to the MTU of the output interface are not correctly fragmented (at IP layer). You should not lower the default MTU of interfaces.
	6628, 6967, 6976	Incoming IP fragmented traffic may be abnormally discarded. Nortel recommends that you avoid the routing of IP fragmented packets by BSGX4e.
	4923	Unnumbered VPN interfaces do not work. You should not configure VPN interfaces with IP address 0.0.0.0, which is sometimes used to set unnumbered VPN interfaces.
Security	6818	When a VPN interface is created, the default MTU may be wrong (it maybe higher than what it should be). As a consequence, large packets may not be correctly tunneled. Nortel recommends that you reboot the unit after you create a VPN interface in order to have a correct default MTU value.
	8123	You cannot configure NAT public addresses if DHCP is enabled on the WAN Ethernet interface of the BSGX4e.

Table 5 Known Problems

Area	Number	Description
Session Controller (SC)	6509	SC CAC (Call Admission Control) reservations are higher than what is required if a VPN tunnel is configured on the BSGX4e to convey data traffic. SC CAC abnormally adds the VPN overhead as if VoIP calls are conveyed through the tunnel, even if they are actually not tunneled. As a consequence, this reduces the maximum number of calls possible.
	5828	SC CAC reservations are lower than what is required if the BSGX4e is configured to IEEE 802.1p tag outgoing packets (SC CAC does not take into account the IEEE 802.1p tag). As a consequence, this can slightly impact voice/video call quality.
	4138, 5887	SC CAC rejects calls between endpoints in the LAN if there is not enough bandwidth available on the WAN for two calls.
	6336	SC CAC does not release the bandwidth after a SIP UA to LAN call is established.
	5671	When a call is re-negotiated to establish a Fax pass through call, SC CAC is not correctly updated with the parameters of the new media session (G.711 clear channel). SC CAC keeps as reference the original CODEC type so makes bad bandwidth reservations.
	5681	In main/branch office topologies where branch offices make VoIP calls through the main office (main office acting as VoIP server for remote offices), SC CAC does not reserve the right amount of bandwidth for VoIP calls terminating branch offices. This may reduce the maximum number of calls possible or may slightly impact the voice/video call quality.
	5684	In main/branch office topologies where branch offices make VoIP calls through the main office (main office acting as VoIP server for remote offices), layer 3 QoS does not protect VoIP calls established between the main and branch offices if direct media is enabled on the main site.
	3454	SC can be bound to a single WAN interface. When several WAN interfaces exist (like VPN, PPP, VIF, or FR interfaces), VoIP calls can be established only through a single interface, the interface through which you can reach the VoIP server (SIP proxy or MGCP Call Agent). The SC cannot establish VoIP calls through the other interfaces.

Table 5 Known Problems

Area	Number	Description
	5774	SC does not update the registrations of the LAN endpoints (including the one of the internal UA) if the IP configuration of the WAN interface changes (when you use DHCP or PPP). As a consequence, no VoIP calls can be placed through the SC until the endpoints are re-registered with the new IP address.
	8097	ACLs to deny calls do not work for incoming calls (WAN to LAN) when they are created while the LAN VoIP endpoints are already registered through the SIP SC. They work once their registration times out.
Legacy Telephone and User Agent (UA)	8142	Display of call waiting tone configuration ("show voice tones") for Luxembourg (LU) doesn't correspond to the tone played.
	8180	Localization for Ukraine (UA) cannot be set with the CLI. It is recommended to configure it with the Web UI.
	8180	Localization for Ukraine (UA) cannot be saved.
	8508	Offhookwarn tone doesn't work as expected when Belgium (BE) is selected for localization.
	8581	Ring cadence doesn't work as expected when Portugal (PT) is selected for localization.
	8144	Localization for Estonia (EE) does not work.
	1773	The JB parameters reported in RTCP-XR messages sent by the UA is always Nominal JB size:30, Max JB Size:30 and ABS JB Size:30. It does not match the settings of the JB emulated by Voice Quality Monitoring.
SIP	8599	SIP PUBLISH messages are not relayed by SIP SC.
	6794	The command show sip sc endpoints abnormally reports an empty entry (0.0.0.0) when heartbeat mode is enabled. This does not impact the operations of the SIP SC.
	5844	The SIP SC rejects calls from Nortel/LG LIP-6812 and LIP-6830 phones if they are configured with Caller ID Blocking enabled.
	7048	The Multi-Line Support RFC 2976 of the SIP UA does not work with Ericsson IMT 3.0 if the SIP UA is busy and receives a call. The user should be notified of this call (by a bip) and should be able to answer (by flashing). This scenario does not work if the SIP UA is configured as IAD/Gateway (Generic SIP Std).

Table 5 Known Problems

Area	Number	Description
MGCP	1033	The commands *show call current* and *show call history* may report incorrect call party numbers if all the digits are not notified to the MGCP Call Agent with a single NTFY message.
Services	5792	DNS resolution takes a long time (about 45 seconds) to answer if the DNS server is unreachable. As a consequence, some applications that require DNS resolution (VPN, for example) are blocked for a short time.
	7889	DHCP server abnormally offers IP addresses configured for static DHCP hosts to DHCP clients having a MAC address different from the one specified in the static DHCP host configuration. Nortel recommends that you configure the IP addresses of the static DHCP hosts outside the IP subnets managed by the DHCP servers.
	6704	There is no protection from DHCP server assigning more than 500 leases (over the different DHCP servers). 500 leases is the maximum number of leases saved in persistent memory that can be retrieved if the unit is restarted. Nortel recommends that you manage no more than 500 leases over the different DHCP servers.

Table 5 Known Problems

Area	Number	Description
Monitoring	3984	PMON and Netflow do not report PPP overhead in byte statistics.
	6884, 6888	PMON and Netflow do not always report correct statistics for routed traffic.
	6835	PMON statistics cannot be cleared.
	2810	PMON and Netflow filters based on ToS field only work for traffic routed through the CPU. For example, these filters do not work for fast routed traffic. You should not filter traffic based on ToS field.
	6817	PMON GRE filtering is not available.
	6421	Netflow filters apply as logical OR instead of logical AND.
	6912	Tcpdump when used with -e option reports bad source and destination MAC addresses.
	6487, 3070, 6752	No detailed statistics are provided for interfaces vifx and vpnx. Only the numbers of packets/bytes transmitted and received are reported.
	5658	SNMP MIBs ifInErrors and ifOutErrors (Interface group) report incorrect values for interfaces eth0, eth1, and ppp0.
	6755	SNMP linkup/linkdown traps are not working correctly for Frame Relay and PPP interfaces. They are not always sent when LMI status gets down/up (Frame Relay) or when PPP status gets up/down (PPP).
	6823	SNMP linkup/linkdown traps are not working correctly for the virtual interfaces vifx. They are not always sent when their operational status is set to up or down.
	3868	The command *summary* page and the system status web page report a wrong number of packets routed when traffic is encrypted or decrypted. It reports double the right value.
	6433	The command *summary* page and the system status web page report no packets routed for video traffic.
	6323	The command *show media status* does not report video media usage.
	5633	VQM (Voice Quality Monitoring), at times, reports bad measurements or no measurements for complex voice scenarios (like conferences, transfers, etc.) This does not impact the operation of the calls.

Table 5 Known Problems

Area	Number	Description
Management	5286	TACACS+ client needs more than one minute to detect the TACACS+ server is unreachable or is not functioning. As a consequence, when TACACS+ is used for log in authentication, the user waits for a long time before being rejected.
	3053	When the BSGX4e is very busy, the CLI does not always echo previous commands (using the up arrow).
	6633	Configuring a login name longer than 30 characters prevents logging into the unit. Nortel recommends that you configure passwords of less than 30 characters.
	6677	Upgrading the BSGX4e with a large corrupted file (more than 10 Mbps) causes it to crash.
	7039	Command *del route table all* doesn't work correctly. It flushes dynamic routes and deactivates static routes when it should only flush static routes. Nortel recommends that you not use this command.
	6666	Static ARL entries are not saved. A work around is to automatically add them after reboot by creating system startup commands (*config system startup <index>* command, *config switch arl*, etc.).
	8159	Emergency call numbers configured with *config lcr settings* are not saved. When the unit is restarted, they are re-initialized to the default numbers of the country selected for localization (see *show system info*).

KNOWN INTEROPERABILITY ISSUES

The following are specific interoperability issues with Nortel equipment (Nortel CS2000-SN09u, LG-Nortel LIP phones, and Nortel Multimedia PC Client).

Table 6 Known interoperability issues

Area	Tracking Number	Description
Session Controller (SC)/SIP	7332	VIDEO BW should not be reserved for downstream flow only.
	7212/ Q01840553	BSGX4e does not persist with subscriptions. Any time the BSGX4e resets, subscriptions associated with SIP clients on the LAN side are lost. As a result any services that are dependant upon subscriptions (like presence) will not work until the clients renew their subscriptions.
	7413	UA on Hold doesn't ring for second call.
	Q01889662	BSG4 - CS2K interop - Directed call pickup with Barge-in fails.
	7461/ Q01840551	BW is not released when LAN phone is put on hold and CS2K doesn't provide MOH.
	7462/ Q01840552	BW is not released when EPs stop sending RTP packets and fail to generate a BYE message.
	Q01893995	BSG4 reset in dynamic DHCP environment renders phones temporarily unusable. BSG4 deployed in dynamic WAN IP address environment obtains a new IP address every time it restarts or when the current lease expires. Each new DHCP request may produces a new IP address. This renders phones behind the BSG4 unreachable after the event of BSG reset or DHCP lease expiry until the phone refreshes its registration. This problem is especially significant in Nortel CS2K and MCS environments where phones register for a period of 24 hours. The mitigation is to provision the phones to re-register for a shorter period of time.
	7490	Session Controller overwrites previously registered endpoint.
	7499/ Q01851700	BSGX4e doesn't support MESSAGE request in LCR mode.

Table 6 Known interoperability issues

Area	Tracking Number	Description
	7662	Media description stripped from SDP for low bandwidth.
	7679	CAC VIDEO bw reservation on two PCC audio calls.
	7694	Video CODECs not stripped.
	7797	LPCC call to LLG forwarded to UA hang sometimes.
	7869	SUA ignores a T.38 SDP offer instead of rejecting.
	7870	BSG4 misroutes ACK to another configured sip server.
	8216/ Q01889252/ Q01889264	SIP heartbeat doesn't bring server status back up.
	8400/ Q01840553 (item 2)	After reboot Subscription dialog is reset.
	8450	BSG4 doesn't strip off "#" at the end of the dialed numbers when routing a call in LCR mode.
	8507	SIP CANCEL message is not relayed by SIP SC when MPCC originates a call then cancels it.
	8523	SUA sometimes doesn't hear CS2K voicemail.
	8705	ACK not relayed when server domain is non-resolvable.
	Q01889970/ 8725	No gratuitous ARP sent on Ethernet interface.

Resolved Issues

Table 7 Resolved Issues

Number	Description of Issue Prior to Resolution
7212/ Q01840553	NOTIFY relayed after reboot.
8215	Lawful Interception doesn't work when parties are on the LAN side of the BSG.
8118	If the softswitch type is Siemens, the SIP forking support is automatically disabled. The value of the parameter forkingenable does not necessarily reflect this setting. Parameter forkingenable may be on when the SIP forking support is disabled.
8146	The scroll list to select the localization country of the Initial Configuration Wizard doesn't work. You must specify the country by entering the ISO 3166 code.
8180	Localization for Germany in Web UI is missing.
8137	Off hook warning tone for Austria (AT) and Belgium (BE) doesn't work as expected.
8139	Display of dial tone configuration (show voice tones) for Czech Republic (CZ) doesn't correspond to the tone played.
8143	Display of dial tone configuration (show voice tones) for Italy (IT) doesn't correspond to the tone played.
8158	Display of stutter tone configuration (show voice tones) for Germany (DE) doesn't correspond to the tone played.

Software Upgrade Procedure

BSGX4e Release 1.2 is made up of two files:

- jogware_T2_2.1.1-02.bin – This is the image of the 2.1.1-02 build.
- boot-1.1.0-03.bin – This is the image of the 1.1.0-03 bootloader associated with the 2.1.1-02 build.

These two files should be applied to the BSGX4e using the standard upgrade method.

The following recommendations apply for upgrades from R2.0.2 builds to R2.1.1 builds:

- It is recommended that the configuration be exported while running R2.0.2. This is required to support reversion to R2.0.2 (i.e. if the migration to R2.1.1 fails).
- The Ethernet preamble, inter-frame gap and FCS are taken into account for upstream QoS rate calculations in R2.1.1, not in R2.0.2. Consequently the QoS rates must be redefined after migrating. Basically rates in R2.1.1 (for QoS link and groups) have to be higher than the ones configured for R2.0.2.
- The DHCP server configuration is completely different in R2.1.1 and r2.0.2. To ensure compatibility when migrating to R2.1.1, DHCP options DNS1, DNS2, TFTP, Filename, Domain, NTP1, NTP2, time-offset, 150, 151, 160 and 161 are kept as parameters of “dhcps pool”. They are not converted in options in “dhcps option”. Note the following:Although the DHCP server is working after migrating to R2.1.1, it is recommended that a proper conversion of the options be made. If an option configured in “dhcps option” overlaps an option in “dhcps pool”, the first one takes precedence on the latter one.

The following procedure has to be applied for backward migration from R2.1.1 builds to or R2.0.2 builds:

- The unit should be rebooted with R2.0.2.
- The configuration that has been saved with R2.0.2 (see above) must be restored. Note in this case SIP/MGCP endpoint registrations may be lost (the SIP/MGCP LAN endpoints may need to be re-registered -- recommended) and DHCP leases may be lost (the LAN endpoints may need to renew their lease -- recommended).

To perform the upgrade, follow the steps below:

1. Open a web browser and enter the IP address of the BSGX4e.
2. Select Upgrade on the left side of the UI.
3. In the upper panel, select the slot in which to load the new image. Normally, this is the slot that is not currently in use. In the lower panel, the slot to boot from will be automatically detected as the slot to which the new image was loaded.
4. Use the Browse button to navigate to the image file (jogware_T2_2.1.1-02.bin) stored on your PC.
5. Click the Upgrade button. The importing process will take a few minutes. You are notified when it is finished, and then you are prompted to reboot the system.

6. If your bootloader version is less than 1.1-0-03, it should be upgraded as well. In the upper panel of the upgrade UI, select bootloader.
7. Use the Browse button to navigate to the bootloader file (boot-1.1.0-03.bin) stored on your PC.
8. Click the Upgrade button. The importing process will take a few minutes. You are notified when it is finished, and then you are prompted to reboot the system.