Dialogic®

Dialogic® BorderNet™ 4000 Session Border Controller

Product Description Document

December 2013 64-0550-06

www.dialogic.com

Copyright and Legal Notice

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Inc. and its affiliates or subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in certain safety-affecting situations. Please see http://www.dialogic.com/company/terms-of-use.aspx for more details.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Inc. at the address indicated below or on the web at *www.dialogic.com*.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 6700 de la Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.**

Dialogic, Dialogic Pro, Dialogic Blue, Veraz, Brooktrout, Diva, BorderNet, PowerMedia, ControlSwitch, I-Gate, Mobile Experience Matters, Network Fuel, Video is the New Voice, Making Innovation Thrive, Diastar, Cantata, TruFax, SwitchKit, Eiconcard, NMS Communications, SIPcontrol, Exnet, EXS, Vision, inCloud9, NaturalAccess and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Inc. and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 6700 de la Cote-de-Liesse Road, Suite 100, Borough of Saint-Laurent, Montreal, Quebec, Canada H4T 2B5. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Table of Contents

Revision History

Revision	Release date	Notes
64-0550-06	December 2013	Release 3.2
64-0550-05	June 2013	Release 3.1
64-0550-04	January 2013	Release 3.0
64-0550-03	September 2012	Release 2.1
64-0550-02	July 2012	Release 2.0
64-0550-01	February 2012	Release 1.0

Refer to www.dialogic.com for product updates and for information about support policies, warranty information, and service offerings.

Hardware Limited Warranty

Refer to the following Dialogic web site for information on hardware warranty information, which applies unless different terms have been agreed to in a signed agreement between yourself and Dialogic Corporation or its subsidiaries. The listed hardware warranty periods and terms are subject to change without notice. For purchases not made directly from Dialogic please contact your direct vendor in connection with the warranty period and terms that they offer.

http://www.dialogic.com/warranties

1. Dialogic® BorderNet™ 4000 Session Border Controller

The Dialogic® BorderNet™ 4000 Session Border Controller (SBC) is a stand-alone device that provides all the functionality required for call signaling, control, and media termination in a VoIP network. It is typically deployed on the border of a network and manages both incoming and outgoing signaling and media traffic for service providers that require call session control and network security.

The BorderNet 4000 SBC delivers fully redundant, high availability session control and is a security platform for interconnect applications, including secure IP peering. The BorderNet 4000 SBC facilitates calls that interwork between different signaling protocols, acts as a firewall to enhance security, conceals the internal topology of a private network, manages bandwidth usage and prioritizes call sessions.

Key Features

The BorderNet 4000 SBC provides:

- Advanced platform infrastructure with “five-nines” availability
- B2BUA architecture, including call management, third party call control (3PCC) and IPv4-IPv6 interworking (IWF)
- SIP, H.323 signaling, application layer gateway (ALG) and profiler
- Security, call admission control, and service assurance
- Access security, including far-end NAT traversal
- Media handling and transcoding
- Integrated web-based management for operations, administration, and maintenance (OAM)
- Interworking between SIP, SIP-I, and SIP-T
- Statistics, reports and alarms

The BorderNet 4000 SBC supplies comprehensive, multi-layer session-to-packet security and protection for OSI Layers 3, 4, 5, 6, and 7. The BorderNet 4000 SBC employs encryption, TCP/UDP connection limits, Access Control Lists, SIP message checks, packet and protocol consistency checks, dynamic packet rate adjustments, and a flow classification engine.

The BorderNet 4000 SBC can operate at 99.999% availability without impacting call sessions during system switchovers or malicious attacks.

B2BUA Architecture

A back-to-back user agent (B2BUA) is a logical entity that controls SIP signaling between the endpoints of a call. A B2BUA acts as a user agent server (UAS) when it receives a request, and then the B2BUA acts as a user agent client (UAC) to process the request. A B2BUA manages the entire call from connection to termination, which means a B2BUA is not limited by strict transparency requirements of a pure SIP-proxy. Instead, a B2BUA acts similar to a proxy in some instances and similar to an end user agent in other instances, depending on the operator's requirements.

The BorderNet 4000 SBC supports a configurable range of B2BUA transparency levels, from a strict B2BUA to a fully transparent B2BUA. The BorderNet 4000 SBC maintains independent dialogs on each side of a call and still allows other SIP message and header information to be passed transparently across the system. Alternatively, the BorderNet 4000 SBC can be configured to suppress, modify, or insert a wide array of information between the two call halves to maintain the strictest privacy while still allowing the widest possible interworking between otherwise incompatible SIP networks.

The BorderNet 4000 SBC maintains full transaction, session, and dialog statefulness ("Dialog Stateful B2BUA" mode). If media management is enabled, full media statefulness is maintained. In this case, the BorderNet 4000 SBC modifies session descriptions in SIP messages so that media passes through the system.

Call Management

BorderNet 4000 SBC B2BUA architecture has the following capabilities:

- Setup, modify, and tear down call sessions
- Manage the independent dialogs (on the separate call-halves) that make up a session
- Allow for varying levels of message and header transparency based on configuration
- Intercept and regulate media traffic

In a point-to-point call scenario, the B2BUA uses its UAS leg to process incoming requests and its UAC leg to determine how the request will be answered.

Certifications and Compliance

Broadsoft Broadworks Certification

The BorderNet 4000 SBC is certified against Broadworks Release 18, which encompasses the basic and advanced Class 5 feature set. See the *Broadworks Session Controller Interoperability Test Report* for additional information.

Miercom Certification

The BorderNet 4000 SBC earned the Miercom Performance Verified Certification for maintaining a maximum of 32,000 simultaneous calls while under an INVITE flood attack. In addition, the BorderNet 4000 SBC:

- Maintained a maximum of 32,000 simultaneous calls while under an INVITE flood attack.

- Achieved 600 cps without dropping calls and maintaining a 25% CPU utilization.
- Withstood a 72 hour INVITE flood attack with normal baseline call traffic.
- Maintained call functionality while being attacked with malformed SIP messages.
- Maximum system uptime achieved with redundant signaling/media, management and HA interfaces.

SIPconnect 1.1 Compliance

The BorderNet 4000 SBC is SIPconnect 1.1 Compliant. SIPconnect 1.1 compliance specifications include:

- Reference architecture that describes the common network elements necessary for Service Provider-to-SIP-PBX peering for the primary purpose of call origination and termination.
- Basic protocols (and protocol extensions) supported by each element of the reference architecture and exact standards associated with these protocols.
- Two modes of operation—Registration mode and Static mode—whereby a Service Provider can locate a SIP-PBX.
- Standard forms of Enterprise Public Identities.
- Signaling messages for Basic 2-Way Calls, Call Forwarding, and Call Transfer.
- Minimum requirements for codec support, packetization intervals, and capability negotiation.
- Minimum requirements for handling fax and modem transmissions, handling echo cancellation, and transporting DTMF tones.

2. Product Specifications

Protocols	
Supported Signaling Protocols	SIP, H.323
Other Protocols	IPV4, UDP, TCP, TLS, IPv6 RFC 768, 1889, 3550 RTCP RTP RFC 3551 - RTP Profile for Audio and Video Conferences 3GPP Interfaces: Mx, Mw, Gm, Ici, Izi
Features	
Security	• Access control—signaled pinhole firewall for media • Network topology hiding via double NAPT for both signaling messages (layer 5) and media flows (layer 3) • NAT traversal • DoS and overload protection for service infrastructure—rate limiting signaling messages and media flows • Session constraint enforcement
Session Admission Control	• License control • Session rate as configured on the interface and/or peer • Auto black listing when the limit is exceeded
IMS, IPX and VoLTE	• Proxy Call Session Control Function (P-CSCF) • Interconnect Border Control Function (I-BCF) • Transition Gateway (TrGW) • Integrated Border Function (I-SBC) • Interworking Function (IWF)SIP and SIP-I/SIP-T Interworking
VLAN Bridging	• 802.1q (LAN) • 1024 VLANs (supports multiple IPs for each VLAN)
Bandwidth Policing	• Media profiling and usage monitoring • Dynamic bandwidth limiting • Media packet rate monitoring and limiting based on media profile characteristics • Bandwidth determination from SDP (limit defined by configuration)
Routing	• Interface/interface static routing • Peer/interface-based static routing • SIP message-based routing • Local DNS table for URI to IP address and port mapping • Load-balancing and priority-based routing • Connectivity with peers • SIP Redirect Server • Policy Based Routing • Routing resolution through external DNS (SRV, A, NAPTR)

	• RFC 4904 Trunk Group Routing support • Multi-tenant routing table support • Emergency services call routing and call prioritization • SIP URN Routing • Dynamic SIP REFER Processing
Media Routing	• Media termination • Separation of signaling and media over VLANs • Media NAT traversal • QoS (including DSCP)
Media Interworking	Transcoding support for the following codecs: • Audio: G.711, G.722,G.723.1, G.726, G.729a, G.729b, AMR-NB, AMR-WB*, GSM-FR, GSM-EFR, iLBC • Video: H.263, H.264, MPEG4 • Fax: G.711 fax, T.38 • Tones: G.711 tones, SIP INFO, RFC 2833 **Note**: Dialogic offers transcoding services on the BorderNet 4000 SBC in two ways: as Integrated Software-based Transcoding supported without the need for additional DSP resources, or via a combination of the BorderNet 4000 SBC and the Dialogic® BorderNet™ 2020 SBC for very large density requirements. * Using the AMR-WB resource in connection with one or more Dialogic products mentioned herein does not grant the right to practice the AMR-WB standard. To seek a patent license agreement to practice the standard, contact the VoiceAge Corporation (as of June 2013) at http://www.voiceage.com/licensing.php.
Reporting	• QoS metrics—packets lost, jitter inter-arrival, latency • Policy enforcement: DSCP marking, ToS Marking • Traffic statistics—total packets and octets transferred
Performance and Capacity	• 600 call attempts per second (CAPS) (signaling and media) • 32,000 concurrent sessions • Access: Up to 256,000 subscribers at 1,600 registrations per second; 3,610 refreshes per second • 1,024 VLANs • 2,048 IP addresses (signaling and media) • 500 SIP interfaces • VLAN bridging: Up to 1,024 802.1q VLANs • 50,000 IPsec tunnels
Network Interfaces	Signaling and Media: • 4 gigabit Ethernet (10/100/1000 Base-T or MM fiber each) with port redundancy

	• 4+4 gigabit Ethernet (10/100/1000 Base-T or MM fiber each) without port redundancy • Full duplex • Management: 1+1 gigabit Ethernet (10/100/1000 Base-T each) with port redundancy • HA control: 1+1 gigabit Ethernet (10/100/1000 Base-T each) with port redundancy
Configuration	• Integrated web-based management (https)
Management	• SNMP traps sent for alarms • Alarms, reports, historical and real-time statistics • Support for Wireshark packet and session tracing • Bulk Provisioning • SOAP/XML
Scalability	• 1024 VLAN • 2048 IP addresses (signaling and media) • 500 SIP interfaces • 4096 peers
Hardware	
Hardware Redundancy	• Hot swappable fans • Hot swappable disks • Hot swappable AC or DC power supplies • Port redundancy
Disk Mean Time Between Failures (MTBF)	• 95,875 hours MTBF per platform
Disk Annualized Failure Rate (AFR)	• 0.62% AFR per platform
Power	
Power Supplies	• Dual hot swappable AC or DC power supplies • Each power supply 650W maximum
AC Power Option	• Autoranging 100-240 VAC +/- 10% with power factor correction • Frequency: 50Hz – 60 Hz • Current: 10A – 5A RMS
DC Power Option	• Voltage Input Range: -40 to -60 VDC • Nominal: -48 VDC • Current: 12A – 6A
Physical	
Dimensions	• Width: 19in (482.6mm) • Depth: 20.75in (527.1mm) • Height: 1.74in (44.2mm)
Weight	• 25.9 lbs
Regulatory Standards	

Safety	• UL/CSA 60950-1 - 2nd Edition (2007) • EN 60950-1: 2006 + A11: 2009
EMC	• FCC 47 CFR Part 15, Class A Digital Device • ICES-003 Issue 4 - Feb 2004, Class A • EN 55022: 2006 + A1: 2007, Class A Limit • Brazil Anatel
Immunity	• EN 55024: 1998 + A1: 2001 + A2: 2003 and EN 300 386 V1.4.1 (2008)
NEBS	• NEBS Ready
Environmental Conditions	
Operating Temperature Range	41°F to 122°F (5°C to 50°C)
Storage Temperature Range	-4°F to 149°F (-20°C to 65°C)
Relative Humidity	Up to 90% non-condensing
Heat Dissipation	Not exceeding 440W (1502 BTU/Hour)
Power Dissipation	• Typical: 400VA (330W) • Max: 470VA (400W) under full load

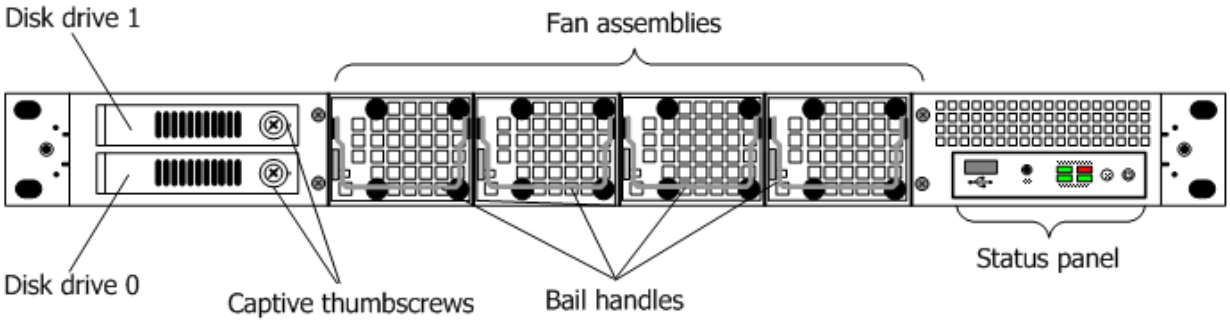
3. Platform Infrastructure

The BorderNet 4000 SBC platform features:

- 1U Chassis (20" depth)
- Hot-swappable redundant AC or DC power supplies
- Four hot-swappable fans
- Dual hot-swappable SATA hard disks (250 GB) configured in RAID 1 configuration for data redundancy
- Front status panel with fault indicator LEDs, power on/off control, system reset control, and system ID control
- Dedicated network interfaces with full redundancy for:
  - Management network connectivity
  - Session network connectivity
  - High Availability link for "HA" deployment
- Four optical or copper gigabit network interfaces with full redundancy for session network connectivity

BorderNet 4000 SBC Front View

Beneath the cover, the front view of the BorderNet 4000 SBC consists of two disk drives, four fans with bail handles, and a status panel.



Hard Disks

The BorderNet 4000 SBC includes dual hot-swappable, high-reliability hard disks. Two hard disks provide data redundancy in a RAID 1 (mirroring) configuration.

Fans

Four hot-swappable fan modules provide redundancy and high reliability. In the event of a fan failure, the remaining fans automatically run at a faster RPM to maintain the system's thermal condition.

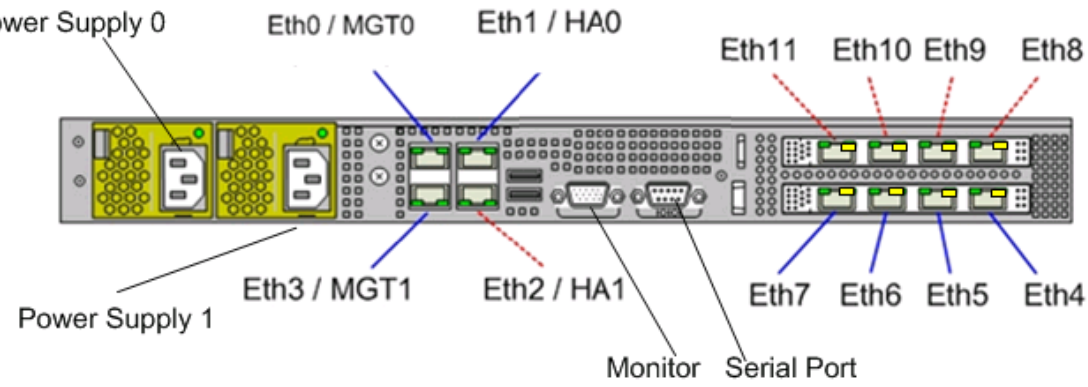
Status Panel

The status panel contains a USB 2.0 connector, Fault Indicator LEDs and panel buttons. The front-facing cover of the BorderNet 4000 SBC does not need to be removed to access the status panel components, and the ID and Reset options are also available via the WebUI.

Status Panel Components	Description
USB	Port for a universal serial bus connector (USB 2.0).
LEDs	**M Fault**—indicates a major fault warning, such as if a component temperature reaches a critical reading. **C Fault**—indicates a critical, non-recoverable event. The BorderNet 4000 SBC will perform a graceful shutdown to protect hardware components from thermal damage. **P Fault**—indicates a power supply fault. This LED illuminates if a fault occurs with a fan, temperature, or voltage reading associated with the power supply. **HDD**—indicates hard drive activity. This LED blinks when a disk drive is reading or being written to and does not change color. When there is no hard drive activity, this LED is off. **Note**: The M, C and P Fault LEDs are normally off unless a fault is triggered.
Panel Buttons	**RST**—this is the Reset button. Push the Reset button to reboot the BorderNet 4000 SBC. **Caution**: Using the Reset button may result in a service interruption. **System ID**—this button is used to identify the BorderNet 4000 SBC for servicing when it is installed in a rack with other systems. The ID button flashes blue when pressed and turns off when pressed again. The system ID can also be illuminated by a remote system ID command. **Power**—this button turns the BorderNet 4000 SBC ON and OFF. Push and hold the button for several seconds to change the power status.

BorderNet 4000 SBC Rear View

The rear view of the BorderNet 4000 SBC consists of two redundant power supplies, four integrated 10/100/1000 BaseT Ethernet ports, monitor and serial ports, and two four-port Gigabit Ethernet cards.



Power Supplies

Dual 650W power supplies provide redundancy. Both power supplies share the load, and each hot-swappable power supply can be either AC or DC.

Copper and Optical Interfaces

The four-port Gigabit Ethernet cards are used for signaling and media network connectivity. These can be either copper or optical interfaces:

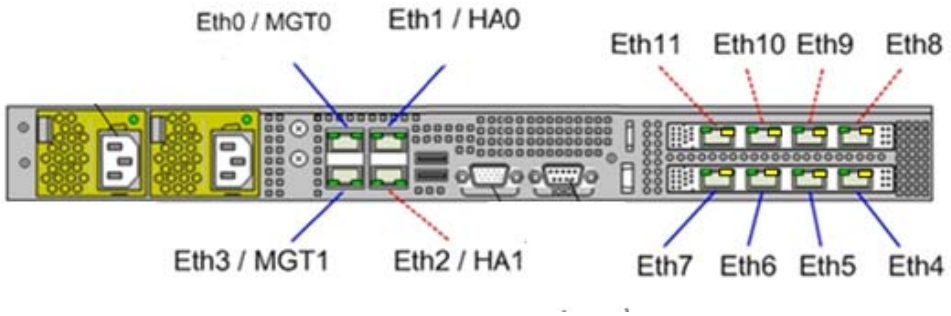
- Copper interfaces are 10/100/1000 Base-T.
- Optical interfaces are multimode fiber (MMF).

Network Connection Redundancy

The standard configuration of the BorderNet 4000 SBC provides full redundancy for all three types of IP network connections:

- A set of two copper Ethernet ports provide redundant management links for all management traffic to the BorderNet 4000 SBC platform.
- A set of two copper Ethernet ports provide redundant High Availability (HA) links for the BorderNet 4000 platforms deployed in a 1+1 configuration.
- A set of eight copper or MMF Gigabit ports provide redundant session links for signaling and media traffic.

Primary and secondary links are paired as follows:



Link Type	Primary Link	Secondary Link
Management link pair	Eth0	Eth3
HA link pair	Eth1	Eth2
Session link pair 1	Eth4	Eth8
Session link pair 2	Eth5	Eth9
Session link pair 3	Eth6	Eth10
Session link pair 4	Eth7	Eth11

Ports

The BorderNet 4000 SBC has two USB ports, one VGA port, and one serial port.

High Reliability and High Availability

The integrated redundancy characteristics of the BorderNet 4000 SBC platform make it highly reliable. The HA configuration ensures high availability. This protects system availability in the event of hardware component failures or Ethernet port or link failures.

Hardware

The BorderNet 4000 SBC system is protected against hardware component failures by:

- Redundant power supplies. In the event of a power supply failure, the secondary power supply keeps the system running and available.
- Redundant hard disks with RAID 1 configuration. In the event of a hard disk failure, the secondary hard disk protects the data and keeps the system running.
- Redundant fan modules. In the event of a fan failure, active fan speed is automatically raised or lowered to protect thermal conditions and maintain a constant temperature.
- Redundant Ethernet ports. In the event of a port failure, the secondary port maintains network connectivity.

Network

Layer 1/2 and Layer 3 redundancy keeps network access to the BorderNet 4000 SBC highly available and makes link failovers transparent to other nodes on the network.

- If the Primary Management link (Eth0) fails, the management IP addresses switch over to the secondary link (Eth3). Management access is seamlessly available over the secondary link with no traffic impact.
- If a Primary Session link (Eth4, Eth5, Eth6, Eth7) fails, the Session and Media IP addresses switch over to the corresponding secondary link (Eth8, Eth9, Eth10, Eth11). Signaling and media session traffic is seamlessly available over the secondary link with no traffic impact.
- If the Primary HA link (Eth1) fails, the HA link IP addresses switch over to the secondary HA link (Eth2). HA access is seamlessly available over the secondary link with no traffic impact. If both HA links fail, the standby system takes over.
- In an HA deployment scenario, if both primary and secondary management links or session links fail, the BorderNet 4000 SBC switches over to the standby platform. The BorderNet 4000 SBC is seamlessly available to other nodes on the network with no traffic impact.

Deployment

The BorderNet 4000 SBC can be deployed in Standalone mode or High Availability mode.

Standalone Mode

In Standalone mode, one BorderNet 4000 SBC is deployed. The redundancy capabilities in Standalone mode achieve high reliability of the system in the event of hardware component failures (fans, disk drives, or power supplies) or network interface failures. Software and platform-level redundancy are not available in this mode.

High Availability Mode

In High Availability mode, two BorderNet 4000 SBCs are deployed in a 1+1 configuration. This deployment achieves high availability and high reliability of the system in the event of hardware component failures, network interface failures, platform-level failures, or dual component failures, providing 99.999% (five 9's) availability.

For High Availability deployment, two BorderNet 4000 SBC platforms are connected to each other using direct Ethernet links (crossover cables) over redundant HA ports (Eth1 and Eth2).

In the High Availability configuration, the paired BorderNet 4000 SBC platforms work in Active-Standby mode. The Active BorderNet 4000 SBC handles the media and signaling sessions; the Standby BorderNet 4000 SBC provides high availability and protects against platform-level failures such as system reboots, power failures, dual network link failures, software failures, software upgrades, or operator-initiated switch-overs.

All configuration data provisioned in the Active BorderNet 4000 SBC is mirrored and kept in sync with the Standby BorderNet 4000 SBC. Existing call contexts (signaling and media sessions) are also mirrored between Active and Standby platforms.

In the event of a platform switch-over, the Standby BorderNet 4000 seamlessly takes over as the Active system and continues service to new and established sessions.* Platform failovers are transparent to signaling and media traffic and the management network.

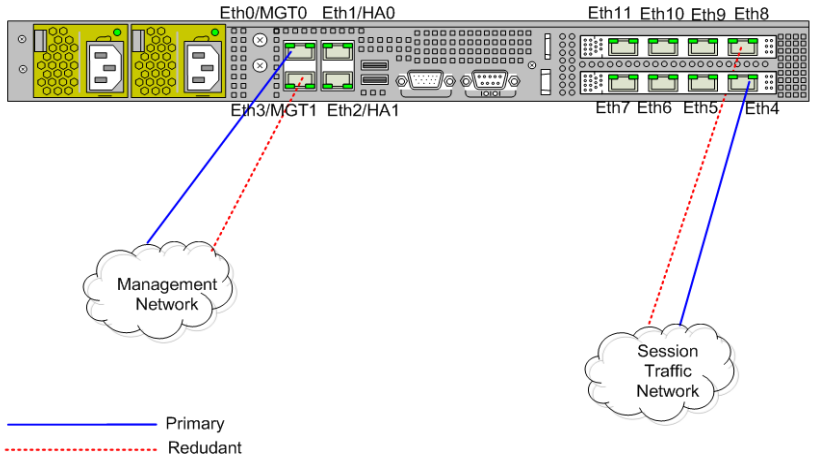
**Sessions involving H.323 legs are not preserved across platform switch-overs.*

4. Networking and Topology

The BorderNet 4000 SBC supports redundant connectivity to IP networks and can connect to switches or routers that support RFC3768. The Virtual Router Redundancy Protocol (VRRP) automatically assigns routers and provides maximum network availability (VRRP must be set up on each router for network-level redundancy).

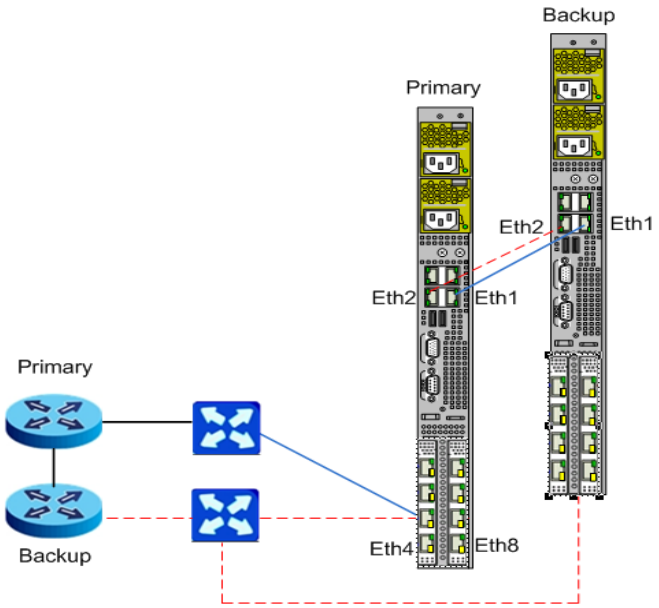
IP Network Connectivity

The BorderNet 4000 SBC separates management and traffic networks.



Network Configuration

In an HA configuration, the BorderNet 4000 SBC traffic ports are connected to a fully redundant IP network.



8021.Q VLAN (Virtual Local Area Network) Support

On the BorderNet 4000 SBC, VLANS can be used to separate signaling and media packets into different logical networks. VLANs can also segregate and route traffic to specific peering entities. The BorderNet 4000 SBC supports the configuration of up to 1024 8021.Q VLANs on session links for signaling and media traffic. The following parameters can be configured for each VLAN:

- Session link
- VLAN ID (1 to 4094)
- Primary IP address subnet mask
- Configured IP addresses
- Default gateway IP address for all traffic from this VLAN

Egress session traffic is tagged with the configured VLAN ID.

When the BorderNet 4000 SBC is deployed in an HA configuration, the IP addresses and VLANs are configured on the platform pair. In the event of a platform switch-over, the same VLAN configuration and IP addresses are available on the secondary platform. Switch-overs are transparent to other nodes on the network.

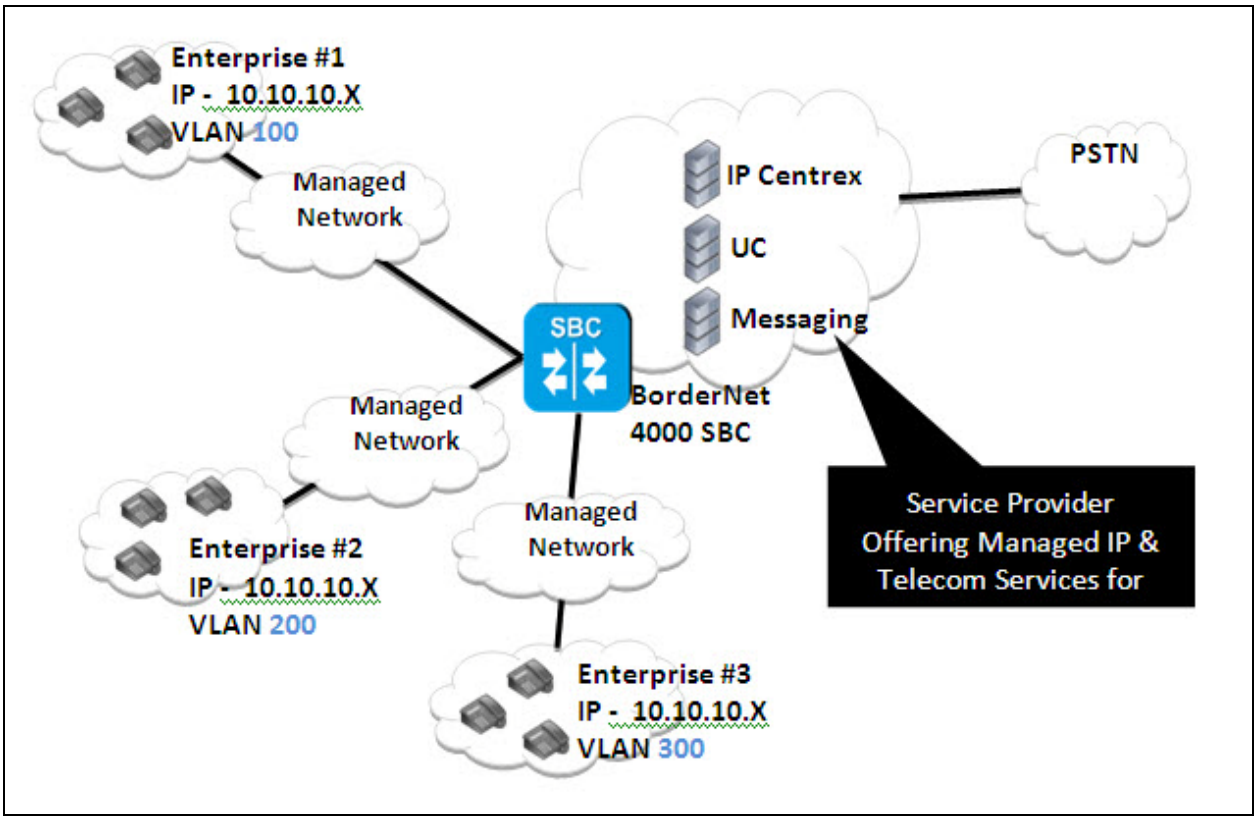
Multiple IP Addresses Per VLAN

The BorderNet 4000 SBC supports up to 254 IP addresses per VLAN, with a system wide limit of up to 2048 IP addresses for signaling and media access across all VLANs. Operators can configure multiple IP addresses per VLAN from the same VLAN subnet on the session link.

Note: VLANs are optional. Networks that do not require VLANs do not need to configure VLANS on the session links.

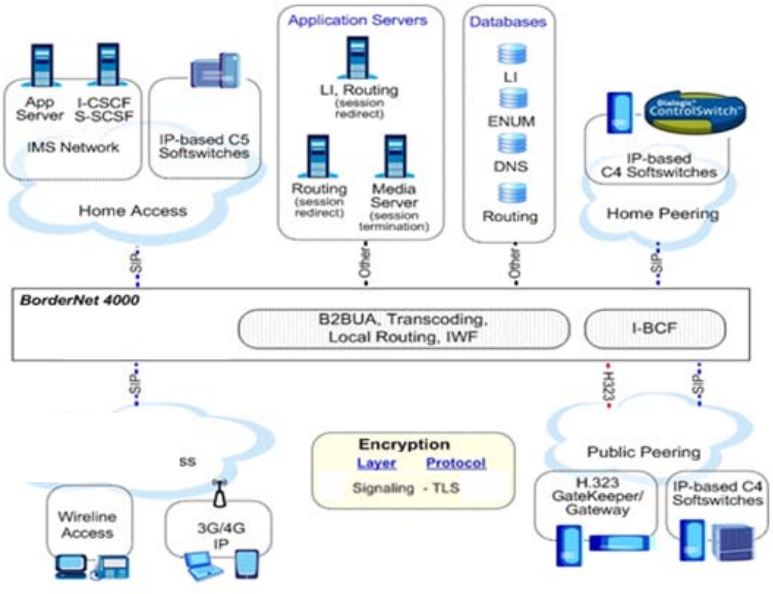
Overlapped IP Address

The BorderNet 4000 SBC supports overlapping private networks with a common IP addressing scheme. These topologies are frequently seen in the managed service provider networks. Typically, VLAN tagging is used to clearly distinguish between different overlapping networks. The BorderNet 4000 SBC's interface definition and peer binding has been enhanced to include specifying VLAN tag associated with each overlapped network. The BorderNet 4000 uses this unique combination of SIP interfaces, peers, and the VLAN tags to route traffic between various overlapping networks.



Topology

The BorderNet 4000 SBC supports Secure IP Peering.



5. Security and Service Assurance

The BorderNet 4000 SBC protects itself and the network infrastructure from malicious attacks while ensuring that VoIP services are uninterrupted. Resources are always available for legitimate sessions, even under high-load conditions, attacks, and hardware or network failures.

The BorderNet 4000 SBC security infrastructure provides protection against attacks at all layers: IP/Transport, Signaling, and Application.

Layer	Security Assurance
6 – 7 Application (SDP)	• Allows sessions from configured peers only • Uses dynamic blacklisting of peers for bad behavior • Provides session constraints • Enables selective information hiding, including topology hiding, with B2BUA architecture
5 (SIP/H.323)	• Provides syntax and semantic validation of signaling messages • Provides TLS for SIP signaling and management traffic
3 – 4 (IP/Transport)	• Provides a firewall to protect against TCP/IP attacks • Employs rate-limiting to protect against DoS attacks • Enables topology hiding via media termination/relay

L3/L4 Security Measures

All incoming IP packets are parsed and checked against a set of rules to detect if the packets are trying to exploit any known vulnerabilities of IP, TCP, UDP and ICMP protocols. These checks ensure that valid traffic-flows are processed according to service level agreements (SLAs) while malicious traffic is dynamically blocked.

Packet Consistency Checks

Each packet entering the BorderNet 4000 SBC through an Ethernet interface is checked to verify that the IP packets are valid. The BorderNet 4000 SBC blocks the following IP packets:

- packets with a multicast or broadcast source IP
- packets with incorrect IP header length
- packets with mismatched IP header checksum
- packets with the value of the IP header length field not equal to five (5)
- truncated packets

Fragmented IP Consistency Checks

Valid IP packet fragmentation, transmission, and reassembly are supported as per RFC 791. Each fragmented packet is checked to ensure validity. The BorderNet 4000 SBC drops any IP packet that fails one of the following consistency checks:

- Fragment length overflow—the reassembled packet length, header and data is larger than 65,535 octets
- Fragment is too small—the minimum size of the first fragment is less than 160 bytes
- Overlapping fragments
- Maximum number of fragments exceeds 70

Protocol Consistency Checks

IP standards provide protocol guidelines that detect and filter non-conforming or malicious packets. The BorderNet 4000 SBC validates every incoming packet against the following guidelines:

- TCP/UDP Protocol
    - Drops packets with fragmented TCP headers
    - Drops packets if the source or destination port equals zero (reserved value)
- ICMP Protocol
    - Verifies the minimum packet length according to ICMP type
    - Drops packets that exceed the fragment length overflow limit (65,535 octets)

Additionally, the BorderNet 4000 SBC handles known TCP/IP vulnerabilities such as:

- LAND attacks (sending packets with the same source and destination hosts/ports)
- TCP XMAS/NULL/FIN (stealth scans)
- TCP bad sequence (packets attacking orphaned open sessions)
- Ping of Death attacks (malformed ping packets)
- SYN flooding (TCP/SYN packet flooding)
- ICMP flooding (sends packets via the broadcast network address)
- "PEPSI" attacks (a UDP attack on diagnostic ports)
- "Rose" attacks (only initial fragment flooding)
- "Tear Drop" attacks (IP fragment overlapping)
- "Boink" attacks (reassembly with different offsets and oversize)
- "Nestea" attacks (IP fragments to Linux systems)
- "Syndrop" attacks (TCP SYN fragments reassembly with overlapping)
- "Jolt" attacks (ICMP incomplete fragment)

Access Control Lists

Access Control Lists (ACLs) selectively allow or deny traffic from specified remote entities. An operator can create a set of static filtering rules to accept or block traffic, and the BorderNet 4000 SBC creates service-specific ACLs based on other configurations. These service-aware ACLs enable fine-grain control over BorderNet 4000 SBC traffic and prevent DoS attacks.

Advanced Packet Rate-Limiting

The BorderNet 4000 SBC provides packet rate limiting to protect against legitimate but misbehaving hosts or DoS attacks from spoofed sources. The incoming traffic is classified into flows based on the combination of parameters, including:

- Layer 3 protocol
- Layer 4 protocol, local IP, local port and remote IP

The flows are subject to rate control as determined by the application or as configured by the operator. From an application perspective, these flows correspond to traffic from remote entities.

Traffic flows are classified into two buckets: white list traffic and grey list traffic. Traffic from a trusted source uses the white list path. Traffic from an untrusted source initially uses the grey list path and is promoted to the white list path based on application feedback. Each of the traffic classes has a pre-determined bandwidth to the BorderNet 4000 SBC. The grey list path uses a small percentage of total available bandwidth. The flows within a traffic class share the bandwidth for that class, and the individual flows have their own bandwidth limits within a class.

Separating traffic into classified flows and the additional verification required from untrusted sources ensures that no single remote entity can compromise the BorderNet 4000 SBC.

Dynamic Packet Rate Adjustment

The packet rate for traffic flows can be controlled by the operator or dynamically adjusted by the BorderNet 4000 SBC based on session constraints, configuration, and call patterns. The BorderNet 4000 monitors each session and determines the expected packet rate, which is used by the flow classifier to police traffic.

Traffic Priority and Overload Protection

Each flow is assigned a priority between zero (0) and (8), with zero being the highest priority. Unclassified packets are assigned the lowest priority.

The BorderNet 4000 SBC protects itself during overload by selectively dropping traffic until the overload condition subsides. It has an adaptive protection mechanism that includes throttling low priority traffic during overloads while guaranteeing higher priority traffic is serviced.

Media Security

Pinholes ensure media security. The BorderNet 4000 SBC dynamically opens and closes pinholes for RTP traffic based on session signaling. When a pinhole is open, the BorderNet 4000 SBC accepts the RTP/RTCP traffic from a specified end-point. Bandwidth is monitored based on the signaled codec to prevent bandwidth theft or DoS attacks on the media ports.

Application Security

IPsec Support

Internet Protocol Security (IPsec) is a suite of IETF-defined protocols for securing communications over IP networks. IPsec protocols offer a range of security functions, including data integrity, anti-replay protection and confidentiality via authenticating and encrypting packets in each IP session. The BorderNet 4000 SBC supports the IPsec Authentication Header (AH), which is used to authenticate and validate IP packets, and the

IPsec Encapsulating Security Payload (ESP). In the ESP mode, IP packets are encrypted. The BorderNet 4000 SBC also supports manual keying as well as IKE v1 and IKE v2.

The BorderNet 4000 SBC IPsec implementation is highly scalable and leverages built-in hardware encryption network processors included with the Network Interface Cards (NIC).

TLS Support

The BorderNet 4000 SBC supports Transport Layer Security (TLS) for securing SIP signaling messages.

Malicious Behavior Handling

The BorderNet 4000 SBC checks all signaling messages and protects against malicious behavior by a peer, including:

- High rate of invalid packets
- High message rate
- High call/session establishment rate

If the behavior persists, an alarm is generated and the peer is dynamically black-listed.

Call Admission Control (Session Constraints)

Call Admission Control protects the infrastructure against excessive traffic from remote entities in real time. The BorderNet 4000 SBC implements Call Admission Control by:

- limiting call attempts per second
- limiting total media bandwidth (in kbps)
- limiting the number of concurrent sessions per customer or per supplier or vendor

These limits are set at peer level to control a single IP address or a group of IP addresses.

Note: The BorderNet 4000 SBC limits the total number of call attempts per second that are sent to other networks. This protects the soft switch and other core components from congestion.

Calls can also be manually disconnected through the BorderNet 4000 SBC WebUI.

HTTP Security

The BorderNet 4000 SBC supports integrated web-based management, uses TLS for secure communication, and supports advanced user management and advanced authentication. Only authorized client requests from pre-configured addresses in the ACL are allowed to manage the BorderNet 4000 SBC via HTTP. Unauthorized packets are dropped.

6. SIP Services

The Session Initiation Protocol (SIP) is a signaling protocol that establishes sessions in an IP network. SIP interfaces connect trusted and untrusted networks, and each SIP interface is associated with an IP interface (VLAN + IP address and port). The BorderNet 4000 SBC supports SIP RFC3261 and UDP, TCP, and TLS transports for SIP.

The BorderNet 4000 SBC routes SIP sessions through a multilevel architecture between SIP interfaces while providing the appearance of multiple virtual SIP gateways. The BorderNet 4000 SBC supports up to:

- 512 SIP interfaces
- 1,024 VLANs
- 2,048 IP interfaces
- 4,096 SIP peers

The BorderNet 4000 SBC parses and validates incoming SIP messages before admitting the SIP messages into the system. Optional topology-hiding may also be employed to prevent details of the SIP messages from being passed across the platform. At both ingress and egress SIP interfaces, the SIP Profiler can add, modify, or delete contents of SIP messages and headers to provide compatibility among incompatible SIP networks.

To further control the session, timers can be configured for each SIP interface:

Timer	Values
SIP Timer T1	Estimates the round-trip message propagation time, which is used to determine the minimum time before a message should be re-transmitted. Default value: 500 milliseconds Range: 500 - 4,000 milliseconds, configured in increments of 100 milliseconds
SIP Timer T2	Provides the maximum retransmission interval for non-INVITE requests and INVITE responses. Default value: 4,000 milliseconds Range: 1,000 - 30,000 milliseconds, configured in increments of 100 milliseconds
Maximum Number of Retransmissions Parameter	Defines the maximum number of times a SIP message will be retransmitted by the BorderNet 4000 SBC. Default value: 4 Range: 1 – 7
SIP Proxy Timer C	Sets the proxy INVITE transaction timeout. The timer starts when a 1xx message is received and terminates if a 2xx message is received. If a 2xx message is not received before Timer C times out, the session is dropped. Default value: 240 seconds

Timer	Values
	Range: 180 – 360 seconds, configured in increments of 10 seconds

SIP Application Layer Gateway

The BorderNet 4000 SBC includes a SIP Application Layer Gateway (ALG) that detects potentially malicious SIP requests from outside the trusted network. The SIP ALG validates syntax and semantics for every SIP message received and inspects each message before any other SIP message handling occurs. The SIP ALG ensures that each message is properly formed, including the message body.

The SIP ALG either drops or modifies messages based on:

- SIP syntax and validity checks
- SIP semantic rules
- SDP rules

If a message does not pass validation, the ALG rejects the message.

The following table provides examples of the SIP and SDP semantic conditions that would be rejected by the ALG, along with the minimum modification required to successfully pass validation.

Condition	Modification
The request is received with no "rport" parameter in the top-most Via.	Add the "rport" parameter with the value of the source port.
The Max Forward header is missing.	Add the Max Forward header with a value of 70.
The "m" lines contain audio, video, or image.	Remove all other "m" lines and associated "a" and "c" lines before propagating the message.

SIP Profiler

SIP Profiler is a tool that enables operators to manipulate SIP headers. The BorderNet 4000 SBC SIP Profiler can manipulate both incoming and outgoing SIP messages on any configured BorderNet 4000 SBC SIP interface.

The BorderNet 4000 SIP Profiler is capable of the following header operations:

- Adding, modifying, and deleting SIP headers and parameters
- Using variables to store header and parameter values for later use
- Linking Profiler scripts together in either series or subroutine calls. For example, one XML file can be designed as a common building block that is written once and called repeatedly on different SIP interfaces as part of more complex header manipulations that may vary only slightly from one another.
- Rejecting SIP messages with custom warning codes

- Performing SIP message and header tests and manipulations, such as: BeginsWith, Contains, EndsWith, Equal, MatchPattern, NotEqual, RemoveString, ReplaceString, and so forth.

PRACK

SIP returns two types of responses: a provisional response or a final response.

- A final response (2xx – 6xx) reliably conveys the request processing result.
- A provisional response (1xx) does not acknowledge the request and is not reliable.

When a provisional SIP response (1xx) must be delivered reliably, a Provisional Response Acknowledgement (PRACK) message is added to the provisional response. The BorderNet 4000 SBC supports PRACK and asymmetric PRACK to ensure reliable transmission of the provisional response.

Call Routing

The BorderNet 4000 SBC provides an extensive array of on-board (built-in) and external call routing capabilities. The on-board routing functions include:

- Message-based routing
- Static Routing
- Policy-based routing
- Time-based routing
- Number normalization and prefix/suffix support
- Least Cost Routing
- ASR and Quality based routing
- Multi-Tenant Routing

Note: LCR, ASR, route quality, and multi-tenant routing requires a separate Dialogic partner product for generation of the appropriate routing table

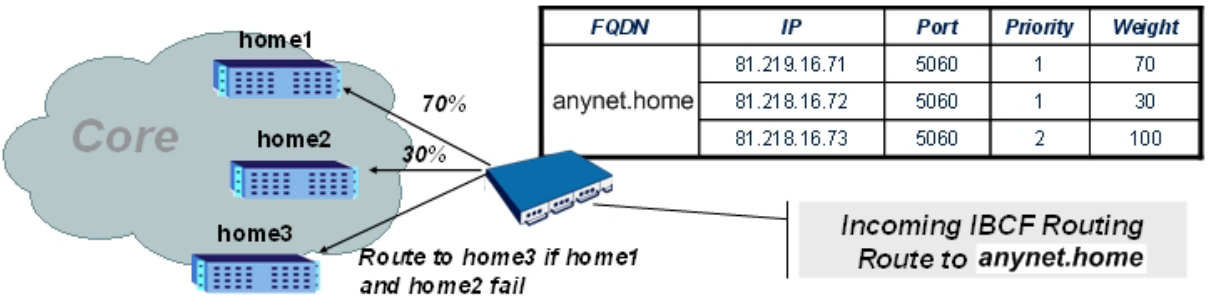
Local DNS

The BorderNet 4000 SBC uses a local DNS table to support FQDN-to-FQDN or FQDN-to-IPv4 address and port number resolution.

Core Network Load Balancing—Incoming Sessions

Load balancing distributes the traffic across multiple remote endpoints. The BorderNet 4000 SBC supports load balancing for inbound sessions to the core network as follows:

- The Fully Qualified Domain Name (FQDN) can be assigned multiple IP addresses within a single subnet, with a maximum of 24 IP addresses per FQDN.
- Priorities and weights can be configured for the group of IP addresses associated with the FQDN.

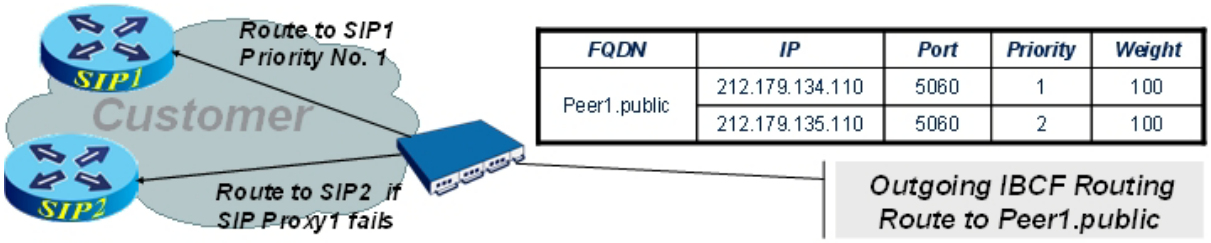


FQDN	IP	Port	Priority	Weight
anynet.home	81.219.16.71	5060	1	70
	81.218.16.72	5060	1	30
	81.218.16.73	5060	2	100

Peer Network Load Balancing—Outgoing Sessions

The BorderNet 4000 SBC supports load balancing for outbound sessions to peer networks as follows:

- The Fully Qualified Domain Name (FQDN) can be assigned multiple IP addresses within a single subnet, with a maximum of 24 IP addresses per FQDN.
- Priorities and weights can be configured for the group of IP addresses associated with the FQDN.



FQDN	IP	Port	Priority	Weight
Peer1.public	212.179.134.110	5060	1	100
	212.179.135.110	5060	2	100

External DNS Support

In addition to the local DNS capability described above, the BorderNet 4000 SBC supports the capability to query external DNS severs for URI resolution. The supported DNS queries include DNS SRV, DNS NAPTR and DNS A record lookups. The BorderNet 4000 SBC DNS implementation is standards-based and IPv6-compatible. The supported standards include RFC 3263, RFC 2782, RFC 291, and RFC 3596. External DNS is useful for call routing, address resolution, and supporting remote peer redundancy.

External Route Server (SIP Redirect Server)

Interconnection to an external Route Server is available. With this feature, Operators can configure the BorderNet 4000 SBC to consult an external routing engine via the SIP INV/3xx method to receive call routing instructions in the form of route lists. To support this feature, the BorderNet 4000 SBC WebUI enables the modification of SIP Profiler entries and parameters to provide access and route traffic to the external Route Server. The BorderNet 4000 SBC also supports routing using trunk group parameters.

Access Features

The BorderNet 4000 SBC provides Access features for residential VoIP, Unified Communications, and enterprise services. Access security features include:

- Access security via DoS, DDoS Protection, and topology hiding
- Registration caching

- Far-end NAT traversal
- Support for Application Services call flows
- Support for forked calls
- DNS (SRV) Application Server redundancy

IPPBX Registration Support

The BorderNet 4000 SBC can process SIP registration requests from both the consumer devices (such as IADs, soft phones, desk phones, mobile extensions, etc.) as well as from the IPBPBXs. IPPBX Registration Support is implemented as per the guidelines in the SIPconnect 1.1 recommendation and RFC 6140—Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)-standard. Specifically, the BorderNet 4000 SBC supports bulk registration of extensions from the IPPBXs.

SIP REFER Handling

The BorderNet 4000 SBC can be configured to terminate SIP REFER messages associated with unattended call transfer messages. Upon termination, The BorderNet 4000 SBC initiates a new call leg with the transfer target and later bridges the original call leg with the transferred leg to locally complete the call transfer. This capability is often desired in contact center and hosted IPPBX solutions where call transfer is routinely used. The advantages of terminating call transfer requests at the border element include cost savings and seamless user experience across various devices and user platforms.

Overload Management

Overload occurs when the BorderNet 4000 SBC cannot handle all of the incoming messages. Overload conditions may cause traffic congestion and could result in a 503 error message until the overload is cleared.

The BorderNet 4000 SBC generates an alarm for each overload level, escalating the alarm as the overload increases. At the same time, the BorderNet 4000 SBC monitors the network interface bandwidth and global system load. Packets are controlled and dropped at the interface level, and the global system load takes precedence over the interface load levels. Incoming packets are categorized and prioritized, and lowest priority traffic is dropped first. Prioritization can occur at the system level or on a specific network interface.

When the next alarm level is reached, the previous alarm is turned off. When the traffic drops below the overload threshold for a minimum period of time, the alarm is turned off.

Note: The BorderNet 4000 SBC does not drop SIP signaling associated with existing sessions, messages related to emergency calls, or packets carrying internal system messaging.

For rejected SIP messages, the BorderNet 4000 SBC returns a *503—Warning: Server Overload* status code to invites from authorized peers. A Retry-After message is sent with all rejected messages, informing the client to retry the request after a specific number of seconds (the default value is 120 seconds).

During overload conditions, the BorderNet 4000 SBC processes the first line of each message to determine if the message should be handled or dropped. BYE or CANCEL messages are parsed; for all other request messages, the BorderNet 4000 SBC compares the request URI with the emergency list as follows:

- If the request URI is present in the emergency list, the message is parsed and handled.

- If the message is a response message, the BorderNet 4000 SBC parses the next header.
- If the message includes a resource-priority header, the response is parsed and handled.

Emergency Call Handling

The BorderNet 4000 SBC ensures that emergency sessions are always handled, even under the most severe level of system overload. Priority levels defined by the ETS namespace values (RFC 4412) are supported in the following priority order:

- ets.0 (highest priority)
- ets.1
- ets.2
- ets.3
- ets.4 (lowest priority)

The BorderNet 4000 SBC recognizes emergency calls by the INVITE message. If the INVITE message contains the resource-priority header with one of the ETS priority levels (ets.0 – ets.4), that message is handled. If the INVITE message contains a To-URI or a Request-URI that contains a match in the Emergency URI Configuration Table, that message is handled.

SIP URN Routing for Emergency Services

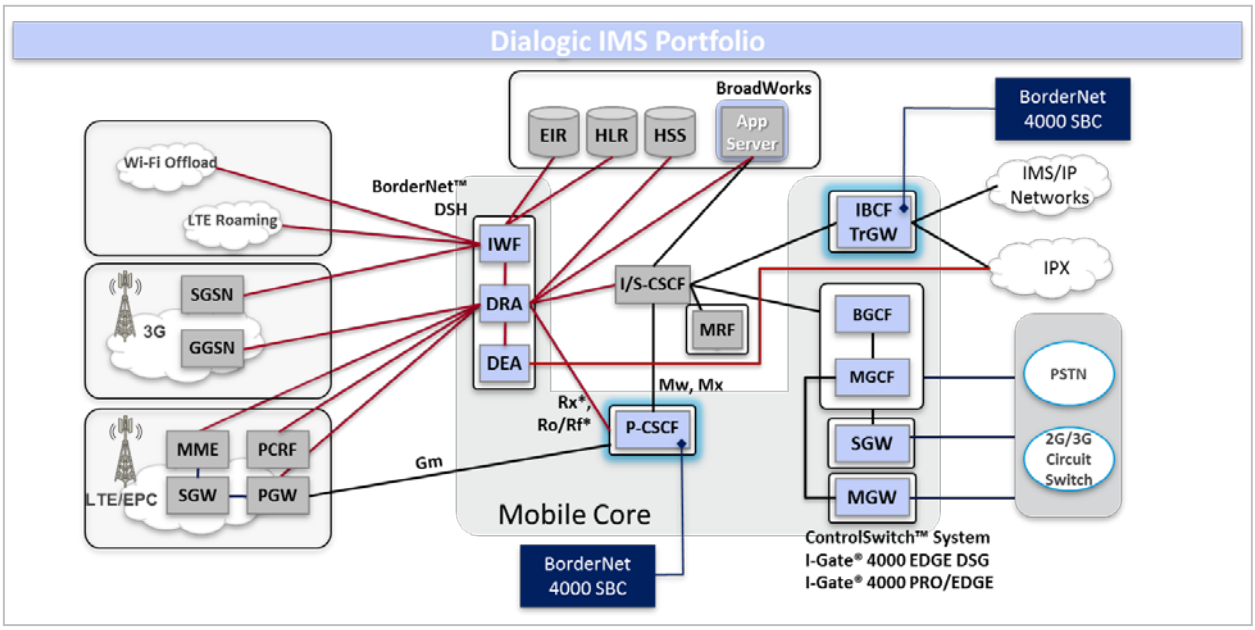
The BorderNet 4000 SBC supports call routing based on the service URN concept proposed in RFC 5031 to handle emergency and other context-sensitive scenarios. Regulatory bodies and leading emergency associations such as the National Emergency Number Association (NENA) have adopted the SIP URN scheme in their next-generation architecture and standards documents. Some example of SIP URN for emergency services include: **urn:service:sos.ambulance, urn:service:sos.fire, urn:service:sos.police, urn:service:sos.poison**. In this scheme, emergency routing is more efficient. Using the available service and subservice context, each call is routed to appropriate first responders. This has an additional benefit of removing region-specific emergency service access (for example, 911 in US, 112 in Europe, or 100 in India) by utilizing a common naming convention.

The BorderNet 4000 SBC is typically deployed as a Border Control Function (BCF) in an Emergency Service Network (ESINet). In this role, the BorderNet 4000 SBC provides core SBC functions such as security, call routing, call prioritization. The BorderNet 4000 SBC can effectively support next generation ESINets by providing the capability to process emergency calls with SIP URN and routing those calls based on URN's service/subservice context. Furthermore, the BorderNet 4000 SBC is also capable of modifying ToS (Type of Service) bytes for emergency calls to ensure expeditious handling of emergency calls by network switching and routing infrastructure.

7. IMS, VoLTE and IPX Support

IMS and VOLTE

The BorderNet 4000 SBC is suitable for deployment as an advanced SBC in 3GPP IP Multimedia Subsystem (IMS) and ETSI/TISPAN based network architecture. The BorderNet 4000 SBC offers best of the breed border element for securing pure-play 3GPP IMS and VoLTE based modern telecom networks. The BorderNet 4000 SBC is a key anchor for seamless delivery of IMS services across IMS, NGN, and legacy TDM networks.



The BorderNet 4000 SBC offers comprehensive border control functionality for both IMS access and interconnect deployments. At the IMS access edge, the BorderNet 4000 can fulfill the role of a P-CSCF, E-CSCF and A-SBC, providing security, signaling, and media interworking functionality defined for these entities in the 3GPP standards. At the IMS interconnect, the BorderNet 4000 SBC can be deployed as an I-BCF, IWF or an integrated I-BGF/TrGW. The product specifications table (see section 2 of this document) summarizes supported 3GPP network interfaces related to the IMS border functions.

BorderNet 4000 Access (P-CSCF) and Interworking (I-BCF/TrGW) Capabilities

The core P-CSCF/E-CSCF border functions available with BorderNet 4000 SBC include:

- **Signaling**
  - **Mw, Mx** SIP Interface
  - 3GPP SIP Call Handling
  - Authentication
  - S/I Selection
  - High subscriber capacity
  - Port Mapping

- **Security and Encryption**
  - Gm Interface
  - Encryption (TLS, IPsec, SRTP)
  - DOS/DDOS Protection
  - ACL
  - Security Hardened stack
  - Protection against malformed messages
  - Rate Limiting (IP and SIP messages)
  - Call Admission Control
- **Emergency Services**
  - Emergency Call Routing
  - Call Prioritization
  - SIP URN Processing
- **Policy Enforcement**
  - Built in Routing Engine
  - Bandwidth Enforcement
- **Interworking**
  - IPv4/IPv6
  - IBCF/TrGW (Ici, Izi)
  - 3GPP/Non-3GPP Access
  - IMS-ALG (Iq)
  - SIP Profiler
- **Charging**
  - CDRs
- **Media Interworking**
  - Media Relay
  - NAT Traversal
  - Bandwidth Rate Limiting
  - Codec Selection and Reordering
  - Media Statistics
  - Transcoding

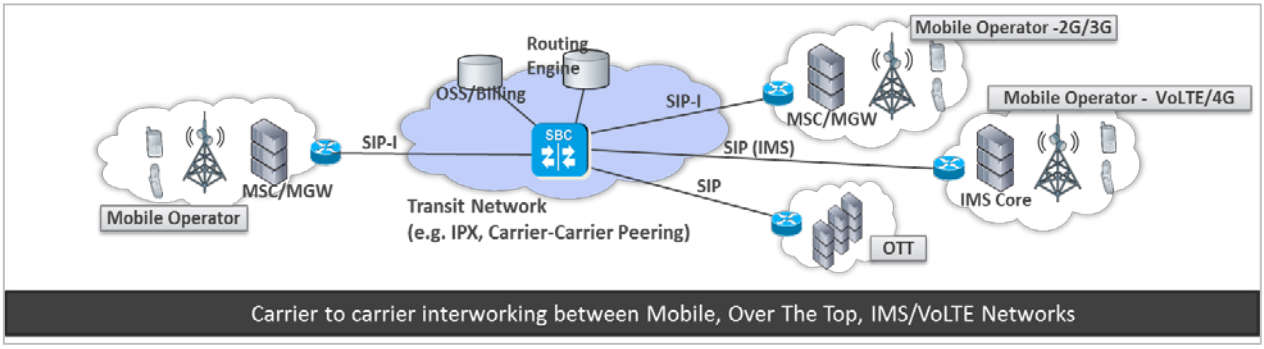
Mobile Interconnect and IPX Support

The BorderNet 4000 SBC offers a range of functionality to support 2G/3G Mobile interconnect and IPX market segments. The BorderNet 4000 SBC is suitable for deployment in different configurations. Some examples include:

- Interconnecting Mobile MSC/MGWs to partner networks over IP links – In a mobile interconnect configuration, the BorderNet 4000 SBC fulfills several critical functions, such as security, SLA assurance transcoding, and interworking. In particular,

interworking between SIP-I and SIP has become a serious issue for the mobile carriers as they connect their subscriber base to Over the Top (OTT) and IMS based network partners. Mobile carriers are ever more relying on border elements such as the BorderNet 4000 SBC to bridge the traditional MSC/MGW mobile cores with variety of SIP-based partner services.

The BorderNet 4000 SBC offers a range of SIP and SIP-I/SIP-T interworking capabilities such as SIP-to-ISUP protocol mapping, management (add/modify/delete) of individual ISUP parameters, call routing based on SIP profiles and ISUP parameters, and recording ISUP contents in the Session Detail Records (SDR) for billing and analysis.



- IPX Networks – GSMA IPX networks are essentially a clearing house for mobile operators. IPX operators typically have few additional requirements beyond the mobile interconnect deployments. Call routing and accounting are two essential pieces for any IPX services. The BorderNet 4000 SBC provides comprehensive on-board and external routing integration. See SIP Services for complete list of routing and accounting capabilities available in the BorderNet 4000 SBC.

8. Interworking Function (IWF)

The Interworking Function (IWF) connects clients with different capabilities, including different protocol dialects.

BorderNet 4000 SBC B2BUA architecture supports the following IWF capabilities:

- **IPv4-IPv6 IWF:**
- **SIP-to-IMS**: The B2BUA adds or removes the IMS SIP protocol extensions (P-headers) so that SIP clients can be connected to an IMS network.
- **SIP, SIP-I, and SIP-T IWF:** Interworking between SIP, SIP-I, and SIP-T.
- **SIP Session Timers (ST) IWF**: Session timers are used to monitor connectivity. The B2BUA connects clients that have different session timer settings.
- **Transport Interworking**: The B2BUA supports multiple transport types (such as TCP, UDP, and TLS) and connects clients with different transport protocols.
- **SIP Profiler**: The SIP Profiler allows extremely flexible alteration of incoming and outgoing messages for improved interworking with otherwise incompatible versions of SIP.

IPv4-IPv6 Interworking Function

The BorderNet 4000 SBC delivers enhanced connectivity through IPv4-IPv6 interworking. The BorderNet 4000 SBC provides native IPv6 support and IPv6 for signaling and media, in addition to allowing dual stack, simultaneous connections to both IPv4 and IPv6 networks. Interworking scenarios include:

- IPv4 to IPv6
- SIP (IPv6) to H.323 (IPv4)

Note: IPv6 functionality requires a license. See Dialogic Technical Support for licensing information.

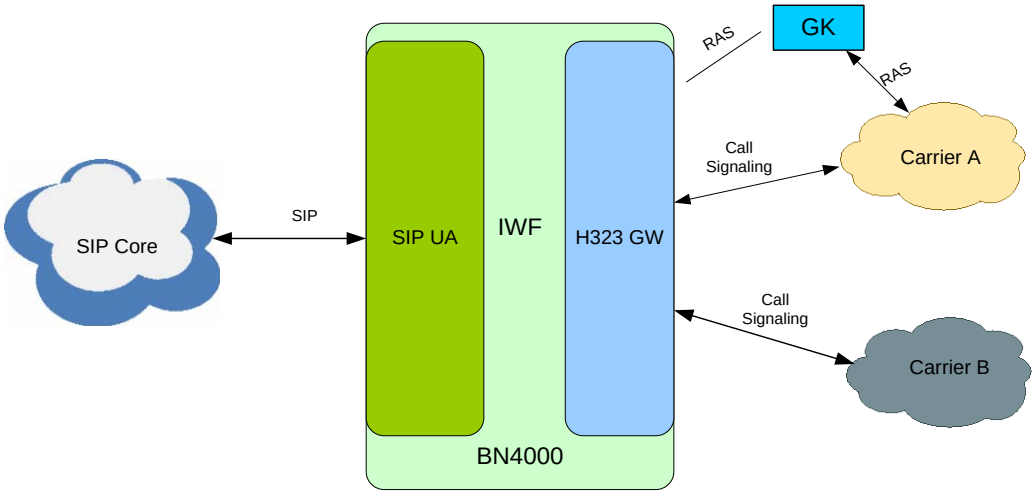
SIP, SIP-I, SIP-T Interworking

The BorderNet 4000 offers a range of SIP and SIP-I/SIP-T interworking capabilities, such as SIP-to-ISUP protocol mapping, management (add/modify/delete) of individual ISUP parameters, call routing based on SIP profiles and ISUP parameters, and recording ISUP contents in the Session Detail Records (SDR) for billing and analysis. The BorderNet 4000 SBC includes a built-in ISUP stack that is capable of decoding ISUP content embedded in the SIP messages to extract various ISUP parameters. The BorderNet 4000 SBC's SIP-to-ISUP interworking follows the recommendations defined in ITU-T's Q.1912.5 specification. The BorderNet 4000 SBC's interworking is complete in that it supports both SIP-to-SIP-I/SIP-T conversion as well as SIP-I/SIP-T-to-SIP conversion.

H.323-to-SIP Interworking Function

The BorderNet 4000 SBC supports H.323 interworking gateway functionality by providing originating and terminating call services using H.323 protocol with a remote gateway. The

H.323 calls are interworked to or from SIP calls. The BorderNet 4000 H.323-IWF can act as a direct gateway or a gatekeeper-managed gateway in an H.323 peering network.



The BorderNet 4000 H.323-IWF provides:

- Default settings for translation parameters
- Support for H.323 gatekeepers (both direct and gatekeeper-routed call models)
- Support for audio, video, and fax sessions
- Support for fast-start and slow-start calls
- Logical channel support, including:
    - Providing a seamless exchange for opening, reopening, changing, and closing media channels during a call
    - Supporting unidirectional channel openings
- The ability to apply normal SIP call routing (IWF does not need to know about proxy servers)
- ToS field settings for H.323 signaling

IWF Call Flow Support

The BorderNet 4000 SBC supports the following call flows:

Call Flow / Type	Description
SIP upstream, H.323 fast-start downstream	The offer received on the SIP INVITE is supported.
SIP upstream, H.323 slow-start downstream	After the offer is received on the SIP INVITE, the BorderNet 4000 SBC attempts an H.323 fast-start downstream. If the downstream endpoint does not support a fast-start, the 4000 SBC switches to a slow-start procedure.
SIP upstream, H.323 downstream (fast-start or	No offer is received on the SIP INVITE.

Call Flow / Type	Description
slow-start)	
H.323 fast-start upstream, SIP downstream	If the H.323 fast-start offer includes alternative codec options, the SDP offer sends the list of alternative codecs to the downstream SIP device in the same order of preference provided by H.323. The most preferred codec is listed first. The SIP endpoint can accept more than one codec; the H.323 fast-start response cannot. In this case, the BorderNet 4000 SBC prunes the codec list to a single codec option and responds with a single codec answer.
H.323 slow-start upstream, SIP downstream	A default SDP offer is made to the SIP downstream; this offer contains a single media channel with the following codecs in order of preference: G.729, G.711 U-law, G.71 1 A-law, and G.723. Capabilities are then negotiated with the H.323 endpoint and a channel is opened with the selected codec. A re-INVITE on the SIP side re-negotiates the codec.
DTMF interworking	DTMF interworking between SIP and H.323 is supported in the signaling plane using the alphanumeric method of UserInputIndication.
Fax handling (T.38)	T.38 fax calls are supported for interworking calls.
Interworking for basic call hold features	Basic call hold features (codec change, hold and resume signaling) are supported in H.323 and SIP calls.

Early Media in SIP-to-H.323 Fast-Start Calls

Early media is supported for SIP endpoints calling H.323 fast-start endpoints. In this case, the caller (SIP endpoint) makes a media proposal on the initial call setup request. The callee (H.323 endpoint) responds to the offer before the call is connected.

H.323 may send a “progress indicator” on any H.225 message that is sent to the BorderNet 4000 SBC. A progress indicator with a value of 1 or 8 indicates that the H.323 endpoint will send early media. The BorderNet 4000 SBC processes early media calls as follows:

- In an interworking call, only the first progress indicator received from the H.323 endpoint is used.
- In an interworking call with a SIP upstream call, if sufficient media parameters were negotiated with the H.323 endpoint, the BorderNet 4000 SBC returns a 183 provisional response to the SIP caller with the SDP indicating early media.
- In an interworking call with a SIP upstream call, if insufficient media parameters were negotiated with the H.323 endpoint, the BorderNet 4000 SBC waits for media

negotiation with the H.323 endpoint to reach a point where the SDP can be generated. When the SDP is generated, then the BorderNet 4000 SBC sends a 183 provisional response.

Early media is also supported for H.323-to-SIP calls. In this case, when SDP is received from the SIP endpoint in either a 180 or 183 message, an appropriate message is generated to H.323 with a progress indicator of 8.

Response Code Mapping

The BorderNet 4000 SBC maps two response codes:

- SIP response codes are mapped to H.225 release codes used by H.323
- H.225 release codes are mapped to SIP response codes

If a downstream SIP endpoint rejects a call, the response is translated into the H.225 release code set for the upstream H.323 device.

If a downstream H.323 endpoint rejects a call, either the H.323 gatekeeper rejects the call or the endpoint sends a Release Complete message to reject the call. This is translated to the appropriate SIP response code.

Calling Line Identification

The BorderNet 4000 SBC supports mapping between H.323 message presentation indicators and SIP Privacy and P-Asserted-Id headers. This supports CLIP/CLIR features.

9. Media Handling

The BorderNet 4000 SBC provides media termination and relay to handle RTP traffic from remote entities signaled through SIP/H.323 messages. It also determines the appropriate media path for a session based on configured options and supports:

- RTP/RTCP, T.38
- Dynamic pin-holing based on SDP
- Rate limits per media flow

Signaling and Media Separation

The BorderNet 4000 SBC can be configured to terminate the signaling and the media, or it can be configured to terminate just the signaling. The IP network topology must enable direct IP routing for media between the two endpoints.

Media Latching

The BorderNet 4000 SBC restricts latching RTP/RTCP media for all calls within the context of a peer or SIP interface. The destination address and port for subsequent RTP packets is determined from the SDP. Media latching can be configured by the operator.

Media Over Multiple Physical Interfaces

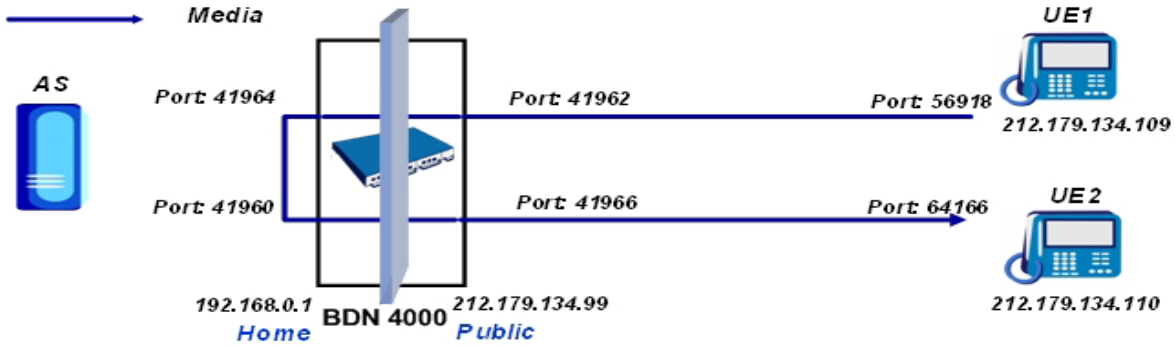
From a single signaling IP address, the BorderNet 4000 SBC can split media over different physical interfaces with different media IP addresses.

Media Rate Limiting

The BorderNet 4000 SBC ensures that media streams associated with a particular session use the appropriate codec (bandwidth) based on the SDP information in the SIP message.

Topology Hiding for Media

The BorderNet 4000 SBC provides topology hiding for the trusted network infrastructure from untrusted networks. This is accomplished by implementing Network Address and Port Translations (NAPT) for media sessions (RTP and RTCP) passing through the BorderNet 4000 SBC. For example, in the following diagram, the remote end points (or gateways) on the public side see only the public IP address (212.179.134.99) and not the core network address (192.168.0.1).



Policy Based Media Routing

Available policies on the BorderNet 4000 SBC can be utilized for control if the media is routed via the BorderNet 4000 SBC or directly between the endpoints. This capability is useful in different instances (such as preserving bandwidth over a skinny WAN link) where it may be preferable to keep the media localized.

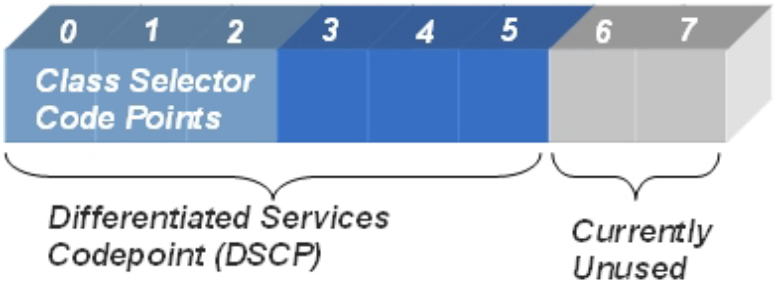
Quality of Service (QOS)

The BorderNet 4000 SBC supports Quality of Service (QOS) settings based on the Differentiated Services (DiffServ) model for media streams. QOS settings are configurable per signaling/media interface by entering a Differentiated Services Codepoint (DSCP) during SIP interface configuration.

The DSCP is a 6-bit pattern (shown below); the pattern is "xyzab0", where:

- "xyz" is the class: 001-class1; 010-class2; 011-class3; 100-class4
- "ab0" is the drop precedence: 01-low; 10-medium; 11-high

Differentiated Services Code Point



The BorderNet 4000 SBC marks the packet based on the operator's needs. The router receiving the packet handles the packet based on the DiffServ value applied by the BorderNet 4000 SBC.

Media Statistics

The BorderNet 4000 SBC collects and reports the following statistics for media on a peer basis:

- Bytes received
- Bytes sent
- Received bit rate
- Sent bit rate
- Dropped packet count
- Bandwidth consumed by dropped packets

Supported Codecs and Methods

The BorderNet 4000 SBC supports identifying various media types registered with the IANA (Internet Assigned Numbers Authority). The BorderNet 4000 SBC has a comprehensive codec profile scheme and is able to recognize, filter, and sort codecs. The BorderNet 4000 SBC monitors media bandwidth and enforces bandwidth based on the profile settings; it also monitors and restricts the media packet rates accordingly. The BorderNet 4000 SBC is

capable of interworking across media subtype notations as well as payload types. Some of the supported codecs are listed below.

Audio	• PCMU • PCMA • G722 • G729 (+/- VAD) • G723 (+/- VAD) • G723-5.3 • G723-6.3 • G728 • G726-32	• GSM • GSM-EFR • AMR (NB/WB+) • Comfort Noise • t38 • iLBC (13.3, 15.2) • clearmode • tone • telephone-event (+ IANA registered)
Video	• H.263 • H.264 • H.261	• MPV • CelB • JPEG (+ IANA registered)
Image	• t38 (+ IANA registered)	

DTMF Relay

The BorderNet 4000 SBC supports DTMF relay via telephone-event or SIP INFO. It also supports H.245 User Input.

Codec Mapping

The following table provides the BorderNet 4000 SBC codec mappings used to convert media specifications between H.245 (used in H.323) and SDP (used in SIP).

H.245 Type	SDP Media Type
g711Ulaw64k	PCMU
g711Ulaw56k	PCMU
g711Alaw64k	PCMA
g711Alaw56k	PCMA
g726	G726-32
g723	G723

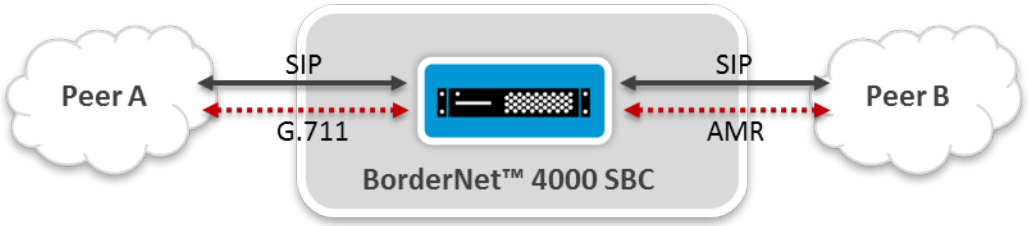
H.245 Type	SDP Media Type
g722	G722
g728	G728
g729wAnnexB	G729
g729	G729 fmtp:18 annexb=no
h261VideoCapability	H261
h263VideoCapability	H263

Media entering the BorderNet 4000 SBC exits the system as per the codec mapping. For example, H.245 type g729wAnnexB exits the system on the SIP side as media type G729.

Note: The BorderNet 4000 SBC IWF uses H.323 Version 4 or later and SIP as specified in RFC3261. Most H.323 signaling uses TCP transport; the exception is RAS, which uses UDP transport.

Software-Based Transcoding

The BorderNet 4000 SBC supports software based real-time transcoding of audio, video, fax and DTMF sessions by utilizing existing on-board computer (CPU) resources on the platform. Traditionally, a resource-intensive media transcoding operation has required the assistance of specialized hardware components, such as Digital Signal Processors (DSPs), and is very expensive. Dialogic has incorporated technology from its industry-leading media server and conferencing products in the BorderNet 4000 SBC to deliver the industry's first scalable transcoding solution.



The BorderNet 4000 SBC software transcoding has several unique features, including:

- Dynamic Transcoding – The BorderNet 4000 SBC determines the transcoding necessary for each call by comparing the ingress and egress codec offers and re-routes the media through an internal transcoding engine.
- Comprehensive Codec Support – The BorderNet 4000 SBC software transcoding includes an extensive list of wireline and wireless codecs. In the current release, the Audio and DTMF transcoding solution is supported. Video and Fax transcoding services will be available in a future release.

Audio	G.711	G.723.1	G.729	AMR-NB	AMR-WB	G.722	G.726
G.711							
G.723.1	✓						
G.729	✓	✓					
AMR-NB	✓	✓	✓				
AMR-WB*	✓	✓	✓	✓			
G.722	✓	✓	✓	✓	✓		
G.726	✓	✓	✓	✓	✓	✓	

- Standalone and Redundant Configuration – The BorderNet 4000 SBC software transcoding can be deployed in either stand alone or redundant (High Availability) configurations. In the redundant configuration, established transcoded and non-transcoded sessions are preserved in case of failure of the active (primary) BorderNet 4000 SBC platform
- Media profiler and transcoding policy – The BorderNet 4000 SBC includes extensive media profiler capability that can be effectively combined with available transcoding policies to tailor the solution to individual customer need. For instance, the media profilers provide extensive codec management capabilities such as the ability to add, remove, and/or re-order codecs, set codec preference, handle packetization period, and manage other media attributes (for example, dynamic payload type).

10. Integrated Management

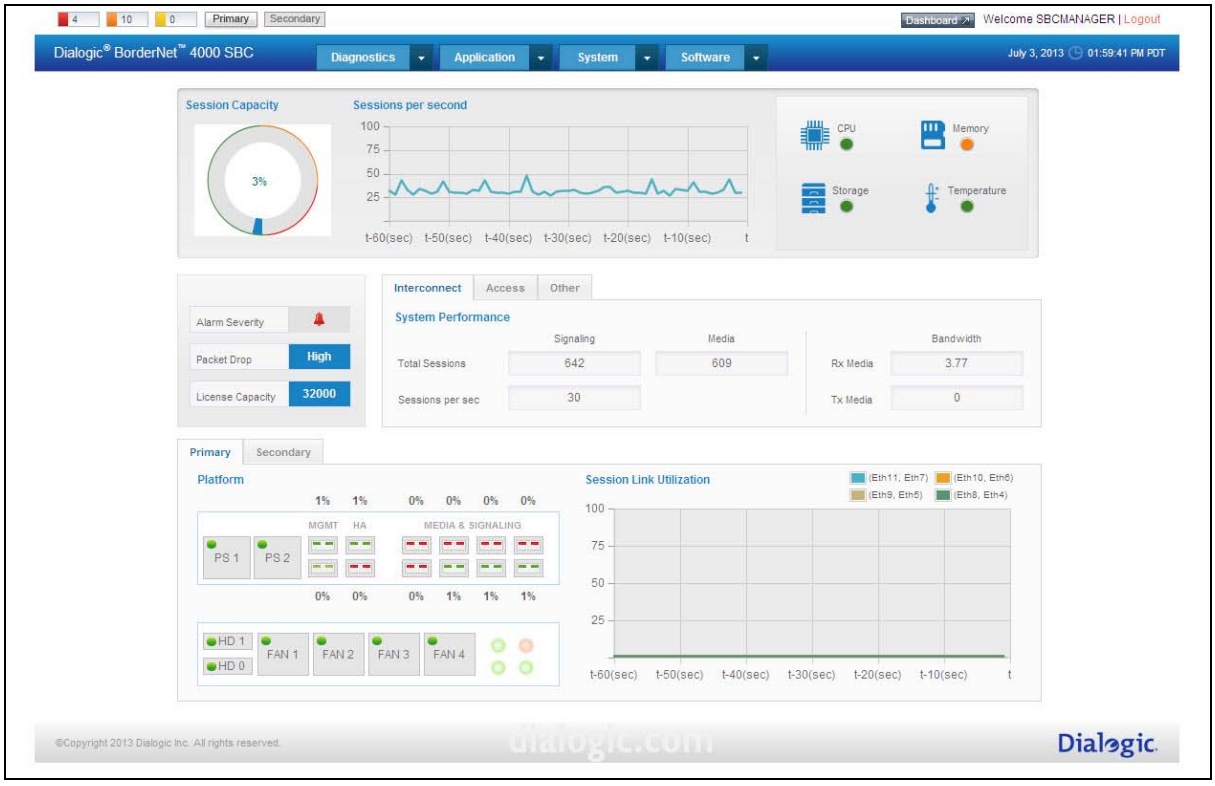
The BorderNet 4000 SBC contains an integrated Local Manager (LM) that provides:

- Software Management for upgrades and releases
- System Configuration to provision the BorderNet 4000 SBC and manage user accounts
- Application Configuration to configure SIP, H.323, security, profiles, and routing policies
- Monitoring and Diagnostics to view performance, statistics, and alarms

Dashboard

Management functionality is accessible through the WebUI. Upon logging into the BorderNet 4000 SBC, the user has access to a system dashboard that displays:

- Current alarms (color-coded by severity)
- Current total number of live signaling and media sessions
- Current processing rate (in calls per second)
- Current total number of live SIP and H.323 signaling sessions
- Real-time charts for the last 60 seconds of CPU activity and bandwidth
- Status and usage level at each network interface
- Hardware component status
- Storage utilization and thermal status



System Configuration

System configuration allows operators to:

- Manage system services, such as NTP, tracing, IBCF, and other services provided by the platform
- Manage IP, IP routing, DNS, and VLAN
- Configure user authorization, authentication, and access control

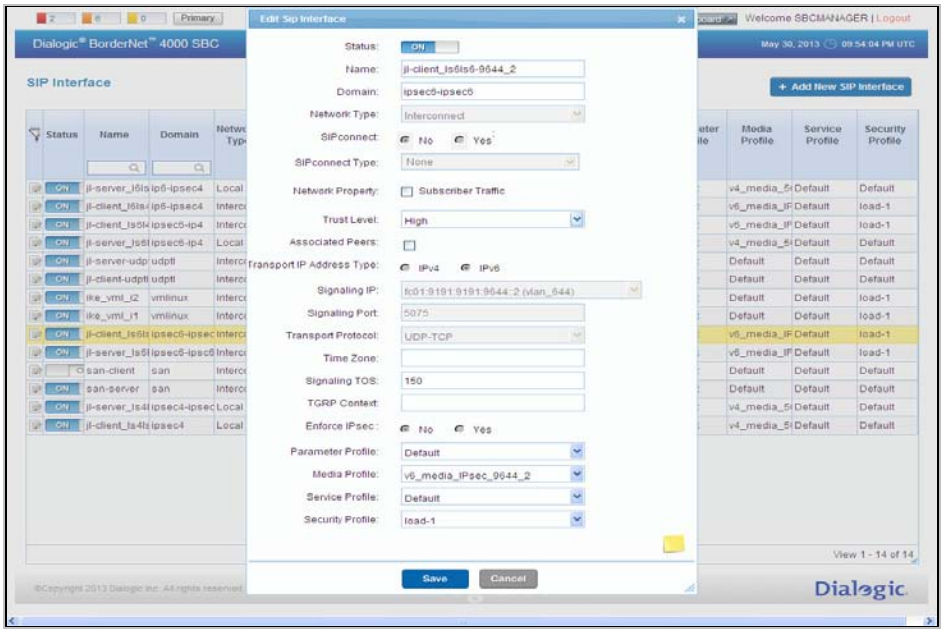
System Audit

The BorderNet 4000 SBC management framework automatically logs all user actions performed via the WebUI. These actions are tracked under the System Administration category and listed as Audit Logs. This feature is provided to facilitate regulatory compliance, internal audits, and troubleshoot configuration and provisioning-related issues. Actions performed on the primary and the secondary servers in a redundant (HA) BorderNet 4000 SBC system are coordinated to ensure a full history of events is available before and after a system switch-over.

Application Configuration

Application configuration allows operators to configure:

- SIP and H.323 interfaces, peers, and interface-peer associations
- SIP and H.323 media profiles and parameter profiles
- SIP message profilers
- Security profiles
- Access control lists
- Service profiles
- Interface-to-interface with peer-level granularity routing, including SIP/H.323 routing
- Runtime configuration, which allows configuration parameters to be modified without switching off or rebooting the system



SOAP/XML API Interface

Dialogic introduces a Service Oriented Application Programming (SOAP) interface to the BorderNet 4000 SBC in Release 3.0.0. This XML-based interface facilitates a number of network operations tasks, including complete automation of common provisioning and servicing tasks, machine-to-machine integration with other OSS/BSS systems in the network, business intelligence, analytics, and reporting. In release 3.0.0, the SOAP interface supports provisioning of peers, interfaces, peer-interface associations, advanced routing, and local DNS. To assist in deploying this feature, Dialogic provides sample code, SOAP Request/Response formats, Authentication scheme, XSD schema, and the Web Services Definition Language (WSDL) for each of the interfaces.

Monitor and Diagnostics

The Fault Management System (FMS) gathers and presents alarm data, such as:

- Pending alarms
- Alarm history
- Alarm definitions

Alarms can be filtered by severity, category, or time. The BorderNet 4000 SBC enables operators to change severity, generate an SNMP trap, or generate email notices for each individual alarm.

Policy-Based Routing

The BorderNet 4000 SBC supports policy-based routing. Routing policies are established by applying parameters and global variables to a configured policy to route traffic. This feature enables operators to establish policy-based routing rules according to:

- Call parameters, which are derived directly from the message
- Non-call parameters, which are derived from:
    - the service profile time zone attached to the incoming peer or interface
    - global variables that store intermediate results used in routing decisions
    - the incoming interface and peers

Trunk Group Routing/RFC 4904 Compliance

The BorderNet 4000 SBC is RFC 4904 compliant and supports trunk group routing. The BorderNet 4000 SBC:

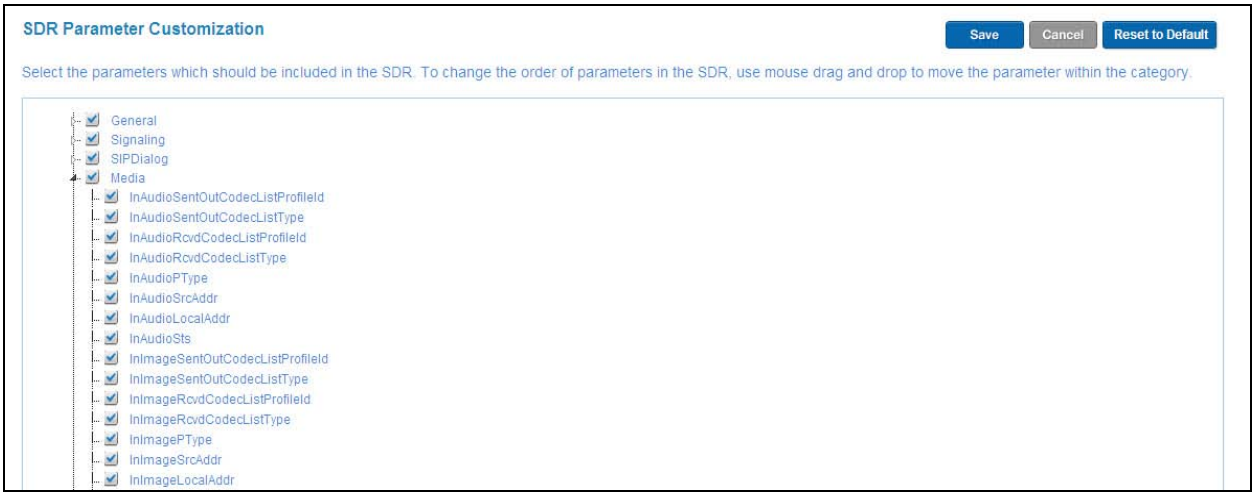
- Enables call routing based on trunk group parameters
- Supports TGRP and Trunk-Context per RFC 4904 and non-standard OTG/DTG
- Provides trunk group information management (pass-thru, add, modify, and delete trunk group parameters)
- Supports trunk group extraction for SIP INVITE and 3xx
- Enables interworking between RFC 4904 and OTG/DTG

Customized Session Detail Records

A Session Control Service (SCS) component takes “snapshots” of call sessions and writes these sessions to a file. This information is recorded in Session Detail Records (SDRs) that can be sent to an external SDR destination to be used for billing or other purposes.

The BorderNet 4000 SBC provides an SDR Parameter Customization feature that enables the operator to:

- Decide what parameters to report in each SDR
- Control the parameter sequence in each SDR, which can be aligned with the Dialogic® ControlSwitch™ System to facilitate reconciliation
- Selectively report additional parameters from SIP Dialog



For additional information on SDR customization, see the *Dialogic® BorderNet™ 4000 SBC Configuration and Provisioning Guide*.

Bulk Provisioning

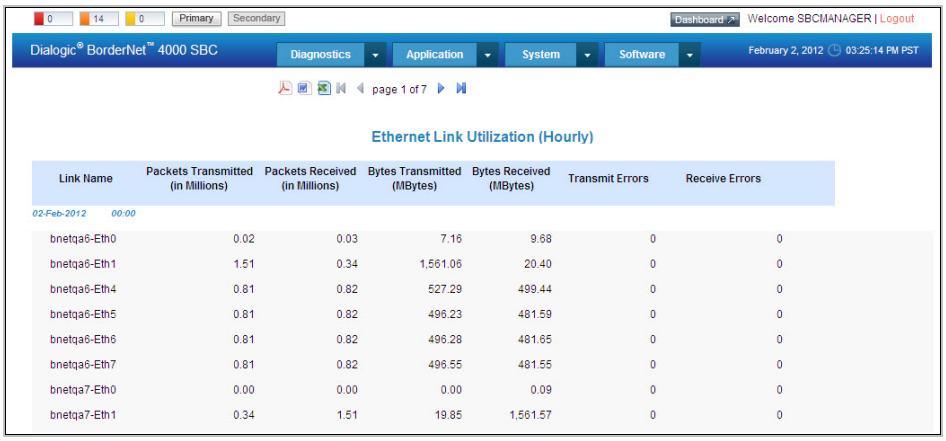
The BorderNet 4000 SBC provides Bulk Provisioning to facilitate mass configuration of SIP data (Peer, Interface, Interface-Peer, Local DNS, and Advanced Policies) via the WebUI. Data can be updated or exported to a .csv or .txt file, and this feature provides M2M integration with external routing and billing engines.

Reports

The BorderNet 4000 SBC generates reports to show traffic and operational information. Statistical data is stored locally on the BorderNet 4000 SBC for up to 1 week (7 days). Statistical reports are automatically calculated at defined intervals throughout the day. The BorderNet 4000 SBC WebUI supports filtering based on date range and allows an Operator to specify report intervals for data samples.

The BorderNet 4000 SBC activity is viewed based on operator-defined time intervals (5 minutes or 1 hour). Reports can be exported to Adobe PDF, Microsoft Word, or Microsoft Excel format via the WebUI.

The following screen is an example of the **Ethernet Link Utilization Report**:



The BorderNet 4000 SBC automatically generates the following reports:

- Ethernet link statistics
- Traffic statistics, including incoming and outgoing data on:
    - Answer to Seizure Ratio (ASR)
    - SIP and H.323 peers
    - SIP and H.323 interfaces
- Security statistics on packets, including the number of packets dropped because of overload, black-list, unaccepted ACL, no flow, or malformed packets

Tracing

The BorderNet 4000 SBC includes a customized plug-in that works with the Wireshark® trace tool. This customized tool captures, stores, and analyzes all SIP messages and IP traffic and provides tracing output in a *.pcap file. The BorderNet 4000 SBC supports two types of tracing: IP level tracing and session level tracing.

IP Level Tracing

IP level tracing captures IP traffic on Ethernet links. It supports multiple IP layer filters on parameters such as source/destination IP, protocol, and source/destination port.

Recording Profiles

Interface level tracing has four recording profiles:

1. Signaling with media
2. Signaling without media (except UDP ports greater than 5100)
3. Media drops (RTP packets dropped because of excessive rate, over-utilizing bandwidth, and so forth)
4. Flow drops (advanced rate limit packet drops)

Session Level Tracing

SIP session level tracing captures SIP messages at various stages of call processing. It supports multiple SIP layer filters on header parameters such as From, Contact, To, and Via.

SIP Parameter Filtering

Session level tracing allows operators to specify filtering criteria on the following parameters:

- Calling Party User
- Calling Party Domain
- Calling Party Scheme
- Called Party User
- Called Party Domain
- Called Party Scheme
- SIP Method, including Invite, Option, Register, and Subscribe

Recording Profiles

Session level tracing has four recording profiles:

1. Signaling without media
2. Signaling with media
3. Media dropped
4. Flows dropped

Media Capture

The BorderNet 4000 SBC supports media capture and recording. The WebUI displays basic RTP stream characteristics, and multiple media streams can be selected and played back.

11. Compliance Specifications

Specification	Details
RFC 1896	The text/enriched MIME Content-type
RFC 1889	RTP: A Transport Protocol for Real Time Applications
RFC 1890	RTP Profile for Audio and Video Conferences with Minimal Control
RFC 1918	Address Allocation for Private Internets
RFC 2029	RTP Payload Format of Sun's CellB Video Encoding
RFC 2032	RTP Payload Format for H.261 Video Streams
RFC 2035	RTP Payload Format for JPEG-compressed Video
RFC 2038	RTP Payload Format for MPEG1/MPEG2 Video
RFC 2045	Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
RFC 2046	Multipurpose Internet Mail Extensions (MIME) Part Two:Media Types
RFC 2047	MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text
RFC 2112	The MIME Multipart/Related Content-type
RFC 2183	Communicating Presentation Information in Internet Messages: The Content-Disposition Header Field
RFC 2190	RTP Payload Format for H.263 Video Streams
RFC 2198	RTP Payload for Redundant Audio Data
RFC 2231	MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations
RFC 2234	Augmented BNF for Syntax Specifications: ABNF
RFC 2246	The TLS Protocol Version 1.0
RFC 2250	RTP Payload Format for MPEG1/MPEG2 Video
RFC 2279	UTF-8, a transformation format of ISO 10646
RFC 2301	File Format for Internet Fax
RFC 2327	SDP: Session Description Protocol
RFC 2387	The MIME Multipart/Related Content-type
RFC 2396	Uniform Resource Identifiers (URI): Generic Syntax
RFC 2429	RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)
RFC 2435	RTP Payload Format for JPEG-compressed Video
RFC 2543	SIP: Session Initiation Protocol

RFC 2617	HTTP Authentication: Basic & Digest Access Authentication
RFC 2633	S/MIME Version 3 Message Specification
RFC 2658	RTP Payload Format for PureVoice Audio
RFC 2782	A DNS RR for specifying the location of services (DNS SRV)
RFC 2806	TelURL
RFC 2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
RFC 2854	The 'text/html' Media Type
RFC 2915	The Naming Authority Pointer (NAPTR) DNS Resource Record
RFC 2976	SIP INFO Method
RFC 3003	The audio/mpeg Media Type
RFC 3016	RTP Payload Format for MPEG-4 Audio/Visual Streams
RFC 3022	Traditional IP Network Address Translator (Traditional NAT)
RFC 3047	RTP Payload Format for ITU-T Recommendation G.722.1
RFC 3087	Control of Service Context using SIP Request-URI
RFC 3189	RTP Payload Format for DV (IEC 61834) Video
RFC 3190	RTP Payload Format for 12-bit DAT Audio and 20- and 24-bit Linear Sampled Audio
RFC 3204	MIME media types for ISUP and QSIG Objects (MIME Support)
RFC 3261	Session Initiation Protocol support
RFC 3262	Reliability of Provisional Responses in the SIP
RFC 3263	Session Initiation Protocol (SIP): Locating SIP Servers
RFC 3264	An Offer/Answer Model with Session Description Protocol (SDP)
RFC 3265	Session Initiation Protocol (SIP)-Specific Event Notification (Subscribe / Notify)
RFC 3267	Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs
RFC 3268	Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)
RFC 3272	Session Initiation Protocol for Telephones (SIP-T)
RFC 3311	The Session Initiation Protocol (SIP) UPDATE Method
RFC 3323	A Privacy Mechanism for the SIP
RFC 3324	Short Term Requirements for Network Asserted Identity
RFC 3325	Private Extensions to the SIP for Asserted Identity with Trusted Networks

	(Privacy Extensions)
RFC 3326	The Reason Header Field for the SIP
RFC 3329	Security Mechanism Agreement for SIP (Security Mechanism)
RFC 3362	Real-time Facsimile (T.38) - image/t38 MIME Sub-type Registration
RFC 3372	Session Initiation Protocol for Telephones (SIP-T): Context and Architectures
RFC 3389	Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN)
RFC 3427	Change Process for the Session Initiation Protocol (SIP)
RFC 3428	Session Initiation Protocol (SIP) Extension for Instant Messaging
RFC 3455	Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)
RFC 3515	The Session Initiation Protocol (SIP) Refer Method
RFC 3550	RTP: A Transport Protocol for Real Time Applications
RFC 3551	RTP Profiles for Audio and Video
RFC 3555	MIME Type Registration of RTP Payload Formats
RFC 3556	Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth
RFC 3558	RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV)
RFC 3581	SIP Extension for Symmetric Response Routing
RFC 3588	Diameter Base Protocol
RFC 3589	Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5
RFC 3596	DNS Extensions to Support IP Version 6
RFC 3629	UTF-8, a transformation format of ISO 10646
RFC 3640	RTP Payload Format for Transport of MPEG-4 Elementary Streams
RFC 3665	Session Initiation Protocol (SIP) Basic Call Flow Examples
RFC 3666	Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows
RFC 3711	The Secure Real-time Transport Protocol (SRTP)
RFC 3761	The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)
RFC 3764	enumservice registration for Session Initiation Protocol (SIP) Addresses-of-Record
RFC 3802	Toll Quality Voice – 32 Kbit/s Adaptive Differential Pulse Code Modulation (ADPCM) MIME Sub-type Registration

RFC 3803	Content Duration MIME Header Definition
RFC 3824	Using E.164 numbers with the Session Initiation Protocol (SIP)
RFC 3840	Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)
RFC 3842	A Message Summary and Message Waiting Indication Event Package
RFC 3891	The Session Initiation Protocol (SIP) "Replaces" Header
RFC 3892	The Session Initiation Protocol (SIP) Referred By Mechanism
RFC 3951	Internet Low Bit Rate Codec (iLBC)
RFC 3952	Real-time Transport Protocol (RTP) Payload Format for internet Low Bit Rate Codec (iLBC) Speech
RFC 3966	The tel URI for Telephone Numbers
RFC 3984	RTP Payload Format for H.264 Video
RFC 3986	Uniform Resource Identifier (URI): Generic Syntax
RFC 4028	Session Timers in the Session Initiation Protocol (SIP)
RFC 4040	RTP Payload Format for a 64 kbit/s Transparent Call
RFC 4123	Session Initiation Protocol (SIP)-H.323 Interworking Requirements
RFC 4175	RTP Payload Format for Uncompressed Video
RFC 4184	RTP Payload Format for AC-3 Audio
RFC 4234	Augmented BNF for Syntax Specifications: ABNF
RFC 4244	Extension to SIP to request history Information
RFC 4298	RTP Payload Format for BroadVoice Speech Codecs
RFC 4317	Session Description Protocol (SDP) Offer/Answer Examples
RFC 4348	Real-Time Transport Protocol (RTP) Payload Format for the Variable-Rate Multimode Wideband (VMR-WB) Audio Codec
RFC 4351	Real-Time Transport Protocol (RTP) Payload for Text Conversation Interleaved in an Audio Stream
RFC 4352	RTP Payload Format for the Extended Adaptive Multi-Rate Wideband (AMR-WB+) Audio Codec
RFC 4396	RTP Payload Format for 3rd Generation Partnership Project (3GPP) Timed Text
RFC 4421	RTP Payload Format for Uncompressed Video: Additional Color Sampling Modes
RFC 4566	SDP: Session Description Protocol
RFC 4569	Internet Assigned Number Authority (IANA) Registration of the Message Media Feature Tag
RFC 4572	Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)
RFC 4585	Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based

	Feedback (RTP/AVPF)
RFC 4587	RTP Payload Format for H.261 Video Streams
RFC 4588	RTP Retransmission Payload Format
RFC 4598	Real-time Transport Protocol (RTP) Payload Format for Enhanced AC-3 (E-AC-3) Audio
RFC 4612	Real-Time Facsimile (T.38) - audio/t38 MIME Sub-type Registration
RFC 4629	RTP Payload Format for ITU-T Rec. H.263 Video
RFC 4694	Number Portability Parameters for the "tel" URI
RFC 4695	RTP Payload Format for MIDI
RFC 4715	The Integrated Services Digital Network (ISDN) Subaddress Encoding Type for tel URI
RFC 4734	Definition of Events for Modem, Fax, and Text Telephony Signals
RFC 4749	RTP Payload Format for the G.729.1 Audio Codec
RFC 4788	Enhancements to RTP Payload Formats for EVRC Family Codecs
RFC 4855	Media Type Registration of RTP Payload Formats
RFC 4856	Media Type Registration of Payload Formats in the RTP Profile for Audio and Video Conferences
RFC 4867	RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs
RFC 4904	Representing Trunk Groups in tel/sip Uniform Resource Identifiers (URIs)
RFC 4961	Symmetric RTP / RTP Control Protocol (RTCP)
RFC 4964	The P-Answer-State Header Extension to the Session Initiation Protocol for the Open Mobile Alliance Push to Talk over Cellular
RFC 5031	A Uniform Resource Name (URN) for Emergency and Other Well-Known Services
RFC 5069	Security Threats and Requirements for Emergency Call Marking and Mapping
RFC 5079	Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)
RFC 5806	Diversion Indication in SIP
RFC 6086	Session Initiation Protocol (SIP) INFO Method and Package Framework
RFC 6140	Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)
RFC 6141	Re-INVITE and Target-Refresh Request Handling in the Session Initiation Protocol (SIP)
RFC 6337	Session Initiation Protocol (SIP) Usage of the Offer/Answer Model
ETSI TS 129 421 v8.1.0	Interworking between IM CN Sub-system and IP Networks
ETSI es_283 018	H.248 Profile for Controlling BGF in RACS

ETSI es_282 003	RACS Functional Architecture (for call flows and usage of H.248)
Media Handling Reference Specifications	
ITU-T H.248.37	IP NAPT Traversal Package
ITU-T H.248.40	Inactivity Detection
ITU-T H.248.43	Packages for gate
ITU-T H.248.52	QoS Support Packages
ITU-T H.248.53	Traffic Management