



## Product Description Guide

# Dialogic<sup>®</sup> BorderNet<sup>™</sup> Session Border Controller (SBC)

## Release 3.8.1

December 2019

# Table of Contents

1. Introduction
  - 1.1 Purpose of this Document
  - 1.2 Glossary
  - 1.3 References
  - 1.4 Contact Us
2. Overview
  - 2.1 Session Border Controller Overview
  - 2.2 Dialogic BorderNet SBC Overview
  - 2.3 Key Features
  - 2.4 Deployment Options
    - 2.4.1 COTS (Commercial Off The Shelf)
    - 2.4.2 Virtual BorderNet SBC
    - 2.4.3 Amazon Web Services (AWS)
    - 2.4.4 BorderNet Edge SBC
    - 2.4.5 BorderNet Scale Up/Scale Down Options
    - 2.4.6 BorderNet Scale Out/Scale In Options
  - 2.5 LDAP Configuration
  - 2.6 RADIUS User Authentication
  - 2.7 Product Specifications
3. Reference Network Topologies
  - 3.1 B2BUA Architecture
  - 3.2 Service Provider Access and Interconnect Scenarios
  - 3.3 IMS and VoLTE
  - 3.4 Transcoding
  - 3.5 Redundancy and High Availability
    - 3.5.1 Geo-Redundancy
    - 3.5.2 Connectivity
    - 3.5.3 Deployment Modes
  - 3.6 802.1Q VLAN (Virtual Local Area Network) Support
    - 3.6.1 Multiple IP Addresses Per VLAN
    - 3.6.2 Overlapped IP Address
4. Media Handling
  - 4.1 Signaling and Media Separation
  - 4.2 Media Latching
  - 4.3 Media Over Multiple Physical Interfaces
  - 4.4 Media Rate Limiting
  - 4.5 Topology Hiding for Media
  - 4.6 Policy Based Media Routing
  - 4.7 WebRTC Support
  - 4.8 Quality of Service (QoS)
  - 4.9 Media Statistics
  - 4.10 Supported Codecs and Methods

- 4.11 DTMF Relay
- 4.12 Codec Mapping
- 5. Security and Service Assurance
  - 5.1 L3/L4 Security Measures
    - 5.1.1 Packet Consistency Checks
    - 5.1.2 Fragmented IP Consistency Checks
    - 5.1.3 Protocol Consistency Checks
    - 5.1.4 Access Control Lists
    - 5.1.5 Advanced Packet Rate-Limiting
    - 5.1.6 Dynamic Packet Rate Adjustment
    - 5.1.7 Traffic Priority and Overload Protection
    - 5.1.8 Media Security
  - 5.2 Application Security
    - 5.2.1 IPsec Support
    - 5.2.2 TLS Support
    - 5.2.3 Malicious Behavior Handling
    - 5.2.4 Call Admission Control (CAC) Session Constraints
    - 5.2.5 HTTP Security
  - 5.3 SRTP and SRTCP Media Security
- 6. SIP Services
  - 6.1 SIP Application Layer Gateway
  - 6.2 SIP Profiler
  - 6.3 Provisional Response Acknowledgement (PRACK)
  - 6.4 Call Routing
    - 6.4.1 Local DNS
    - 6.4.2 External DNS Support
  - 6.5 Rerouting
    - 6.5.1 External Route Server (SIP Redirect Server)
    - 6.5.2 Local Number Portability (LNP)
    - 6.5.3 Matrix
    - 6.5.4 ENUM
  - 6.6 Access Features
  - 6.7 IP PBX Registration Support
  - 6.8 SIP Refer Handling
  - 6.9 Overload Management
  - 6.10 Emergency Call Handling
    - 6.10.1 SIP URN Routing for Emergency Services
    - 6.10.2 Border Control Function (BCF)
  - 6.11 Local Ring Back Tone
  - 6.12 UDP to TCP Automatic Transition
  - 6.13 Trunk Authentication
  - 6.14 Number Translation
  - 6.15 Directory Lookup Service
  - 6.16 Criteria Set Service
  - 6.17 SIP-REC
    - 6.17.1 SIPREC extensions to SIP and SDP

- 6.17.2 Metadata
- 7. IMS, VoLTE and IPX Support
  - 7.1 IMS and VoLTE
  - 7.2 Interworking Capabilities (I-BCF/TrGW)
  - 7.3 Mobile Interconnect and IPX Support
  - 7.4 Optimal Media Routing and Local Break Out
  - 7.5 TRF - Transit & Routing Function
- 8. Interworking Function (IWF)
  - 8.1 IPv4-IPv6 Interworking Function
  - 8.2 SIP, SIP-I, SIP-T Interworking
  - 8.3 H.323-to-SIP Interworking Function
    - 8.3.1 IWF Call Flow Support
    - 8.3.2 Early Media in SIP-to-H.323 Fast-Start Calls
    - 8.3.3 Response Code Mapping
    - 8.3.4 Calling Line Identification
  - 8.4 Diameter Ro and Rf Interfaces
  - 8.5 Diameter Rx Interface
- 9. Element Management System(EMS)
  - 9.1 EMS Dashboard
  - 9.2 Topology View
  - 9.3 Application Parameters
  - 9.4 Fault Management
  - 9.5 User Management
  - 9.6 Reports and Statistics
  - 9.7 Analytics
  - 9.8 Network Wide License Management
  - 9.9 Provisioning
- 10. Integrated Management
  - 10.1 Dashboard
  - 10.2 System Configuration
  - 10.3 System Audit
  - 10.4 Application Configuration
  - 10.5 SNMP Support
  - 10.6 SOAP/XML API Interface
  - 10.7 Monitor and Diagnostics
  - 10.8 Policy-Based Routing
  - 10.9 Trunk Group Routing/RFC 4904 Compliance
  - 10.10 Customized Session Detail Records
  - 10.11 Bulk Provisioning
  - 10.12 Reports
  - 10.13 Tracing
    - 10.13.1 IP Level Tracing
    - 10.13.2 Session Level Tracing
    - 10.13.3 Media Capture
- 11. Network Wide Licensing (NWL)
- 12. Dialogic Analytics

**13. Lawful Interception (LI)**

**14. Compliances and Certifications**

**14.1 Specifications Compliance**

**14.2 Certifications of Compliance**

**14.2.1 BroadSoft BroadCloud R22 Certification**

**14.2.2 SIPconnect 1.1 Compliance**

## Copyright and Legal Notice

Copyright © 2019 Dialogic Corporation. All Rights Reserved. You may not reproduce this document in whole or in part without permission in writing from Dialogic Corporation at the address provided below.

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 Corporation 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 Corporation at the address indicated below or on the web at [www.dialogic.com](http://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 3300 Boulevard de la Côte-Vertu, Suite 112, Montreal, Quebec, Canada H4R 1P8.

**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, Veraz, Brooktrout, Diva, BorderNet, PowerMedia, PowerVille, PowerNova, MSaaS, ControlSwitch, I-Gate, Cantata, TruFax, SwitchKit, Eiconcard, NMS Communications, SIPcontrol, Exnet, EXS, Vision, inCloud9, and NaturalAccess, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Corporation 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 3300 Boulevard de la Côte-Vertu, Suite 112, Montreal, Quebec, Canada H4R 1P8. 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.

#### Document History

Version #	Version Date	Update Description
1.0	January 2013	Release 3.0
1.1	June 2013	Release 3.1
1.2	December 2013	Release 3.2
1.3	February 2016	Release 3.3.1
1.4	February 2016	Release 3.4 – HP DL360 platform introduced.
1.5	May 2016	Release 3.4.1 – HDD size increased.
1.6	November 2016	Release 3.5.0 Added: <ul style="list-style-type: none"> <li>• Software transcoding</li> <li>• RTP media encryption</li> <li>• 10GB Interfaces to the BorderNet SBC 1U rack mount platform</li> <li>• COTS 2U rack mount DL380 platform</li> </ul>
1.6	November 2016	VM requirements modification
1.7	January 2017	Typo fixes
1.8	January 2017	Codecs list updated
1.9	January 2017	Corrections in power supply specifications

Version #	Version Date	Update Description
2.0	March 2017	<p>Updated for release 3.6.0</p> <ul style="list-style-type: none"> <li>• Hardware Transcoding</li> <li>• Implementation in AWS</li> <li>• Analytic Platform</li> <li>• Codecs G.722, G.726, and EVS narrow-band added to transcoding</li> </ul>
2.1	March 2017	<ul style="list-style-type: none"> <li>• Session and Performance update</li> <li>• Added KVM support</li> <li>• BorderNet SBC terminology replace the BorderNet SBC 4000</li> <li>• Figures have been updated</li> <li>• Added BorderNet Edge SBC</li> </ul>
3.0	September 2017	<p>Dialogic Analytic chapter modified. Updated for release 3.7.0 added:</p> <ul style="list-style-type: none"> <li>• SIP INFO in DTMF transcoding</li> <li>• Charging Correlation</li> <li>• Local Ring Back Tone</li> <li>• OMR and LBO</li> <li>• Refer message handling</li> <li>• Network Wide Licensing</li> </ul>
4.0	March 2018	<p>Updated for release 3.7.5 added:</p> <ul style="list-style-type: none"> <li>• TRF - Transit &amp; Routing Function</li> <li>• SIP UDP to TCP transition</li> <li>• Trunk Authentication</li> <li>• Number Translation</li> <li>• Directory lookup Service</li> <li>• Criteria Set Service</li> <li>• Update DTMF transcoding</li> <li>• Update TLS support added a CSR support for CA sign</li> <li>• SIP-REC</li> </ul>
4.1	June 2018	<p>Updated for release 3.7.5 added:</p> <ul style="list-style-type: none"> <li>• Adding BorderNet EMS</li> <li>• General enhancements</li> <li>• General editing issues</li> </ul>



Version #	Version Date	Update Description
4.2	December 2018	Updated for release 3.8.0 added: <ul style="list-style-type: none"><li>• Diameter Rx interface</li><li>• Fax transcoding</li><li>• Scale up/down</li><li>• Web RTC support</li><li>• Rerouting</li><li>• LNP</li><li>• Matrix</li><li>• ENUM</li></ul>
4.3	April 2019	BNET Edge on HP DL20 platform introduced. This is COTS which comes preinstalled by Dialogic.
4.4	June 2019	Updated for release 3.8.1. Added: <ul style="list-style-type: none"><li>• Geo-Redundancy</li><li>• SNMPv3 Support</li><li>• Scale in/out on Amazon</li><li>• NW Licensing with EMS</li><li>• EMS Provisioning</li><li>• LDAP Configuration</li><li>• RADIUS Authentication</li><li>• Codecs EVS and EVRC support</li></ul>

# 1. Introduction

## 1.1 Purpose of this Document

This Product Description is intended to familiarize the reader with the **Dialogic® BorderNet™ Session Border Controller (SBC)**, its features, and benefits.

## 1.2 Glossary

For the purposes of this document the following abbreviations apply:

Abbreviation	Meaning
AG	Application Gateways
AWS	Amazon Web Services
API	Application Programming Interface
ARPU	Average Revenue Per User
AS	Application Server
B2BUA	Back-to-Back User Agent
BGC	Border Gateway Controller
CAC	Call Admission Control
COTS	Commercial Off the Shelf
CS	Control Switch
DA	Digit Analysis
DCA	Data Collection Agents
DoS	Denial of Service
DSCP	Differentiated Services Codepoint
DSE	Directory Services Engine
DTMF	Dual Tone – Multi Frequency
ERS	Event Relay Server
EMS	Element Management System
GTT	Global Title Translation
HA	High Availability
HTML	Hypertext Markup Language

Abbreviation	Meaning
HTTP	Hypertext Transfer Protocol
LBO	Local Break Out
LRBT	Local Ring Back Tone
IBCF	Interconnection Border Control Function
IMS	IP Multimedia Subsystem
IMT	Inter-Machine Trunk
IN	Intelligent Network
IP	Internet Protocol
IPsec	Internet Protocol Security
IPX	IP Exchange
IWF	Interworking Function
LSG	LNP Signaling Gateway
MRC	Media Resource Controller
NAT	Network Address Translation
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NFV-MANO	Network Functions Virtualization Management and Orchestration
NFVO	Network Function Virtualization Orchestrator
NGN	Next Generation Network
NWL	Network Wide Licensing
OMR	Optimal Media Routing
QoS	Quality of Service
RTCP	RTP Control Protocol
RTP	Real-Time Transport Protocol
RSG	Routing Signaling Gateway
RTC	Real-Time Communication
SBC	Session Border Controller
SCCP	Signaling Connection Control Part
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol

Abbreviation	Meaning
TCAP	Transaction Capabilities Application Part
TCAPSE	Transaction Capabilities Application Part Signaling Element
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRF	Transit and Roaming Function
UDP	User Datagram Protocol
UE	User Equipment
VLAN	Virtual Local Area Network
vCPU	Virtual CPU
VIM	Virtual Infrastructure Manager
VNF	Virtual Network Function
VNFC	Virtual Network Function Component
VNFM	Virtual Network Function Manager
VoIP	Voice over IP
VoLTE	Voice over LTE
VPC	Virtual Private Cloud
XML	eXtensible Markup Language

Table 1-1: Glossary

## 1.3 References

- [1] BorderNet SBC Transcoding User's Guide
- [2] BorderNet SBC SRTP User's Guide
- [3] BorderNet SBC Element Management System (EMS) User's Manual

## 1.4 Contact Us

For a list of Dialogic locations and offices, please visit: <https://www.dialogic.com/contact>.

## 2. Overview

### 2.1 Session Border Controller Overview

Today's fixed line and mobile **Real-Time Communication (RTC)** Service Providers of all types are experiencing significant business challenges causing them to re-evaluate existing business models while continually innovating and transforming their businesses both technically and commercially.

Challenges include:

- Declining wholesale revenues and declining **Average Revenue Per User (ARPU)**.
- High ratio of capital and operating expenses to revenue.
- Interoperability and interworking with many types of networks, protocols and media.
- Competition from new cloud-based Service Providers with innovative and highly competitive business models.

Confronted with these challenges, RTC Service Providers are compelled to find ways to deliver new revenue generating services that include SIP PBX trunking solutions, IMS VoLTE services with roaming, and competitive “over-the-top” and WebRTC-based services.

Global wholesale Service Providers are transforming their business models from providing basic TDM and VoIP interconnect services to becoming **IP exchange (IPX)** or interconnection providers for the exchange of IP-based RTC traffic between customers of both mobile and fixed operators as well as between other types of IP Service Providers using “all-IP” interconnection models.

**Session Border Controllers (SBCs)** have been developed over the past decade to solve the challenging, diverse, and complex task of securely interconnecting and reliably delivering all types of IP-based real-time audio and video services. As traditional high-scale mobile and fixed line voice networks have evolved to **IP Multimedia Subsystem (IMS)** networks the SBC has become an essential network element providing secure interconnection between IMS networks and other IP-based networks.

SBCs are also relied upon to provide secure access-oriented services that depend on end-to-end IP service continuity for all types of mobile and fixed network user equipment (UE). The SBC secures IP-based application servers (AS) delivering these access services from within both IMS core and VoIP Service Provider networks of all types.

Due to the heavy processing and media handling demands placed on SBCs they have historically been built and deployed as purpose-built platforms on customized hardware. High reliability and High Availability are typically architected directly into these platforms to ensure continual service delivery even under fault conditions.

Service Provider engineering staff use capacity planning and conservative deployment models to ensure continual service delivery under high network load conditions. Real-time telecommunication infrastructure elements like SBCs are typically over-provisioned by 30-50% in an attempt to ensure that individual SBCs are never overwhelmed by network-degrading traffic spikes that can impact customer **Quality of Experience (QoE)**.

As Service Providers begin migrating to virtualized communication infrastructure, virtual SBCs are expected to provide high quality performance and deterministic operational characteristics similar to purpose-built platforms.

In most cases, today's virtual SBCs are perpetuating past architectures in an attempt to maintain performance and high QoE in two different fundamental ways:

- By returning to the multi-layer **Next Generation Network (NGN)** architecture of separating signaling and media handling onto a separate virtual network infrastructure.
- By modeling internal purpose-built platform architectures in the virtual environment by statically pre-allocating compute platform virtual CPUs (vCPUs) for different flow types to ensure virtual network infrastructure is not overwhelmed by any single high-intensity packet flow or processing requirement, such as signaling and media encryption.

In some cases, in an attempt to maintain performance and high QoE, both separation of signaling and media onto separate infrastructure and the pre-allocation of compute platform vCPU resources are combined to drive the highest levels of potential inefficiency.

This return to past architectures weakens the business case to transition from appliance-based SBCs to virtualized SBCs and raises questions regarding the long-term viability of moving SBCs to cloud deployment models.

Static resource pre-allocation models drive higher operational and capital costs by putting the engineering and monitoring burden on the SBC operator while simultaneously creating the likelihood for significant resource under-utilization as traffic profiles and associated processing requirements vary over time across specific virtual SBC compute infrastructures.

Today's real-time communication Service Providers are looking for ways to sustain their existing businesses by reducing capital and operational costs while simultaneously building new lower-cost cloud-based services that can scale geographically with traditionally high customer QoE. The architectures and associated business models of the past are under significant pressure to change.

## 2.2 Dialogic BorderNet SBC Overview

The **Dialogic® BorderNet™ Session Border Controller (SBC)** provides comprehensive and secure signaling, call control, and media termination for both VoIP and IMS-based mobile and fixed line network operators.

The **BorderNet SBC** provides call signaling, control and media termination in a VoIP network. It is deployed on the border of a network, managing the incoming and outgoing signaling and media traffic for service providers that require call session control and network security.

The BorderNet SBC provides an integrated Web UI that contains management for **Fault, Configuration, Accounting, Performance and Security (FCAPS)** functionality and monitoring capabilities to perform system management tasks, using the following browsers:

- **Internet Explorer (v8,v9,v10) Note: IE 11 is not supported.**
  - **Mozilla Firefox (v5 and above)**
  - **Google Chrome**
1. The BorderNet SBC is typically deployed on core network edges to securely interconnect Service Provider networks as well as on the demarcation between Service Providers and enterprises for SIP trunking services.
  2. The BorderNet SBC manages incoming and outgoing signaling and media traffic for peering between all types of mobile and fixed line networks, as well as for access service delivery to mobile and fixed line user equipment (UE).
  3. The BorderNet SBC assures revenues by securing and protecting application servers from malicious entities and attack.

4 The BorderNet SBC enables new revenue opportunities and speeds time-to-revenue by providing extensive protocol normalization and interworking for both interconnect and access networks, thereby ensuring that VoIP networks and applications of all types can communicate and interwork with each other.

5. The BorderNet SBC protects revenue generation by concealing internal private network topology, managing bandwidth usage, and prioritizing call sessions for both network interconnections and for service delivery to individual UE.

6. The BorderNet SBC software delivers industry-leading performance while simultaneously reducing Service Provider virtual SBC total cost of ownership (TCO) by efficiently and effectively leveraging today's powerful multi-core compute platforms in a way that automatically enables superior network infrastructure resource utilization.

7. The BorderNet SBC software has been architected to dynamically distribute processor loads across all platform vCPUs while simultaneously protecting each vCPU from overload. The highest level of performance is achieved without the typical manual, tedious and recurring engineering costs associated with designing, deploying and operating today's current virtual SBCs

Common BorderNet SBC software increases Service Provider agility by supporting a wide range of current and evolving deployment models with the same SBC software, while delivering efficient high performance across all of these models. Deployment models range from deploying on pre-qualified and benchmarked X86-based multi-core COTS platforms to deploying on generic network virtualization infrastructure with a variety of virtualization technologies for both public and private cloud, including **Network Function Virtualization (NFV)**.

Increased agility through ease of media interworking is achieved by methods such as Codec transcoding and transrating, which can be performed both natively within the BorderNet SBC software or through on-board DSP resources in the COTS deployment model. All integrated BorderNet SBC media handling is based on 30 years of DSP and in-house media expertise, resulting in industry leading efficiency and quality with a highly attractive cost model that lowers the performance and cost barriers to implementing software-based transcoding in forward looking cloud and NFV environments.

The virtual BorderNet SBC enables operators to achieve maximum financial benefit from their network compute infrastructure investment by supporting a dynamic compute resource allocation model.

Common BorderNet SBC software, whether deployed on a COTS platform or as a virtual cloud-based element, creates owner/operator value and agility with lower TCO and investment protection through unique architectural advantages and unparalleled in-house media expertise. The evolving BorderNet SBC software protects and future-proofs operator investments today, by enabling operators to deploy on COTS today and gradually evolve through virtualization to a private, public, or NFV-based cloud without losing their investment in software licensing or operational knowledge base.

The all-software BorderNet SBC is designed to meet today's VoIP network access and peering challenges while seamlessly evolving to support cloud models of all type.

The **Cloud BorderNet SBC** is successfully installed and deployment in the **Amazon Web Services (AWS) Virtual Private Cloud (VPC)**, using **Amazon Elastic Computing Cloud (EC2)** resources and tools.

The BorderNet SBC can be peered with the customer's User Agents, located in different VPCs, using any BorderNet SBC service for any network.

## 2.3 Key Features

The BorderNet 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 interworking
- Media Security (SRTP and SRTCP)
- Transcoding
- Integrated web-based management for operations, administration and maintenance (OAM)
- Interworking between SIP, SIP-I and SIP-T
- Statistics, reports and alarms
- Lawful Interception
- Recording service
- Local Ring Back Tone
- OMR (Optimal Media Routing) and LBO (Local Break Out)
- Network Wide Licensing (NWL)
- Element Management System. Simultaneous and comprehensive management tool for handling up to one hundred BorderNet SBCs

The BorderNet SBC supplies comprehensive, multi-layer session-to-packet security and protection for OSI Layers 3, 4, 5, 6 and 7.

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

## 2.4 Deployment Options

The **Dialogic BorderNet SBC** is common software that can be used in different deployment types.

The BorderNet SBC, whether deployed on a COTS platform, virtual SBC or Amazon Web Services (AWS), delivers fully redundant, high-availability session control and security for interconnect applications, including secure IP peering.

The BorderNet 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.
- prioritizes call sessions.

### 2.4.1 COTS (Commercial Off The Shelf)



The BorderNet SBC COTS platform is based on the HP DL380 Gen10 platform. DL20 is for the BorderNet Edge SBC and comes preinstalled by Dialogic.

Specifications concerning COTS platform scale and performance are provided here:

## BorderNet SBC COTS Platform Scale and Performance



Performance Metric	BorderNet SBC (Enterprise) HP DL20	BorderNet SBC (High Scale) HP DL380
Concurrent Sessions (signaling & media)	Up to 5,000	100,000 <sup>1</sup> G.729 / 75,000 G.711
Concurrent Sessions (TLS/SRTP)	Up to 5,000 (SRTP – RTP)	20,000 (SRTP – RTP)
Sessions/Sec (SPS)	300	1,000
IP Interfaces (signaling & media)	2,048	2,048
Access: Subscribers	128,000	Up to 256,000
Access: Registrations	1,000 per second	1,600 per second; 3,610 refreshes per second
SIP Interfaces	500	500
VLANs	1,024	1,024
Peers	4,000	4,000
Profiles	1,024	1,024
Local DNS Entries	65,000	65,000
Policies	5,000	5,000

COMPANY CONFIDENTIAL © COPYRIGHT 2018 DIALOGIC CORPORATION. ALL RIGHTS RESERVED. V4 14-19.

1) Full calls, 20 msec, 10 Gb Interface; performance varies with network and traffic profiles

1

Specifications	HP DL20 Gen10 Server (Enterprise)	HP DL380 Gen10 Server (High Scale)
Signaling and Media Interfaces	3 x 1 Gb (1 x Private, 2 x Public)	8 x 1 Gb or 4 x 10Gb
High Availability (HA) Interfaces	-	2 x 1 Gb
Management Interfaces	1 x 1 Gb (Management and HA)	2 x 1 Gb
Processor	Intel® Core™ i3-8300 (4 core, 3.7 GHz, 12MB, 62W)	Intel® Xeon® Silver 4114 Processor (10 core, 2.2 GHz, 85W)
Memory	8 GB	64 GB
Expansion Slots	-	6 PCIe slots (4 slots for transcoding cards)
Form Factor	1 Rack Unit (RU)	2 Rack Units (RU)
Dimensions without Bezel (H x W x D)	1.70 x 17.11 x 15.05 in 4.32 x 43.46 x 38.22 cm	17.54 x 28.75 x 3.44 in 44.55 x 73.02 x 8.73 cm
Weight	9.46 kg (20.86 lbs.)	12.25 kg (27 lbs.)

For more details on COTS platforms, see BorderNet SBC Installation Guidelines.

## 2.4.2 Virtual BorderNet SBC

- The **Virtual BorderNet SBC** operates in a hypervisor environment on a generic Intel x86 server virtual network infrastructure. Leading hypervisors, such as KVM/VMware vSphere v5.0 or later are supported. The minimum 2 virtual CPU configuration can be deployed to support thousands of signaling and media sessions on minimal virtual network infrastructure that includes virtual CPU, memory, storage and network interfaces.

- The Virtual BorderNet SBC can be either scaled up or scaled out as desired. Scale up is accomplished by increasing virtual CPU speed and/or quantity along with associated memory and storage to increase both concurrent sessions and sessions per second performance per SBC instance.
- Media and signaling bandwidth requirements must be calculated and the appropriate Ethernet interfaces must be supported on the virtual network infrastructure. **Dialogic** can assist in these calculations and in determining the appropriate network infrastructure interfaces.
- The Virtual BorderNet SBC can be easily scaled out by instantiating multiple software instances across a common network infrastructure configuration to support multiple SBCs of similar performance and scale.

## 2.4.3 Amazon Web Services (AWS)

The solution components are instantiated within an Amazon VPC (Virtual Private Cloud) using Amazon EC2 API and tools and set up to provide Session Initiation Protocol (SIP) interfaces towards a Service Provider's Application Servers (AS), access servers, as well as other fixed and mobile networks of other peering network operators. The Amazon EC2 tools provide the ability to efficiently scale up/down and scale in/out the solution components as needed.

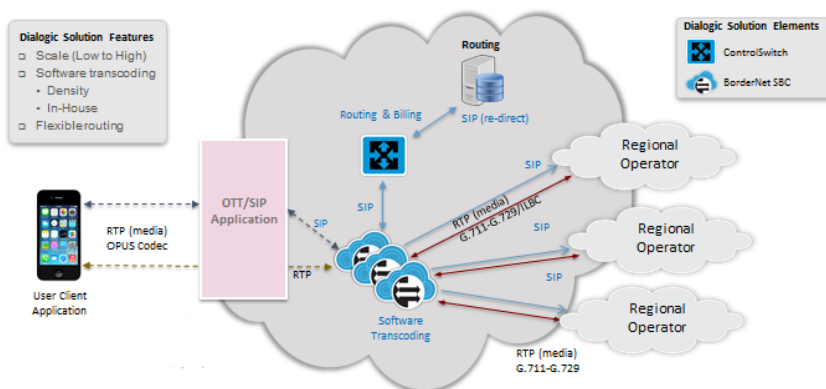


Figure 2-1: BorderNet *Single-Software* SBC in Amazon EC2

### 2.4.3.1 Virtualized Session Border Controller-AWS

The BorderNet SBC is an all-software platform that supports multiple session control functions including routing, protocol mediation and manipulation and transcoding. It serves as the front end to the public network, and also provides security features between the customer's network and the various end points in other connected Service Provider networks. SIP header manipulation with the BorderNet SBC is highly flexible and makes the task of modification and normalization of tags, headers and SDP parameters of SIP messages that traverse the network boundary easier.

The BorderNet SBC's SIP-Profiler feature operates on dialog transactions and sessions to increase security, protect mission critical infrastructure, and enable service continuity and delivery. The customer is required to define specifically the SIP trunk parameters and features otherwise traffic will be blocked.

### 2.4.3.2 Service Infrastructure-AWS

The elements that make up the virtualized infrastructure to deliver a voice service are illustrated in Figure 2-3 below. In this scenario the functional modules that make up the call control platform and SBC are deployed in virtual machines in a self-contained VPC. It connects to another VPC where various virtualized application, Local Number Portability (LNP), authentication, routing and access gateway network functions are deployed in support of the customer's overall VoIP service.

The media and signaling traverse the two VPCs through separate interfaces. The Dialogic solution includes the required interfaces on the ControlSwitch System to communicate with the applicable customer's servers to support the various call flows.

The below figure details the **ControlSwitch** System components used to deliver a SIP protocol-based service.

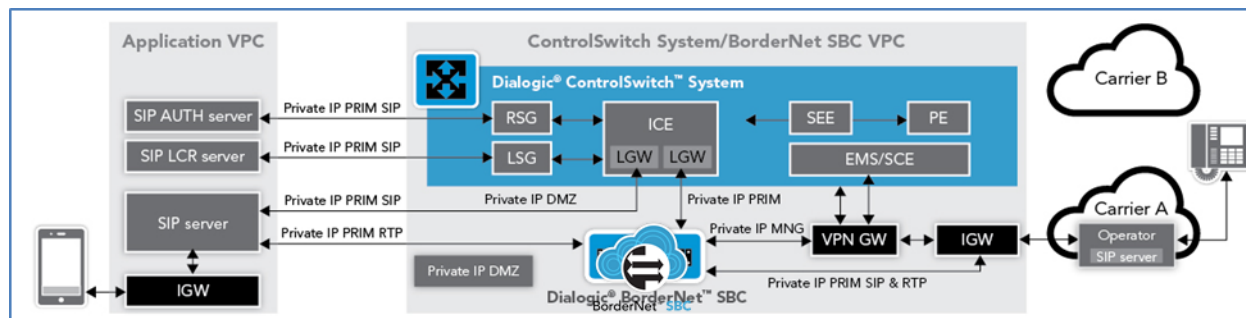


Figure 2-2: VoIP Service infrastructure using two Amazon VPCs

## 2.4.4 BorderNet Edge SBC

**Dialogic's** future-proof all-software **BorderNet Edge vSBC** reduces Service Provider CAPEX and OPEX while enabling future-proof deployment models based on x86 COTS platforms, private Cloud (VMWare), public Cloud (Amazon EC2) and NFV.

Today's real-time communication Service Providers are looking for ways to sustain their existing businesses by reducing capital and operational costs while building new lower-cost cloud-based services that can scale geographically and provide customers with a high quality of experience (QoE).

Service delivery architectures and legacy business models are being challenged by Cloud offerings and are under significant pressure to change.

**Dialogic's** future-proof all-software BorderNet Edge vSBC meets Service Providers' secure Enterprise Access and SIP Trunking connectivity requirements with an attractive range of cloud-based deployment options and business models.

The BorderNet Edge SBC provides:

- 25 to 1000 sessions
- Up to 10,000 registered users
- Software-based encryption: IPsec, TLS, SRTP
- Software-based transcoding up to 100 sessions
- System, network and peer level MOS reports based on R-Factor
- HA redundancy
- SIP, H.323
- COTS, VMware, Amazon (Xen), KVM

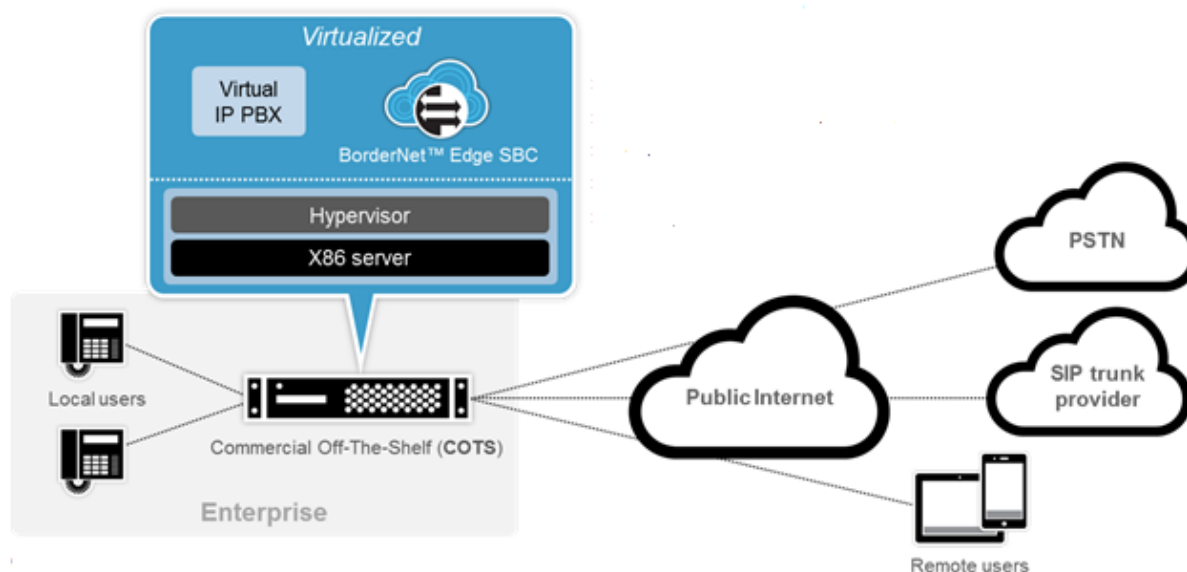


Figure 2-3: BorderNet *Single-Software* SBC for the Enterprise Premise

## 2.4.5 BorderNet Scale Up/Scale Down Options

The BorderNet SBC can be scaled up and down (vertical scaling) according to system requirements. Both actions require that the server be shut down and restarted.

- **Scale Up** refers to the addition of resources to the existing system such as CPU, memory, storage.
- **Scale Down** refers to a downgrade to a less powerful machine type.

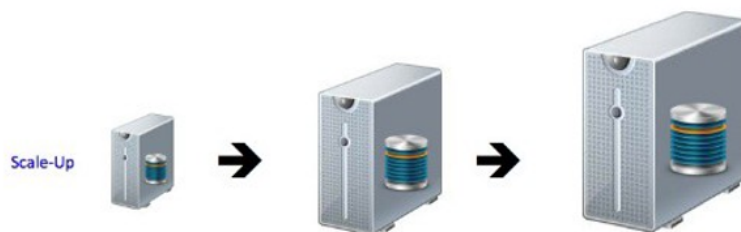


Figure 2-4: Scale Up

**Scale Up** and **Scale Down** work only on AWS and require a failover procedure initiated by the active platform. This will terminate calls which have not yet been answered and also active calls using TCP or TCP-based signaling protocol, including TCP, TLS and WebSocket.

Once the new instance with the new machine type has become the Active platform, the new instance process is conducted again on the current Standby system, in order for both the Active and Standby platforms to have the same instance type.

The following process is necessary:

- Shut down the Standby system (the system with the previous machine type).
- Change the instance type to the new machine type chosen.

- Load the new instance with the BorderNet configuration.

After synchronization the process is complete.

#### NOTES:

- If the measured value of CPU utilization is **equal or above** the value set in the **CPU Utilization Threshold (%)** parameter, AND if it is kept at that level for a duration equal or more than the time set in the **Threshold Contiguous Time (sec)** parameter, then a switch machine type procedure shall be triggered, with a machine type value taken from the **Scale-Up** configuration.
- If the measured value of CPU utilization is **equal or below** the value set in the **CPU Utilization Threshold (%)** parameter, AND if it is kept at that level for a duration equal or more than the time set in the **Threshold Contiguous Time (sec)** parameter, then a switch machine type procedure shall be triggered, with a machine type value taken from the Scale-Down configuration.
- After having one machine type already migrated to the new instance type, the process of migrating the second platform should only be conducted once.
- After both platforms have migrated to the new instance type there is no extra failover required.

The **Scale Up** and **Scale Down** actions are directly controlled from the GUI through the **Edit Scalability Profile** window.

**Scale UP/DOWN configuration**

Enable:

**Scale Up Parameters**

Cpu Utilization Threshold (%)

Concurrent Session Threshold

Threshold Configuration Time (Sec)

Machine Type

**Scale Down Parameters**

Cpu Utilization Threshold (%)

Concurrent Session Threshold

Threshold Configuration Time (Sec)

Machine Type

Figure 2-5: Editing Scale Up/Down Parameters

## 2.4.6 BorderNet Scale Out/Scale In Options

The BorderNet SBC can be scaled out and in (horizontal scaling) according to system requirements. Both actions require that the server be shut down and restarted.

- **Scale Out** refers to the addition of servers to the existing server or multiple servers. It requires support of a distributed architecture, where the workload is balanced between the different servers. Scalability can be architected into the system, so it is not automatic and is generally more challenging than Scaling Up.
- **Scale In** refers to the process in which a set of servers are removed (brought down), leaving a lower number of servers (or even a single one) in an operational state



Figure 2-6: Scale-Out

**Scale Out** and **Scale In** work only on AWS and require a failover procedure initiated by the active platform. This will terminate calls which have not yet been answered and also active calls using TCP or TCP-based signaling protocol, including TCP, TLS and WebSocket.

The following limitations refer to the scope for Scale Out/Scale In on the BorderNet SBC:

- Only Amazon (AWS) is supported.
- Only a concurrent sessions indicator is used as a threshold parameter for scaling decisions.
- Abnormal scenarios, such as a new instance which is not able to become active or is not responsive, are not handled in the current phase.
- Changing configuration at runtime is not part of the current phase. This will be implemented after the full integration of EMS.
- New instances are not yet configured. A change of configuration will be done only in a full scale-in state where only the redirect BorderNet is up.
- In the current phase, only the first redirect can be deployed in a High Availability configuration. All new instances will be deployed as standalones.

The **Scale Out** and **Scale In** actions are directly controlled from the GUI through the **Edit Scalability Profile** window.

### Scale IN / OUT configuration

Enable:	<input checked="" type="checkbox"/>
Scale AMI name	<input type="text" value="ami-00b50551c9f811760"/>
Machine Type	<input type="text" value="c4.xlarge"/>
Scale IN Concurrent Session Threshold	<input type="text" value="100"/>
Scale IN Threshold Configuration Time (Sec)	<input type="text" value="180"/>
Scale OUT Concurrent Session Threshold	<input type="text" value="300"/>
Scale OUT Threshold Configuration Time (Sec)	<input type="text" value="60"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Figure 2-7: Editing Scale Out/In Parameters

## 2.5 LDAP Configuration

**LDAP (Lightweight Directory Access Protocol)** is a software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet.

On TCP/IP networks, the **Domain Name System (DNS)** is the directory system used to relate the domain name to a specific network address (a unique location on the network). LDAP allows you to search for an individual on the network without knowing where they're located.

An LDAP directory can be distributed among many servers. Each server can have a replicated version of the total directory that is synchronized periodically. An LDAP server is called a **Directory System Agent (DSA)**. An LDAP server that receives a request from a user takes responsibility for the request, passing it to other DSAs as necessary, but ensuring a single coordinated response for the user.

LDAP uses a relatively simple, string-based query to extract information from MS Active Directory. A regular end user will never have to manually perform an LDAP query, because Outlook is LDAP-enabled and knows how to perform all the necessary queries on its own.

BorderNet supports a TLS/LDAPS secure connection and the default port for the secure LDAP is 636. Certificates received from the LDAP server are automatically accepted by BorderNet and EMS. No customized role attribute is required as role definition is performed based on role groups and the user's association to a role group.

In BorderNet the group names match the pre-defined roles available on the BorderNet. In order to support different privileges options for different BorderNets, the customer can define groups with the BorderNet pre-defined roles prefixed with a string. For example: IL\_SYSTEM\_ADMIN and US\_SYSTEM\_ADMIN. The BorderNet has an optional prefix parameter (example: prefix=IL, prefix=US)

In the EMS new roles are created with new names, so the customer can either create a new group or use an existing one. There is no need for a group prefix. The EMS roles can be customized and there is a single EMS on a network.

The Authentication process works as follows:

- Search the user.
- If a 'member of' attribute is available, then this attribute lists all the groups this user belongs to. (No need to search for groups, they are already listed).
- If a 'member of' attribute does not exist, then search all the groups to find the ones containing this user.
- Use the list of groups as a list of roles.
- The group list can contain also other group names in the tree, so it will ignore any unknown role name.
- Order of authentication – local users, LDAP, RADIUS.
- The required parameters are shown in the table below.

Parameter Name	Description	Mandatory	Optional Values	Default Value
Enable	Enable/disable LDAP configuration. Type: checkbox.		Checked/unchecked	Disable (not checked)
Connection				

Parameter Name	Description	Mandatory	Optional Values	Default Value
<b>LDAP Server IP</b>	IP address of the LDAP server	Yes	IPv4 address	None
<b>LDAP Server Port</b>	TCP port number of the LDAP server	Yes	0-65535	389
<b>Use TLS</b>	Enable secure connection using LDAP over TLS (usually over port 636) Type: checkbox.		Checked/unchecked	Disable (not checked)
<b>Admin DN</b>	A user with privilege to access the LDAP server directory. A full path is required.	No	String. Example: CN=Administrator,CN=Users DC=dialogic,DC=com	None
<b>Admin password</b>	Password of Admin user. Should be hidden (the user should see ‘*’ signs and not the real password)	No	String	None
Users				
<b>Users base DN</b>	Search scope to look for users (search starting with this point/ under this branch)	Yes	String CN=Users,DC=dialogic,DC=com	None
<b>User identification attribute</b>	Attribute type to uniquely identify a user. This is the attribute that will be used as the login identifier. Usually ‘uid’. For AD it will be sAMAccountName	Yes	String	uid
Groups				
<b>Group membership attribute</b>	Attribute of a user entry listing all the groups this user is associated with.	No	String	memberOf
<b>Groups base DN</b>	Search scope to look for groups containing the user (search starting with this point/ under this branch)	Yes	String Example: CN=Guests,DC=dialogic,DC=com	None
<b>Group identification attribute</b>	Attribute type to uniquely identify a group (a group search filter). This is the attribute that will be used as the group name which is mapped to an access level role.	Yes	String Example: CN	None
<b>Only on BorderNet: Group name prefix</b>	String placed before the ‘group identification’ and removed by the BorderNet. Used for flexible provisioning of several groups with several prefixes on the LDAP server.	No	String	None



## 2.6 RADIUS User Authentication

**Remote Authentication Dial-In User Service (RADIUS)**, was originally designed to deliver AAA services for dial-up internet. As such, most of its parameters are network access oriented and are aimed to supply different networking properties for the user accessing the network services. Typical parameters include service type, protocol type, IP address to assign the user (static or dynamic), access list to apply, or a static route to install in the NAS routing table.

A **Network Access Server (NAS)** operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response which is returned.

The RADIUS server response includes a list of attribute-value pairs that describe the parameters to be used for a session.

As part of its authentication capabilities, the RADIUS protocol is widely used for user authentication which is not necessarily related to network access. On top of the regular PAP/CHAP password authentication, it can also support a variety of other user authentication protocols like EAP-TTLS, EAP-TLS and PEAP.

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and the RADIUS server, to eliminate the possibility that someone snooping on an unsecure network could determine a user's password.

RADIUS uses UDP as the transport layer, and therefore it implements reliability options on the application (RADIUS) level. If no response is returned within a predetermined length of time, the request is re-sent a number of times. The client can also forward requests to an alternate server or servers in the event that the primary server is down or unreachable.

RADIUS message types include the following:

- **Access-Request** - This is the first message sent from the client to the server, asking permission to access the network. It contains user and network information for authentication and authorization. An Access-Request can include multiple attributes, each containing some information regarding the requested service.
- **Access-Accept** - Sent from the server to the client, granting permission to access the network. An Access-Accept message can provide specific configuration information for the client, such as IP address, QoS profile, user authorization or any other attribute needed.
- **Access-Reject** - Sent from the server to the client, denying permission to access the network. Can include reject cause and a message to the user.
- **Access-Challenge** - Sent by the server to issue a challenge to which the user must respond. The client then re-submits its original Access-Request with the extra information required by the Access-Challenge.

## 2.7 Product Specifications

The below table describes the product specifications.

PRODUCT SPECIFICATIONS
Protocols

PRODUCT SPECIFICATIONS	
Supported Signaling Protocols	<ul style="list-style-type: none"> <li>• SIP</li> <li>• SIP-I</li> <li>• H.323</li> </ul>
Other Protocols	<ul style="list-style-type: none"> <li>• IPv4, UDP, TCP, TLS, IPv6</li> <li>• RFC 768, 1889, 3550 RTCP RTP</li> <li>• RFC3711, SRTP, and SRTCP</li> <li>• RFC 3551 - RTP Profile for Audio and Video Conferences</li> <li>• 3GPP Interfaces: Mx, Mw, Gm, Ici, Izi</li> </ul>
Features	
Security	<ul style="list-style-type: none"> <li>• Access control — signaled pinhole firewall for media</li> <li>• Network topology hiding via double NATP for both signaling messages (layer 5) and media flows (layer 3 – including RTCP)</li> <li>• NAT traversal</li> <li>• DoS and overload protection for service infrastructure—rate limiting signaling messages and media flows</li> <li>• Session constraint enforcement</li> </ul>
Session Admission Control	<ul style="list-style-type: none"> <li>• License control</li> <li>• Session rate as configured on the interface and/or peer</li> <li>• Auto black-listing when the limit is exceeded</li> </ul>
IMS, IPX and VoLTE	<ul style="list-style-type: none"> <li>• Interconnect Border Control Function (I-BCF)</li> <li>• Transition Gateway (TrGW)</li> <li>• Integrated Border Function (I-SBC)</li> <li>• Interworking Function (IWF)SIP and SIP-I/SIP-T Interworking</li> <li>• Charging correlation</li> <li>• OMR (Optimal Media Routing) and LBO (Local Break Out)</li> </ul>
VLAN Bridging	<ul style="list-style-type: none"> <li>• 802.1q (LAN)</li> <li>• 1024 VLANs (supports multiple IPs for each VLAN)</li> </ul>
Bandwidth Policing	<ul style="list-style-type: none"> <li>• Media profiling and usage monitoring</li> <li>• Dynamic bandwidth limiting</li> <li>• Media packet rate monitoring and limiting based on media profile characteristics</li> <li>• Bandwidth determination from SDP (limit defined by configuration)</li> </ul>

## PRODUCT SPECIFICATIONS

Routing	<ul style="list-style-type: none"> <li>• Interface/interface static routing</li> <li>• Peer/interface-based static routing</li> <li>• SIP message-based routing</li> <li>• Local DNS table for URI to IP address and port mapping</li> <li>• Load-balancing and priority-based routing</li> <li>• Connectivity with peers</li> <li>• SIP Redirect Server</li> <li>• Policy Based Routing</li> <li>• Routing resolution through external DNS (SRV, A, NAPTR)</li> <li>• RFC 4904 Trunk Group Routing support</li> <li>• Multi-tenant routing table support</li> <li>• Emergency service call routing and call prioritization</li> <li>• SIP URN Routing</li> <li>• Dynamic SIP REFER Processing</li> </ul>
Media Routing	<ul style="list-style-type: none"> <li>• Media termination</li> <li>• Separation of signaling and media over VLANs</li> <li>• Media NAT traversal</li> <li>• QoS (including DSCP)</li> </ul>
Media Interworking	<ul style="list-style-type: none"> <li>• Transcoding between different Codecs</li> <li>• Packetization</li> <li>• DTMF transfer modes, and between T.38</li> <li>• Fax pass-through</li> </ul>
Reporting	<ul style="list-style-type: none"> <li>• QoS metrics—packets lost, jitter inter-arrival, latency</li> <li>• Policy enforcement: DSCP marking, ToS Marking</li> <li>• Traffic statistics—total packets and octets transferred, rFactor and more.</li> </ul>

**PRODUCT SPECIFICATIONS**

Performance and Capacity	Performance Metric	Virtual 2 vCPU	Virtual 8 vCPU	Virtual 8 vCPU	Virtual 16 vCPU	Virtual 32 vCPU
	Concurrent Sessions	1,2 <sup>4</sup> ,000	1,2 <sup>12</sup> ,000	1,3 <sup>30</sup> ,000	1,3 <sup>60</sup> ,000	1,3 <sup>90</sup> ,000
	Concurrent Sessions (TLS/SRTP)	1,2,4 <sup>500</sup>	1,2,4 <sup>3,000</sup>	1,3,4 <sup>3,000</sup>	1,3,4 <sup>12,000</sup>	1,3,4 <sup>18,000</sup>
	Packets Per Second (pps)	200,000	500,000	1,600,000	3,000,000	5,000,000
	Access (subscribers)	5,000	64,000	64,000	64,000	64,000
	Performance Metric	<b>COTS - HP (1Gb I/F)</b>	COTS - HP (10Gb I/F)			
	Concurrent Sessions	1 <sup>50</sup> ,000	1 <sup>100</sup> ,000			
	Concurrent Sessions (TLS/SRTP)	4 <sup>20</sup> ,000	4 <sup>20</sup> ,000			
	Sessions/Sec (SPS)	1,000	1,000			
	Packets Per Second (pps)	6,000,000	6,000,000			
Access (subscribers)	256,000	256,000				

Notes: 1) One session per call, including media; G.729, 20 msec media profile  
 2) Virtual SBC performance through vSwitch  
 3) Virtual SBC performance with Passthrough  
 4) SRTP - RTP call model

PRODUCT SPECIFICATIONS																											
Network Interfaces	Signaling and Media: <ul style="list-style-type: none"> <li>• 4 x 1Gb Ethernet (10/100/1000 Base-T or MM fiber each) or 2 Fiber 10Gb</li> <li>• 4+4 x 1 Gb Ethernet (10/100/1000 Base-T or MM fiber each), or 2+2 Fiber 10Gb</li> <li>• Full duplex</li> <li>• Note: 10Gb Ethernet is available for HP DL380 and DL20 platforms.</li> <li>• Management:                             <ul style="list-style-type: none"> <li>• 1+1 Gb Ethernet (10/100/1000 Base-T each) with port redundancy</li> <li>• HA control:                                     <ul style="list-style-type: none"> <li>• 1+1 Gb Ethernet (10/100/1000 Base-T each) with port redundancy</li> </ul> </li> </ul> </li> </ul>																										
Configuration	<ul style="list-style-type: none"> <li>• Integrated web-based management (https)</li> </ul>																										
Management	<ul style="list-style-type: none"> <li>• SNMP traps sent for alarms</li> <li>• Alarms, reports, historical and real-time statistics</li> <li>• Support for Wireshark packet and session tracing</li> <li>• Bulk Provisioning</li> <li>• SOAP/XML</li> </ul>																										
Scalability	<table border="1"> <thead> <tr> <th>Performance Metric</th> <th>Virtual</th> <th>COTS – HP</th> </tr> </thead> <tbody> <tr> <td>VLAN</td> <td>128</td> <td>1,024</td> </tr> <tr> <td>IP addresses (signaling and media)</td> <td>128</td> <td>2,048</td> </tr> <tr> <td>SIP interfaces</td> <td>64</td> <td>500</td> </tr> <tr> <td>Peers</td> <td>512</td> <td>4,000</td> </tr> <tr> <td>Profiles</td> <td>128</td> <td>1,024</td> </tr> <tr> <td>Local DNS Entries</td> <td>1,024</td> <td>65,000</td> </tr> <tr> <td>Policies</td> <td>1,000</td> <td>5,000</td> </tr> </tbody> </table>			Performance Metric	Virtual	COTS – HP	VLAN	128	1,024	IP addresses (signaling and media)	128	2,048	SIP interfaces	64	500	Peers	512	4,000	Profiles	128	1,024	Local DNS Entries	1,024	65,000	Policies	1,000	5,000
Performance Metric	Virtual	COTS – HP																									
VLAN	128	1,024																									
IP addresses (signaling and media)	128	2,048																									
SIP interfaces	64	500																									
Peers	512	4,000																									
Profiles	128	1,024																									
Local DNS Entries	1,024	65,000																									
Policies	1,000	5,000																									

Table 2-1: Product Specifications

COTS Platform: HP DL380 Gen10 (2RU)	
Hardware Redundancy	<ul style="list-style-type: none"> <li>• Hot swappable fans</li> <li>• Hot swappable disks</li> <li>• Hot swappable AC or DC power supplies</li> <li>• Port redundancy</li> </ul>
Physical	

COTS Platform: HP DL380 Gen10 (2RU)	
Dimensions without Bezel (W x D x H)	HP DL380 (2U): 17.54 x 28.75 x 3.44 in. (44.55 x 73.02 x 8.73 cm)
Weight	<ul style="list-style-type: none"> <li>• 25 Kg (27.00 lb.) - includes hard drive, power supply and processor.</li> </ul>

Table 2-2: Hardware Specifications for HP Platform

Specification	Value
Environment	<p><b>Temperature range:</b></p> <ul style="list-style-type: none"> <li>• Operating: 10°C to 35°C (50°F to 95°F)</li> <li>• Non-operating: -30°C to 60°C (-22°F to 140°F)</li> </ul> <p>Relative humidity (non-condensing):</p> <ul style="list-style-type: none"> <li>• Minimum to be the higher (more moisture) of -12°C (10.4°F) dew point or 8% relative humidity.</li> <li>• Maximum to be 24°C (75.2°F) dew point or 90% relative humidity.</li> <li>• Non-operating: 5% to 95% 38.7°C (101.7°F), maximum wet bulb temperature</li> </ul>
Power	<p>Power Supplies: Dual hot swappable AC or DC power supplies Each power supply 800W maximum</p> <p><b>AC Power Option:</b></p> <ul style="list-style-type: none"> <li>• Input Voltage Range (V rms): 100 to 240 VAC</li> <li>• Frequency Range (Nominal) (Hz):50 Hz to 60 Hz</li> <li>• Nominal Input Current (A rms):9.1 A at 100 VAC, 4.4 A at 200VAC, 3.7A at 240 VAC</li> </ul> <p><b>DC Power Option:</b></p> <ul style="list-style-type: none"> <li>• Input Voltage Range (VDC): -40 to -72</li> <li>• Nominal Input Voltage (VDC): -40 VDC, -48 VDC, -72 VDC</li> <li>• Nominal Input Current (A -DC):22.0 at -40 VDC, 18.1 at -48 VDC, 11.9 at -72 VDC</li> </ul>

Table 2-3: Environment and Power Specifications

Virtualized BorderNet SBC: Minimum Hardware Requirements	
Server	<p>Any x86 hardware, compatible with the KVM/VMWare vSphere (ESXi version 6.0 or higher) Hypervisor. Dialogic has tested and qualified the BorderNet SBC on the following servers:</p> <ul style="list-style-type: none"> <li>• Dell PowerEdge R710 and R720 Servers</li> <li>• HP ProLiant BL and ML series servers</li> <li>• HP DL380</li> </ul>

Virtualized BorderNet SBC: Minimum Hardware Requirements	
CPU	<ul style="list-style-type: none"> <li>• 2 x 64-bit CPU or 1 x 64-bit dual core processor (Itanium IA64 processor not supported)</li> <li>• 2.4GHz or faster Intel 64 or AMD 64 processor</li> </ul>
Memory	<ul style="list-style-type: none"> <li>• 8 GB or 2 GB per machine CPU (the larger of these as a minimum)</li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li>• A 2 core machine will have 8 GB (minimum requirement).</li> <li>• A 3 cores machine will have 8 GB RAM.</li> <li>• A 10 cores machine will have minimum of 20 GB RAM.</li> </ul>
Disk Space	80 GB or higher preferred
Network Interfaces	<p>4 x 1GB Ethernet interfaces, including:</p> <ul style="list-style-type: none"> <li>• 2 x 1Gb Ethernet interfaces for signaling / media</li> <li>• 1 x 1Gb Ethernet for high availability</li> <li>• 1 x 1 Gb Ethernet for administration</li> </ul>

Table 2-4: Virtualized BorderNet SBC Minimum Hardware Requirements

## 3. Reference Network Topologies

### 3.1 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 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 the strict transparency requirements of a pure SIP-proxy. Instead, a B2BUA acts similarly to a proxy in some instances and similarly to an end user agent in other instances, depending on the operator's requirements.

The BorderNet SBC supports a configurable range of B2BUA transparency levels, from a strict B2BUA to a fully transparent B2BUA. The BorderNet 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 SBC can be configured to suppress, modify, or insert a wide array of information between the two sides of the call – in order to maintain the strictest privacy while still allowing the widest possible interworking between otherwise incompatible SIP networks.

The BorderNet 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 SBC modifies session descriptions in SIP messages so that media can traverse the network.

The BorderNet SBC B2BUA architecture enables 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
- SRTP and transcoding

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.

### 3.2 Service Provider Access and Interconnect Scenarios

The BorderNet SBC enables Service Providers to peer with other Service Providers while simultaneously delivering hosted class 5-like services including Unified Communications, hosted PBX, hosted contact center or VoIP services (Consumer or Business) to their customers in a number of different ways.

The BorderNet SBC can be deployed within a Service Provider network for different applications such as:

- SIP/SIP-I peering connections between Service Providers



- SIP trunks to an Enterprise edge
- SIP lines to SMB / consumer endpoints
- These are illustrated in Figure 3-1 below.

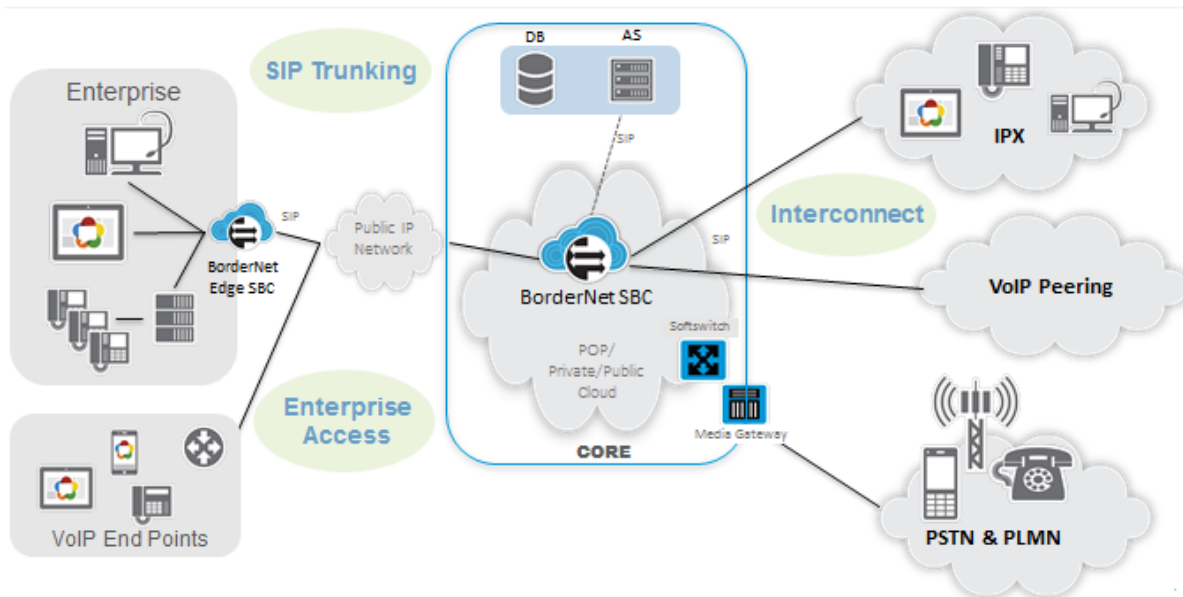


Figure 3-1: Service Provider Access and Interconnect Scenarios (1)

The BorderNet SBC can be deployed by the Service Provider at the Enterprise Edge to terminate SIP trunks and provide remote visibility. A Service Provider may deploy the BorderNet SBC as either a virtualized SBC or on a COTS platform provided by **Dialogic**.

A single BorderNet SBC may be configured for both Access and Interconnect SBC applications simultaneously or for Peering only.

### 3.3 IMS and VoLTE

The BorderNet SBC can be deployed as an advanced SBC in the 3GPP **IP Multimedia Subsystem (IMS)** and the **ETSI/TISPAN** based network architecture.

The BorderNet SBC offers a best-of-breed border element for securing pure play 3GPP IMS and VoLTE-based modern telecom networks.

The BorderNet SBC is a key anchor for seamless delivery of IMS services across IMS, NGN and legacy TDM networks.

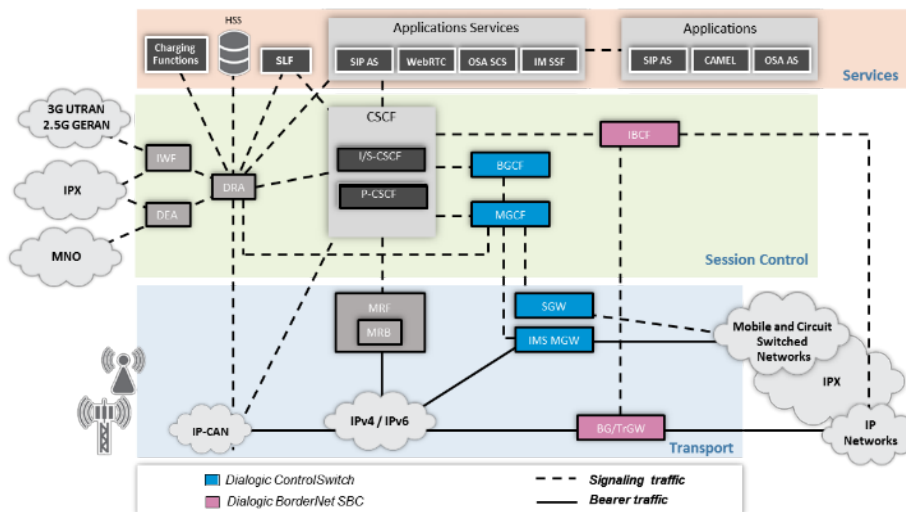


Figure 3-2: Service Provider Access and Interconnect Scenarios (2)

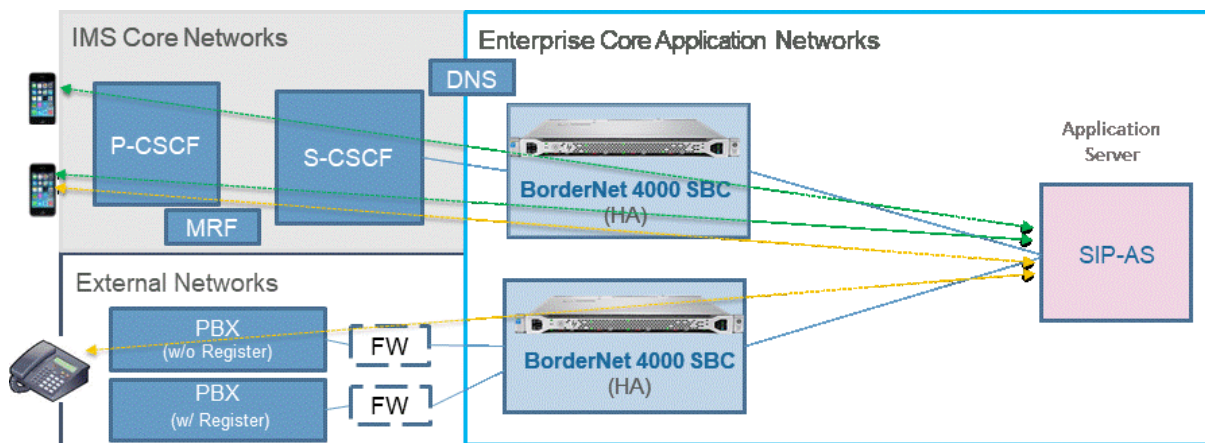


Figure 3-3: Dialogic IMS Support

The BorderNet SBC offers comprehensive border control functionality for IMS access and interconnect deployments. At the IMS interconnect, the BorderNet SBC can be deployed as an I-BCF, IWF or an integrated I-BGF/TrGW. IMS access scenario includes service interworking through the IMS core for services that include SIP trunking and real-time communication (RTC) service delivery to and from mobile user equipment (UE).

The product specifications table (see section 2 of this document) summarizes supported 3GPP network interfaces related to the IMS border functions.

### 3.4 Transcoding

The BorderNet SBC transcoding capability is designed to provide the following implementation options:

- **Software.** The transcoding is provided by software only, using the CPU resources of the BorderNet SBC.



Figure 3-4: Software Transcoding

- **Hardware.** The BorderNet SBC transcoding card provides the transcoding using dedicated DSP resources. Hardware transcoding is activated, if the BorderNet SBC platform (DL20/DL380) populates the transcoding (DSPK-R3e) card/s. When the hardware resources end, then the software resources are used to continue the transcoding operation in the BorderNet SBC. The DL380 platform populates up to four transcoding cards.

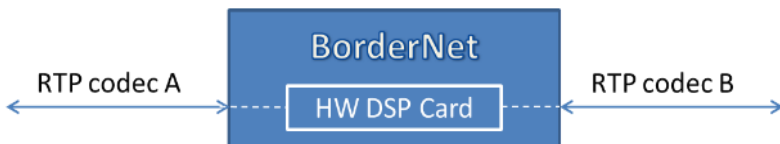


Figure 3-5: Hardware Transcoding

The media information is exchanged between peers and negotiated via the SIP offer-answer model.

**The transcoding service is activated using the management system GUI and can be configured per SIP interface/peer.**

BorderNet SBC software transcoding provides the following media type conversions:

- Codecs:
  - G.711A, G.711UG.711A, G.711U
  - G.722
  - G.723
  - G.726
  - G.729, G.729A, G.729B, G.729AB
  - **GSM-EFR**, GSM-AMR@12.2, GSM-AMR@10.2, GSM-AMR@7.95, GSM-AMR@7.40, GSM-AMR@10.2, GSM-AMR@6.70, GSM-AMR@5.90, GSM-AMR@5.15, GSM-AMR@4.75, GSM-AMR-SID@1.80
  - AMR-WB@6.6, AMR-WB@8.85, AMR-WB@12.65, AMR-WB@14.25, AMR-WB@15.85, AMR-WB@18.25, AMR-WB@19.85, AMR-WB@23.05, AMR-WB@23.85
  - iLBC@13.3 (iLBC30), iLBC@15.2 (iLBC20)
  - OPUS@6, OPUS@8, OPUS@12OPUS@6, OPUS@8, OPUS@12
  - **EVS narrow-band (only for software transcoding)**

---

**Note:**

A session can be transcoded when it is encrypted as SRTP:

- Incoming SRTP sessions are transcoded after decryption.
  - Outgoing SRTP sessions are transcoded before encryption.
- 

- **Packetization:** Transrating between various packetization times is supported.
- **DTMF: The BorderNet SBC transcodes DTMF between:** In Band, RFC2833, and SIP-INFO DTMF transfer methods. The BorderNet is able to transcode only DTMF signals, for sessions using the same Codec but with different DTMF transport mechanism.
- **Fax: The BorderNet SBC transcodes** between Fax Pass-through and T.38 fax relay.

## Fax Transcoding

The BorderNet supports fax transcoding between T.38 fax relay and G711 Fax Pass-through.

Fax transcoding shall be performed only if a transcoding profile is assigned. Fax transcoding with T.38 is supported only with a single image line, using a re-invite to indicate a fax image type.

Multiple m-lines in an offer means multiple (concurrent) media streams are being offered and used. Using multiple 'm' lines with one of them being T.38 will not trigger transcoding.

Using RTP as a transport for fax is not supported (rfc-4612, definition of the audio-RTP type for T.38). Only UDPTL is used for transcoding.

The BorderNet SBC supports High Availability configurations for transcoding sessions.

Fax transcoding is activated by enabling a checkbox by a parameter in the **Transcoding Profile**.

Figure 3-6: Enable Fax Transcoding

For detailed information on the BorderNet SBC Transcoding see the *BorderNet SBC Transcoding User's Guide* document.

## 3.5 Redundancy and High Availability

The BorderNet 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).

In a **High Availability (HA)** configuration, the BorderNet SBC traffic ports are connected to a fully redundant IP network.

The below figures show the interfaces connectivity in 1GB and 10G configurations (found at the rear panel of the platform):

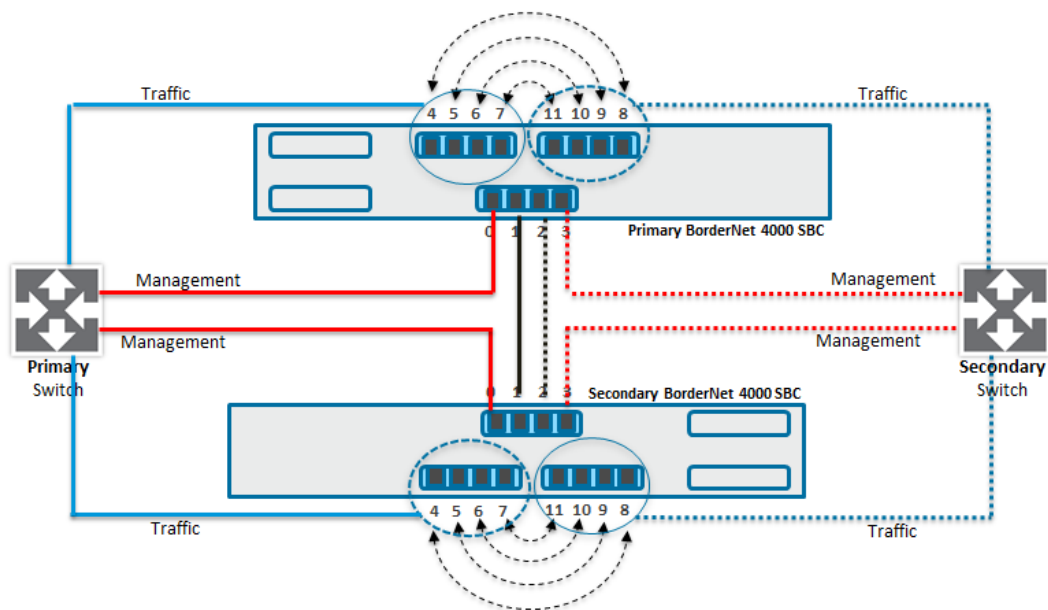


Figure 3-7: High Availability for 1G Interface

The port bondings demonstrated are as follows:

- NIC4 bond with NIC8
- NIC5 bond with NIC9
- NIC6 bond with NIC10
- NIC7 bond with NIC11

Upon the failure of, for example NIC4, NIC8 takes over.

In the example above all the primary NICs (4 to 7), are connected to a primary switch, and all the secondary ones (8 to 11), to a secondary switch.

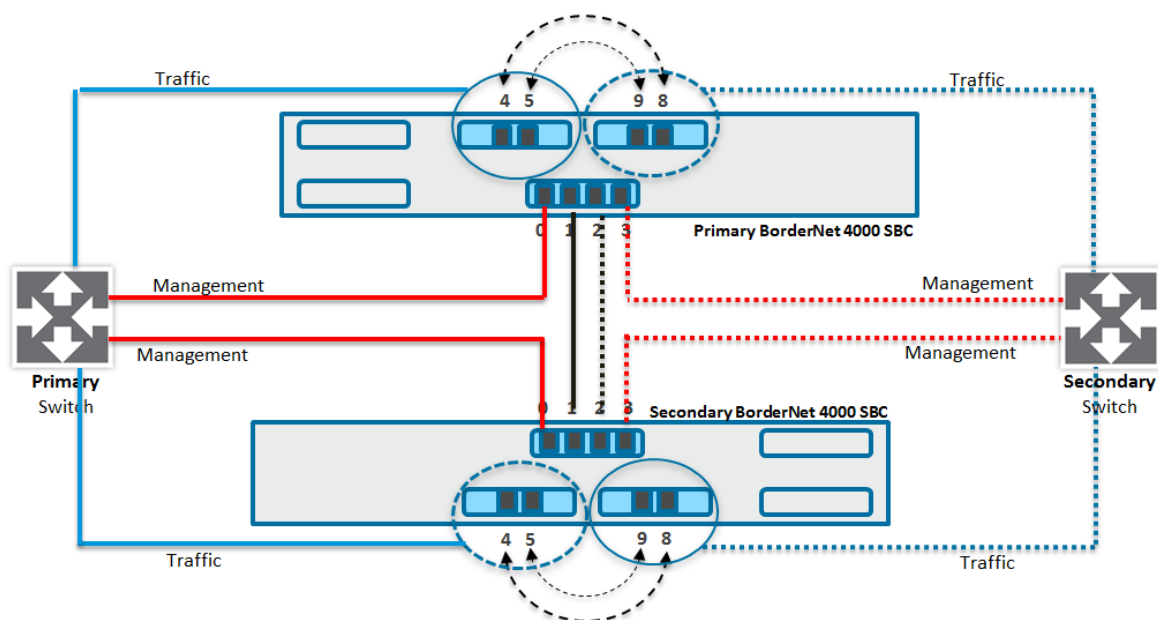


Figure 3-8: High Availability for 10G Interface

The connectivity depicted in the figure above, is found at the rear panel of the platform.

The port bondings demonstrated are as follows:

- NIC4 bond with NIC8
- NIC5 bond with NIC9

Upon the failure of, for example NIC4, NIC8 takes over. In the example above the primary NICs (4 and 5), are connected to a primary switch, and the secondary ones (8 and 9), to a secondary switch.

### 3.5.1 Geo-Redundancy

Geo-Redundancy enables the deployment of the BorderNet SBC in High Availability mode where each platform/instance (primary and secondary) is located on two different networks or sites.



Figure 3-9: BorderNet in Geo-Redundancy Mode

In this deployment mode, each BorderNet SBC has its own set of IP addresses which can be on a totally different network:

- Management IP address: Each platform has its own management IP address as opposed to normal HA deployment mode where the management IP addresses are shared between primary and secondary
- Utility IP address
- HA link IP address
- HA link Gateway IP address (since each platform can be placed on a different network, the BorderNet SBC needs a Gateway IP address to be able to reach its partner platform)
- Traffic IP addresses: Each platform will have its own sets of traffic IP addresses as opposed to normal HA deployment mode where traffic IP addresses are shared between primary and secondary

Geo-Redundancy can be implemented on bare metal deployment, virtualized deployment or cloud deployment.

In the diagram below, in a Geo-Redundancy configuration, during normal operation, traffic runs from Peer A to the active platform/instance and vice-versa. If the active platform/instance fails, the standby platform/instance senses the failure and there is no keep-alive response from the active platform via the HA link. The standby platform declares the mated pair as failed and assumes the active role by sending a re-invite to Peer A, displaying its IP address so that Peer A starts sending traffic to that platform/instance instead.

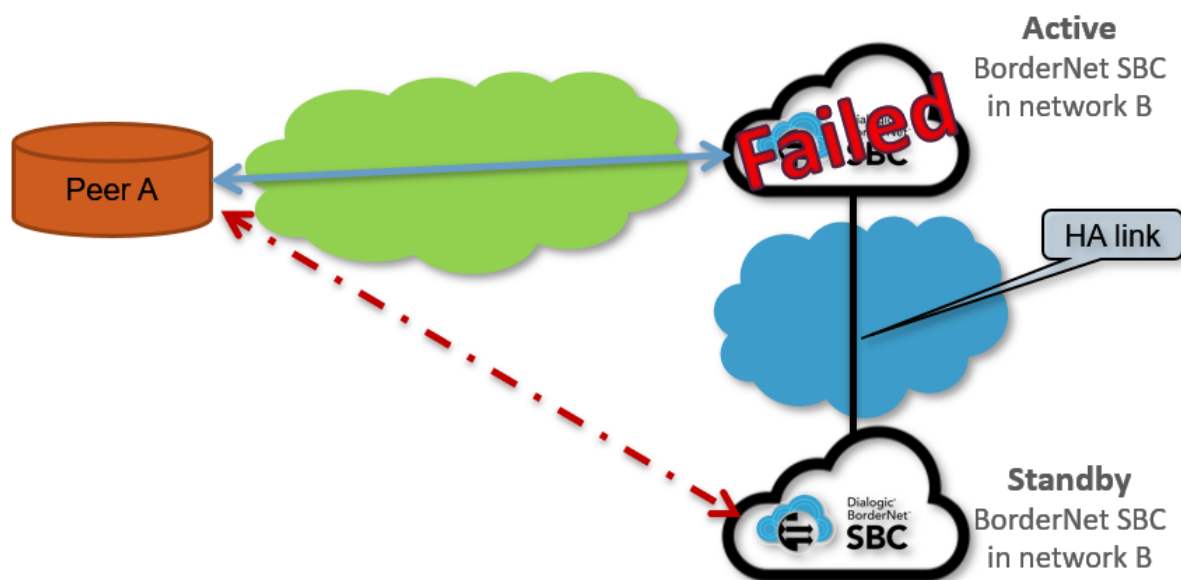


Figure 3-10: Geo-Redundancy Scenario

### 3.5.2 Connectivity

The BorderNet SBC standard configuration provides full redundancy, as follows:

- A set of two copper Ethernet ports provides redundant management links.
- A set of 8 copper or MMF Gigabit ports / 4 fiber 10 Gb ports provide redundant session links for signaling and media traffic.

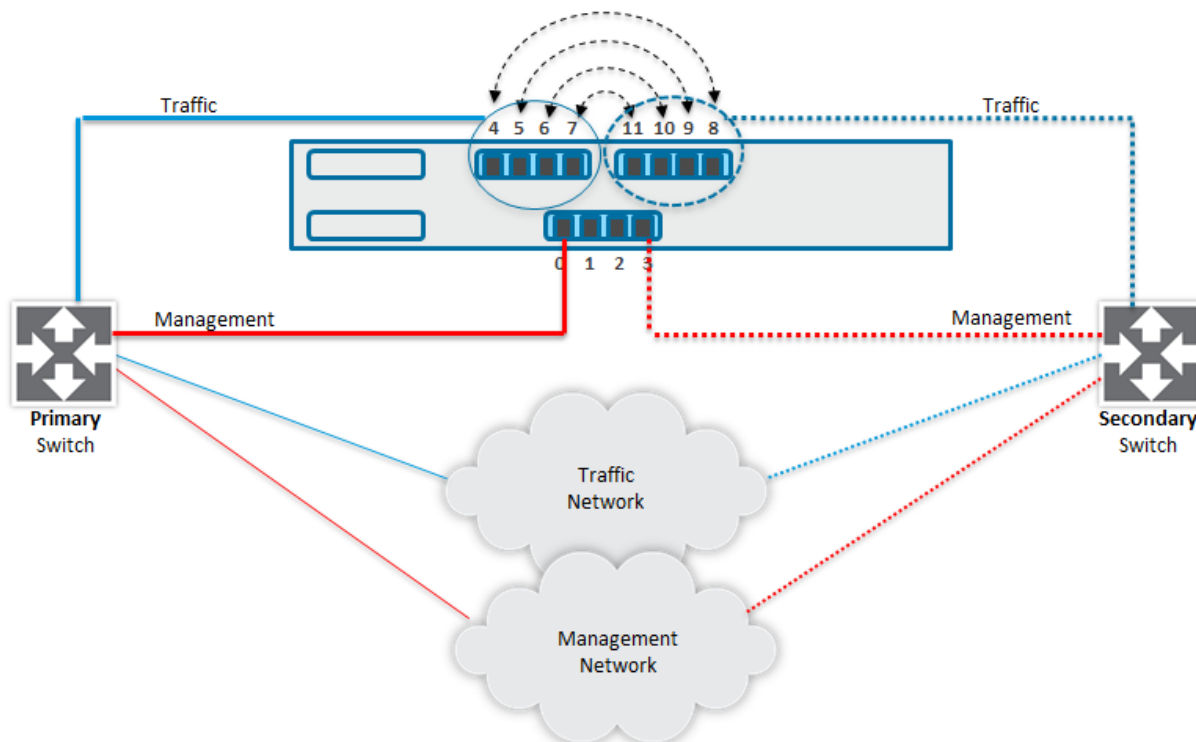


Figure 3-11: Network Connection Redundancy for 1G Interface Configuration

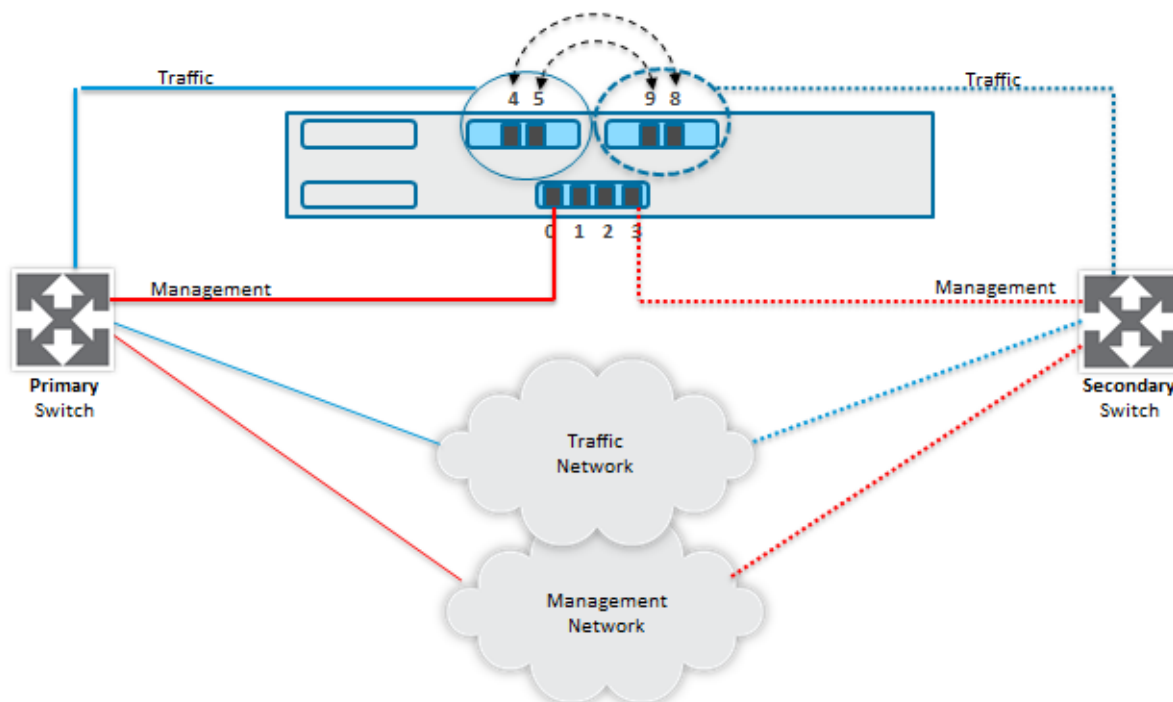


Figure 3-12: Network Connection Redundancy for 10G Interface Configuration

### 3.5.3 Deployment Modes

The BorderNet SBC can be deployed in the following modes:

- **Standalone Mode:** In this mode, one BorderNet SBC is deployed. For the hardware platform configuration, high reliability of the system is achieved in hardware components (fans, disk drives, or power supplies) and network failovers. Software and platform-level redundancy are not available in this mode.
- **High Availability Mode:** Two BorderNet 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.
- **Geo-Redundancy Mode:** There is no restriction with regards to the locations of the BorderNet SBCs. This enables more complex deployments where each BorderNet entity has its own set of IP addresses that can be on a totally different network. Therefore Geo-Redundancy allows each BorderNet SBC on a High Availability deployment to be located in cities or countries thousands of miles apart from each other.

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

The paired BorderNet SBC platforms work in **Active-Standby** mode.

The Active BorderNet SBC handles the media and signaling sessions. The Standby BorderNet 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 SBC is mirrored and kept in sync with the Standby. 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** seamlessly takes over as the **Active** system and continues service to new and established sessions.

The paired links are detailed in the table below.

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 (1GB only)	Eth6	Eth10
Session link pair 4 (1GB only)	Eth7	Eth11

Table 3-1: Primary and Secondary Links

- 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 SBC switches over to the standby platform. The BorderNet SBC is seamlessly available to other nodes on the network with no traffic impact.

## 3.6 802.1Q VLAN (Virtual Local Area Network) Support

On the BorderNet 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 SBC supports the configuration of up to 1024 802.1Q 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 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.

### 3.6.1 Multiple IP Addresses Per VLAN

The BorderNet 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.

---

### 3.6.2 Overlapped IP Address

The BorderNet SBC supports overlapping private networks with a common IP addressing scheme.

These topologies are frequently seen in managed Service Provider networks. Typically, VLAN tagging is used to clearly distinguish between different overlapping networks.

The BorderNet SBC's interface definition and peer binding has been enhanced to include specifying VLAN tag associated with each overlapped network.

The BorderNet SBC uses this unique combination of SIP interfaces, peers and the VLAN tags to route traffic between various overlapping networks.

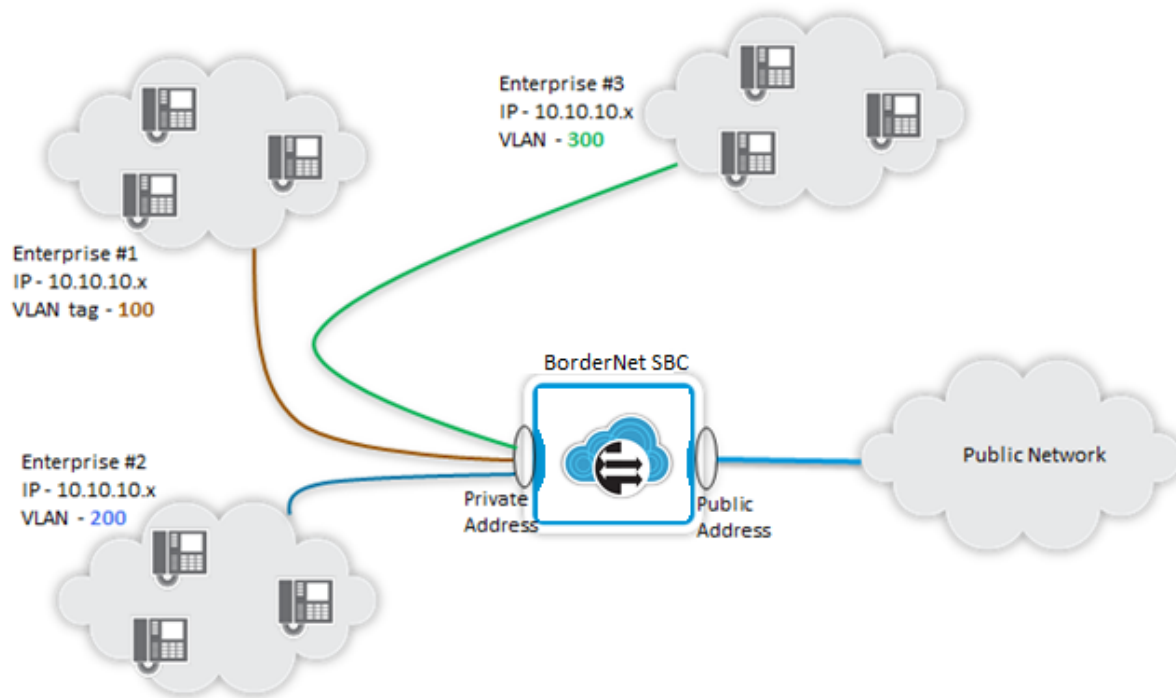


Figure 3-13: Overlapped IP Address

-

## 4. Media Handling

The BorderNet SBC provides media termination and relay to handle RTP traffic from remote entities signaled through SIP/H.323 messages.

The BorderNet SBC 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

### 4.1 Signaling and Media Separation

The BorderNet 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.

### 4.2 Media Latching

The BorderNet 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.

### 4.3 Media Over Multiple Physical Interfaces

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

### 4.4 Media Rate Limiting

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

### 4.5 Topology Hiding for Media

The BorderNet 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 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).

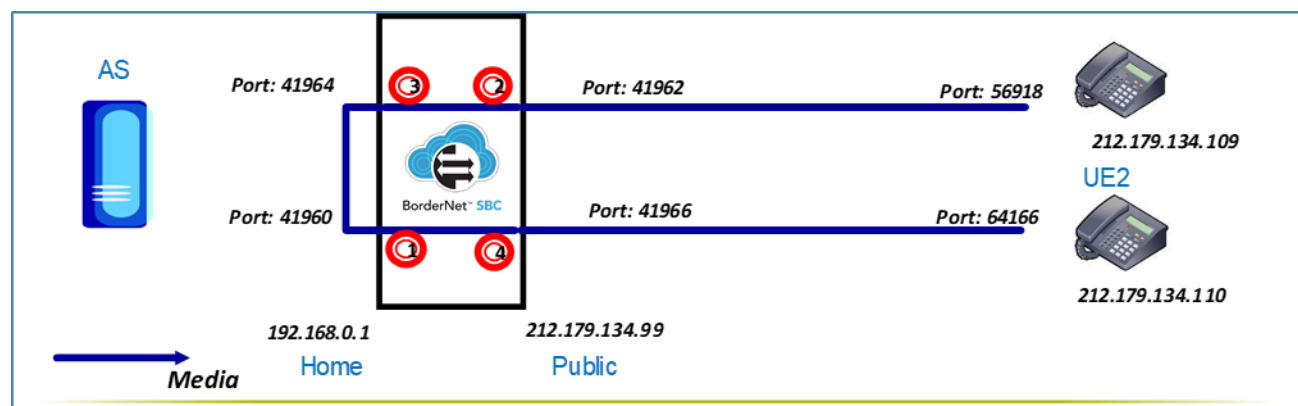


Figure 4-1: Topology Hiding for Media

## 4.6 Policy Based Media Routing

Available policies on the BorderNet SBC can be utilized for control if the media is routed via the BorderNet 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.

## 4.7 WebRTC Support

The main goal of WebRTC is to offer real time communication natively from a web browser. It is a framework that enables peer to peer connections and allows exchange of audio, video and data between connected web browsers.

This framework includes a collection of communications protocols and APIs that enable real-time peer to peer connections within the browser.

Traditionally, these interfaces have been delivered by plugins, which had to be downloaded and installed separately from the browser.

WebRTC introduces the possibility of making those interfaces available in a standardized way within the browser.

WebRTC works only on the Access Public interface type and there is also a WebRTC Gateway between the WebRTC and SIP.

The total WebRTC effort consists of two major parts, each consisting of multiple documents:

- IETF protocol specification - describes the different network protocols to be supported when implementing WebRTC.
- World Wide Web Consortium (W3C) JavaScript API specification - describes a set of APIs, embedded in the client browser, which enable a JavaScript code using it to establish a real time connection between browsers.

WebRTC call setup has been designed to focus on controlling the media plane, leaving signaling plane behavior up to the application as much as possible. The rationale is that different applications may prefer to use different protocols, such as the

existing SIP call signaling protocol, or something custom to the particular application, perhaps for a new use case. In this approach, the key information that needs to be exchanged is the multimedia session description, which specifies the necessary transport and media configuration information necessary to establish the media plane.

The BorderNet's deployment will obviously use SIP as the signaling protocol, sent as SIP over WebSocket.

BorderNet shall support the secured **WebSocket** protocol (**WSS**), for connecting with peers.

The **WSS** is a WebSocket protocol on top of a TLS connection. When selecting WSS from the interface configuration screen, then TLS profile will appear as well.

Protocols implemented for **WebRTC** support include the following:

- WebSocket Secured (WSS)
- ICE-Lite
- STUN connectivity checks
- DTLS-SRTP
- RTCP-Mux
- RTCP-Based Feedback (RTP/AVPF)
  - Audio+Video
  - Transparent transfer of SDP attributes and RTCP packets

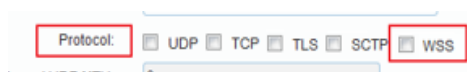


Figure 4-2: Selection of WSS Protocol

## 4.8 Quality of Service (QoS)

The BorderNet 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

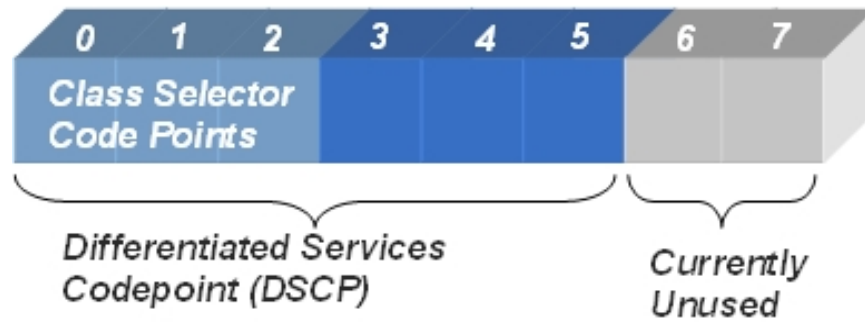


Figure 4-3: Differentiated Services Code Point

The BorderNet 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 SBC.

## 4.9 Media Statistics

The BorderNet SBC collects and reports statistics for media on a system, peer and interface basis, such as:

- Packets received
- Lost packets
- Round trip time
- Jitter
- Dropped packets
- Rate exceeded

The statistics can be displayed as a table or as individual charts, per data.

## 4.10 Supported Codecs and Methods

The BorderNet SBC supports identifying various media types registered with the IANA (**Internet Assigned Numbers Authority**).

The BorderNet SBC has a comprehensive Codec profile scheme and is able to recognize, filter and sort Codecs.

The BorderNet SBC monitors media bandwidth and enforces bandwidth based on the profile settings. It also monitors and restricts the media packet rates accordingly.

The BorderNet SBC is capable of interworking across media subtype notations as well as payload types. Some of the supported Codecs are listed below.

Audio	<ul style="list-style-type: none"> <li>• G.711U, G.711A</li> <li>• G.722, G.722A, G.722B,</li> <li>• G.723</li> <li>• G.726, G.726-16, G.726-24, G.726-32, G.726-40</li> <li>• G.728</li> <li>• G.729, G.729A, G.729B, G.729AB</li> <li>• GSM-HR, GSM-EFR</li> <li>• GSM-AMR@12.2, GSM-AMR@10.2, GSM-AMR@7.95, GSM-AMR@7.40, GSM-AMR@10.2, GSM-AMR@6.70, GSM-AMR@5.90, GSM-AMR@5.15, <a href="#">GSM-AMR@4.75</a>, GSM-AMR-SID@1.80</li> <li>• <a href="#">AMR-WB@6.6</a>, <a href="#">AMR-WB@8.85</a>, <a href="#">AMR-WB@12.65</a>, <a href="#">AMR-WB@14.25</a>, <a href="#">AMR-WB@15.85</a>, <a href="#">AMR-WB@18.25</a>, <a href="#">AMR-WB@19.85</a>, <a href="#">AMR-WB@23.05</a>, <a href="#">AMR-WB@23.85</a></li> <li>• iLBC@13.3 (iLBC30), iLBC@15.2 (iLBC20)</li> <li>• OPUS@6, OPUS@8, OPUS@12</li> <li>• EVS</li> <li>• EVRC</li> </ul>
Video	<ul style="list-style-type: none"> <li>• H.263</li> <li>• H.264</li> <li>• H.261</li> </ul>

Table 4-1: Supported Codecs

## 4.11 DTMF Relay

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

## 4.12 Codec Mapping

The following table provides the BorderNet 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



H.245 Type	SDP Media Type
g726	G726-32
g723	G723
g722	G722
g728	G728
g729wAnnexB	G729
g729	G729 fmp:18 annexb=no
h261VideoCapability	H261
h263VideoCapability	H263

Table 4-2: Codec Mappings

Media entering the BorderNet 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 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.

---

## 5. Security and Service Assurance

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

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

Layer	Security Assurance
6 – 7 Application (SDP)	<ul style="list-style-type: none"> <li>• Allows sessions from configured peers only</li> <li>• Uses dynamic blacklisting of peers for bad behavior</li> <li>• Provides session constraints</li> <li>• Enables selective information hiding, including topology hiding with B2BUA architecture</li> </ul>
5 (SIP/H.323)	<ul style="list-style-type: none"> <li>• Provides syntax and semantic validation of signaling messages</li> <li>• Provides TLS for SIP signaling and management traffic</li> </ul>
3 – 4 (IP/Transport)	<ul style="list-style-type: none"> <li>• Provides a firewall to protect against TCP/IP attacks</li> <li>• Employs rate-limiting to protect against DoS attacks</li> <li>• Enables topology hiding via media termination/relay</li> </ul>

Table 5-1: Security Assurance

### 5.1 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.

#### 5.1.1 Packet Consistency Checks

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

The BorderNet 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

## 5.1.2 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 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

## 5.1.3 Protocol Consistency Checks

IP standards provide protocol guidelines that detect and filter non-conforming or malicious packets.

The BorderNet 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 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)

## 5.1.4 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 SBC creates service-specific ACLs based on other configurations. These service-aware ACLs enable fine-grain control over BorderNet SBC traffic and prevent DoS attacks.

## 5.1.5 Advanced Packet Rate-Limiting

The BorderNet 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 **gray list traffic**.

Traffic from a trusted source uses the white list path. Traffic from an untrusted source initially uses the gray 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 SBC. The gray 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 SBC.

## 5.1.6 Dynamic Packet Rate Adjustment

The packet rate for traffic flows can be controlled by the operator or dynamically adjusted by the BorderNet SBC based on session constraints, configuration and call patterns.

The BorderNet SBC monitors each session and determines the expected packet rate, which is used by the flow classifier to police traffic.

## 5.1.7 Traffic Priority and Overload Protection

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

The BorderNet 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.

## 5.1.8 Media Security

Pinholes ensure media security.

The BorderNet SBC dynamically opens and closes pinholes for RTP traffic based on session signaling. When a pinhole is open, the BorderNet 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.

## 5.2 Application Security

### 5.2.1 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 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 SBC also supports manual keying as well as IKE v1 and IKE v2.

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

### 5.2.2 TLS Support

**Transport Layer Security (TLS)** provides privacy and integrity between two communicating end-points, using digital certificates for authentication, and session key establishment.

The BorderNet SBC TLS encryption supports the following:

- Allows the operator to manage certificates including generation, importing, exporting and viewing the certificate content (using the management system).
- Certificates and private keys are stored in XML records.
- Uses the certificates to establish TLS sessions (using SIP URIs), by sending the certificate to a remote end, validating the remote certificate using the configured trusted certificates and selecting the cipher for the session.

The BorderNet SBC supports x.509 v3 (PKIX profile) public key digital certificates for asymmetric cryptography. Both self-signed and CA certified certificates are supported.

The BorderNet SBC supports certificates encoded in PEM/base64 format.

The BorderNet SBC is capable of generating a **CSR (Certificate Signing Request)** to be sent to a desired CA. Once the certificate is signed by the CA it can be uploaded to the BorderNet SBC.

The following diagram shows a TLS handshake where a remote system (client) originates a TLS connection with the BorderNet SBC (server).

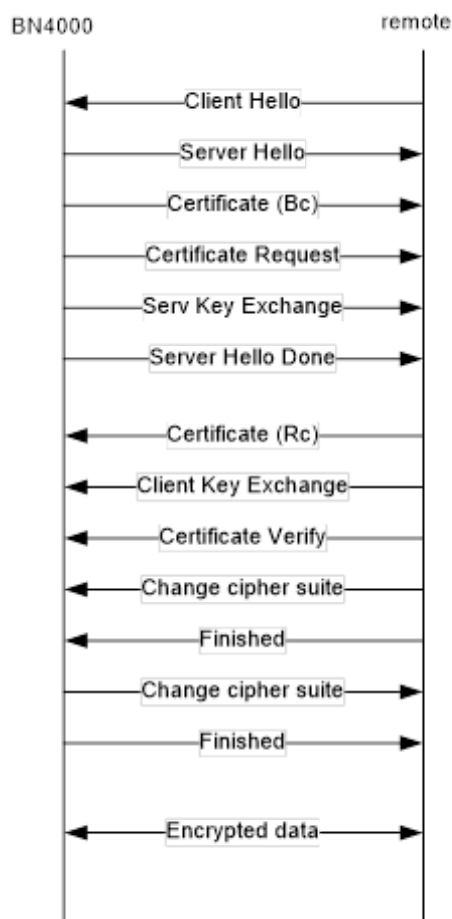


Figure 5-1: TLS Handshake

The process is as follows:

- The “Client” starts the TLS connection by sending *Client Hello*, including protocol version and the supported cipher suites.
- The BorderNet (server) selects the cipher from the client list and sends its “Certificate Bc”.
- If mutual authentication is enabled, it requests the client certificate.
- The “Client” validates the server “Certificate Bc” using its “trust list Rt”. It then sends its own “certificate Rc” and an indication to validate the certificate.
- The “Server” uses its “trust list Bt” to validate the client certificate.
- Other messages are used to establish the session key.
- The selected cipher is used to encrypt the SIP message body and transfer it over a secured transport layer.

## 5.2.3 Malicious Behavior Handling

The BorderNet 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.

## 5.2.4 Call Admission Control (CAC) Session Constraints

**Call Admission Control (CAC)** protects the infrastructure against excessive traffic from remote entities in real time.

The BorderNet 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 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 SBC WebUI.

## 5.2.5 HTTP Security

The BorderNet 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 SBC via HTTP. Unauthorized packets are dropped.

## 5.3 SRTP and SRTCP Media Security

Secure RTP (SRTP) is a protocol used to encrypt RTP media between two entities, enabling media confidentiality and message authentication. This protocol does not provide a key management solution. It relies on various existing mechanisms for secure key exchange.

The SRTP encryption keys and encryption algorithms are signaled in the SDP (via the SIP protocol) exchanged between peers. This information is described in the SDP media level, using the SDP attribute: "a=crypto". The crypto attribute is used to signal and

negotiate cryptographic parameters for media streams in general, and for SRTP in particular, using the offer/answer model.

The crypto keys exchanged in the SDP during the offer/answer process are unidirectional. Each side sends the encryption key used to encrypt its transmitted packets.

The BorderNet SBC negotiates the crypto-attributes in the SDP, in accordance with the SIP Offer/Answer model, supporting the following parameters:

- Tag
- Crypto-suite
- Key-params (key-method=inline)
- Session-params (shall be supported in future releases)
- Cryptographic Transforms. AES\_CM\_128\_HMAC\_SHA1\_80 and AES\_CM\_128\_HMAC\_SHA1\_32 are supported. . AES\_CM\_128\_HMAC\_SHA1\_80 and AES\_CM\_128\_HMAC\_SHA1\_32 are supported.

The BorderNet SBC acts as a B2BUA, so it treats each call leg as a separate SIP and SRTP session, supporting the following scenarios:

- SRTP to RTP sessions
- RTP to SRTP sessions
- SRTP on both incoming and outgoing sessions
- RTP packets exchanged directly between peers without intervention (based on provisioning)

The BorderNet SBC currently supports the same encryption and authentication for SRTP and SRTCP.

The BorderNet SBC (R3.5.0) currently does not support fax security (T.38 is not encrypted, and fax pass-through is treated as a regular call).

The BorderNet SBC supports two 'm' lines in use cases where one stream is audio and the second stream is video. Each 'm' line includes a separate crypto attribute at the media level.

SRTP operation is reflected in the SDR as well as the Statistics Reports.

The BorderNet SBC supports SRTP high availability and all SRTP sessions are maintained upon failover.

SRTP is activated through the BorderNet SBC management system. Once it is enabled the relevant parameters can be configured.

For more details on SRTP functionality and configuration please refer to the *BorderNet SBC SRTP User's Guide* document.



## 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 SBC supports **SIP RFC3261** and **UDP, TCP** and **TLS** transports for SIP.

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

The BorderNet SBC supports up to:

- 500 SIP interfaces
- 1,024 VLANs
- 2,048 IP interfaces
- 4,000 SIP peers

The BorderNet 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.

Session timers can be configured per SIP interface for further control as follows:

Timer	Values
SIP Timer T1	<p>Estimates the round-trip message propagation time, which is used to determine the minimum time before a message should be re-transmitted.</p> <ul style="list-style-type: none"> <li>• Default value: 500 milliseconds</li> <li>• Range: 500 - 4,000 milliseconds</li> <li>• Configured in increments of 100 milliseconds</li> </ul>
SIP Timer T2	<p>Provides the maximum retransmission interval for non-INVITE requests and INVITE responses.</p> <ul style="list-style-type: none"> <li>• Default value: 4,000 milliseconds</li> <li>• Range: 1,000 - 30,000 milliseconds</li> <li>• Configured in increments of 100 milliseconds</li> </ul>
Maximum Number of Retransmissions Parameter	<p>Defines the maximum number of times a SIP message will be retransmitted by the BorderNet SBC.</p> <ul style="list-style-type: none"> <li>• Default value: 4</li> <li>• Range: 1 - 7</li> </ul>

Timer	Values
SIP Proxy Timer C	<p>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.</p> <ul style="list-style-type: none"> <li>• Default value: 240 seconds</li> <li>• Range: 180 – 360 seconds</li> <li>• Configured in increments of 10 seconds</li> </ul>

Table 6-1: SIP Interface Timers

## 6.1 SIP Application Layer Gateway

The BorderNet 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 <b>"rport"</b> parameter in the top-most Via.	Add the <b>"rport"</b> parameter with the value of the source port.
The <b>Max Forward</b> header is missing.	Add the <b>Max Forward</b> header with a value of 70.
The <b>"m"</b> lines contain audio, video or image.	Remove all other <b>"m"</b> lines and associated <b>"a"</b> and <b>"c"</b> lines before propagating the message.

Table 6-2: SIP/SDP Semantic Conditions for ALG Rejection

## 6.2 SIP Profiler

The **SIP Profiler** is a tool that enables operators to manipulate SIP headers.

The BorderNet SBC SIP Profiler can manipulate both incoming and outgoing SIP messages on any configured BorderNet SBC SIP interface.

The BorderNet SBC 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.

For more details on SIP Profiler and its configuration see the *BorderNet SBC SIP Profiler User's Guide* document.

## 6.3 Provisional Response Acknowledgement (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 SBC supports PRACK and asymmetric PRACK to ensure reliable transmission of the provisional response.

## 6.4 Call Routing

The BorderNet 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 require a separate Dialogic partner product for generation of the appropriate routing table.

---

## 6.4.1 Local DNS

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

### 6.4.1.1 Core Network Load Balancing—Incoming Sessions

Load balancing distributes the traffic across multiple remote endpoints.

The BorderNet 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.

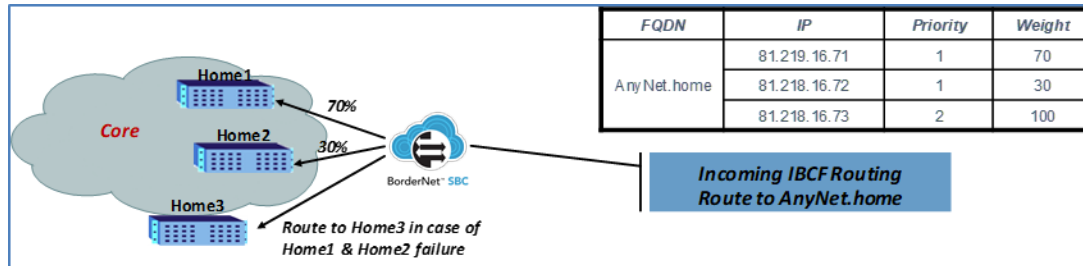


Figure 6-1: Core Network Load Balancing – Incoming Sessions

### 6.4.1.2 Peer Network Load Balancing—Outgoing Sessions

The BorderNet 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.

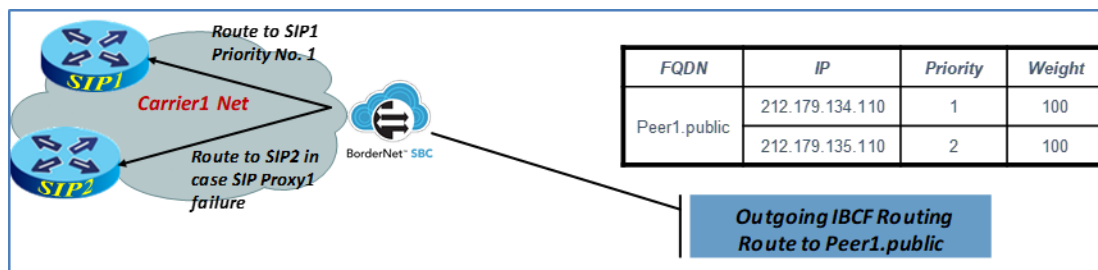


Figure 6-2: Core Network Load Balancing – Outgoing Sessions

## 6.4.2 External DNS Support

In addition to the local DNS capability described above, the BorderNet SBC supports the capability to query external DNS servers for URI resolution.

The supported DNS queries include **DNS SRV**, **DNS NAPTR** and **DNS A** record lookups.

The BorderNet 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.

## 6.5 Rerouting

Rerouting a session means trying a new destination when the session initialization attempt towards an existing server fails. Before v3.8.0, BorderNet retries all existing Egress servers when there is a failure, except for 486. To enable operators to control this behavior and provide alternate actions like REJECT, SKIP\_CARRIER, REDIRECT or CONTINUE, rerouting is used.

The following session rerouting options are available:

Treatment	Functionality
Reject	Rejects the call and stops attempting further routes. An optional cause value can also be set
SKIP Carrier	SKIPs the carrier associated to the current Egress point and jumps to the next
Continue Next Route	Continues to attempt the next route identified earlier
Redirect	Ability to drop existing routes and reanalyze new routes
LNP	Dips to an External server for LNP
External Routes	Dips to an External server specified for routing destinations
Try with Transcoding	Triggers a reattempt to the existing route with transcoding
ENUM Lookup	Dips to an External ENUM Server for TEL>SIP URI translations

### 6.5.1 External Route Server (SIP Redirect Server)

Interconnection to an **External Route Server** is available. With this feature, operators can configure the BorderNet SBC to consult an external routing engine via the SIP INV/3xx method to receive call routing instructions in the form of route lists.

The **ExternalRoutes** treatment provides information about routing the call towards the External Route Server, which itself provides the routes. These External Routing servers are SIP-based and in response to a request on INVITE provide routes in the form of a 302 response.

Additional features available include the following, which are applicable for the entire release and not just for the specific External Route Server:

- Ability to control rerouting based on Cause Codes.
- Ability to lookup into the External Route Server for routes/destinations.
- Ability to identify a group of peers as carriers.
- Ability to skip peers for a given carrier.
- Ability to lookup into the external server for **Local Number Portability (LNP)**.
- Ability to lookup into an in-switch LNP.
- Ability to define routing templates for a large data of rules (**Matrix Feature**).
- Policy control to reattempt a destination with transcoding.
- A fallback mechanism for external route server failures.

To support this feature, the BorderNet SBC WebUI enables the modification of SIP Profiler entries and parameters to provide access and route traffic to the External Route Server.

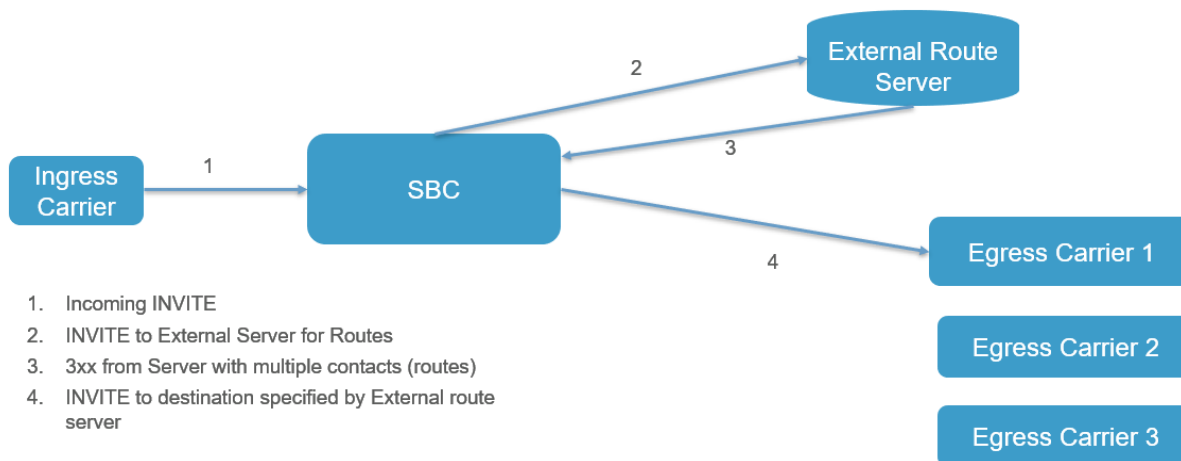
The BorderNet SBC also supports routing using trunk group parameters as part of this feature.

This indicates the action which needs to be taken after an **ExternalRoute** lookup can be configured by the operator based on the **ExternalRouteLookupStatus** field.

The possible values of the **ENUMLookupStatus** are:

- **DipNotDone**
- **Failure**
- **NoRoutes**
- **RoutesAvailable**

The **External Routing** process is illustrated in the following diagram.



## 6.5.2 Local Number Portability (LNP)

**Local Number Portability (LNP)** is a service that allows subscribers to switch local or wireless carriers and still retain the same telephone number.

BorderNet performs external lookups for LNP and one or more peers can be configured as LNP servers. If one server times out then the lookup is referred to another server. When all external servers are exhausted, the system will lookup into the advanced policy with the parameter **LNP lookup failed**.

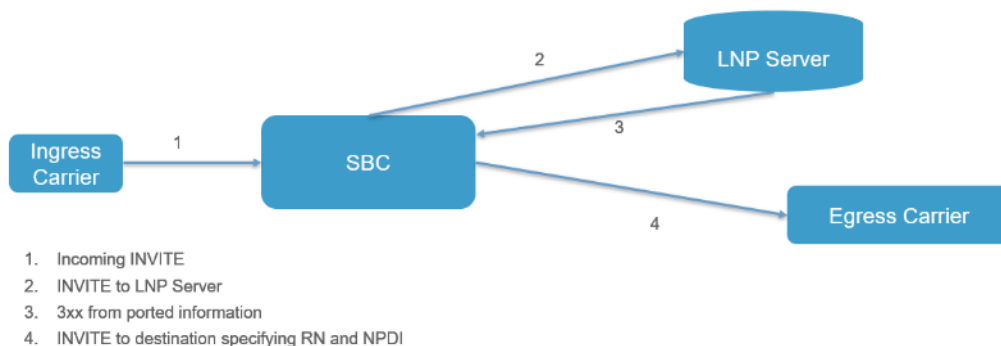
In the case of a 302 response where the LNP Dip is performed and the number is not translated, after a response from the LNP Server (even on timeout), an additional advanced policy is performed. Based on the value of the **LNPLookupStatus** parameter value, the operator can decide on any action.

The possible values of the **LNPLookupStatus** parameter are:

- **Dip Done Not translated**
- **DipNotDone**
- **Failure**
- **DipDoneTranslated**

Where the LNP lookup leads to a new translated number, then an advanced policy lookup is performed to ‘re-analyze’ the new data and any treatment if present, will be discarded.

The **LNP Lookup** process is illustrated in the following diagram.



## 6.5.3 Matrix

All advanced policies define rule parameters and data for making policy decisions. With the introduction of features like **Number Translation**, **Criteria Lookup** and **Directory Lookup**, in BorderNet large data can be bulk-loaded and data kept in isolation to the policy rules, making it quick for access. Criteria Lookup allows rule parameters to have data outside of the policy.

The **Matrix** feature of the Control Switch allows multiple criteria fields defined in the policy to use bulk data configured separately. The Criteria Lookup feature allows the same, but is limited to only one field.

All rule parameters that contain 'Criteria belongs to' and 'Criteria doesn't belong to' actions support the 'Lookup into Matrix' parameter. The Matrix lookup is a Rule type, whose values are in the configured Matrix table. The treatment could be any of the possible values, thereby leaving the Matrix lookup for extracting data, rather than being limited to providing routes. Matrix allows the creation of a template of rules, where the data can be separate from the rules.

## 6.5.4 ENUM

BorderNet supports DNS functionality, and is also able to parse NAPTR and SRV records. This functionality has been enhanced to support **ENUM** routing and ENUM LNP functionality. The user is able to choose by configuration to apply either a SIP LNP or an ENUM LNP. An ENUM server is actually a DNS server, holding NAPTR records with E.164 to URI mappings.

When LNP information is queried from the ENUM LNP server, an optional '**rn**' parameter can be added in order to indicate the desired routing for the ported number.

When sending an ENUM query to a configured ENUM server, BorderNet uses an NAPTR record type as the record requested. When an NAPTR response is received from the ENUM DNS server, BorderNet verifies that it contains the proper service parameters for ENUM, namely either 'E2U+SIP', 'E2U+pstn:tel' or 'E2U+pstn:sip'.

If no service is present in the answer, or the service is different than the above types, BorderNet shall lookup the advanced policy by setting the LNP lookup failed parameter. The action which needs to be taken after an ENUM lookup can be configured by the operator based on the **ENUMLookupStatus** field.

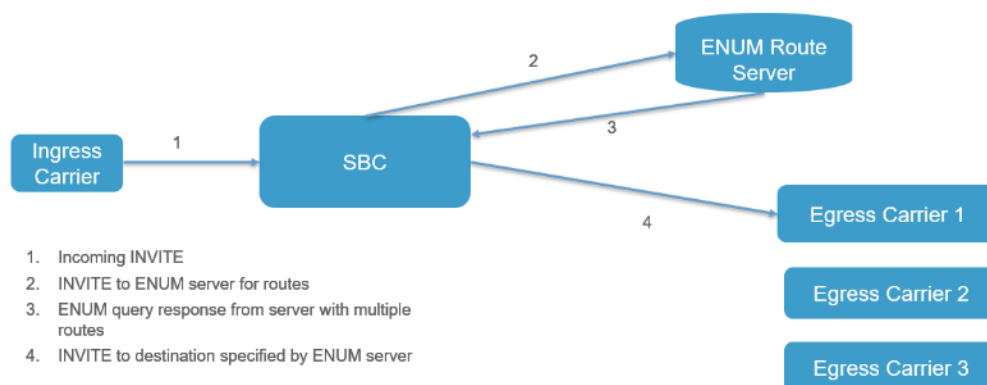
The possible values of the **ENUMLookupStatus** are:

- **DipNotDone**
- **Failure**



- NoRoutes
- RoutesAvailable

The ENUM Lookup process is illustrated in the following diagram.



## 6.6 Access Features

The BorderNet 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

## 6.7 IP PBX Registration Support

The BorderNet 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 IP PBXs.

IP PBX 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 SBC supports bulk registration of extensions from the IP PBXs.

## 6.8 SIP Refer Handling

The BorderNet SBC can be provisioned to support the call transfer capability when receiving a SIP *Refer* message. Upon the termination of the ongoing call, the BorderNet SBC initiates a new call leg between the transferee and the transfer target, completing the call transfer.

The following illustration shows a basic call transfer flow:

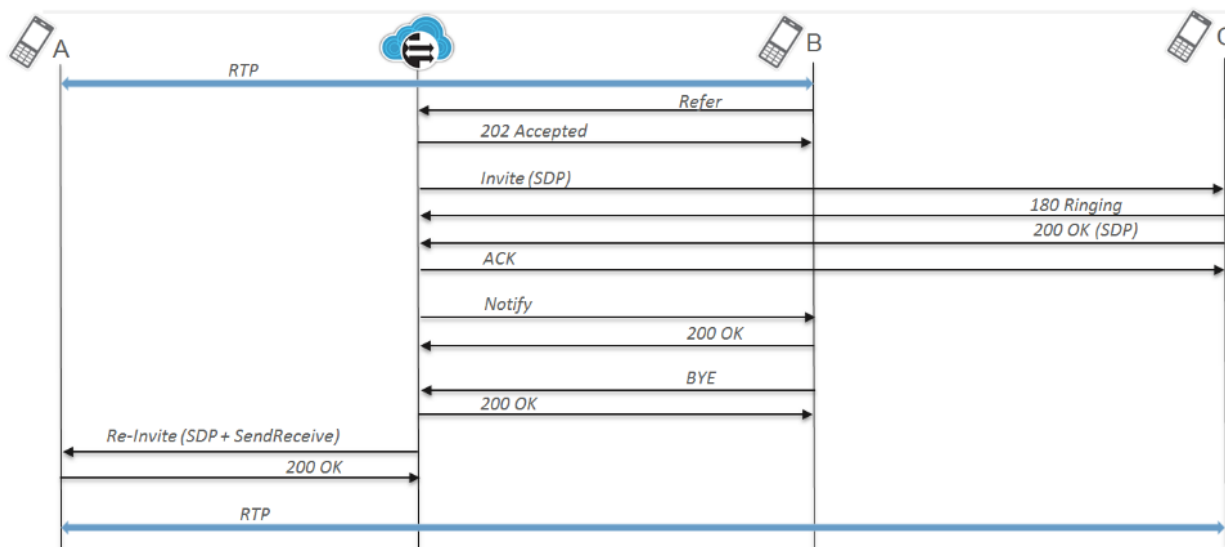


Figure 6-3: Basic Call Transfer Flow

- A call between A and B, has been established.
- B makes a call transfer to C, by putting A on hold, and sending a *Refer* message to the BorderNet SBC.
- The BorderNet SBC replies with a *202 Accepted* message, indicating that it is handling the *Refer* message.
- The BorderNet SBC sends an *Invite* towards C (indicated in the *Refer-To* header), which is constructed as if it was initiated from A (the transferred party). If the *Refer-To* header contains an embedded *Replaces* header, then it is extracted and added as a standalone header in the new *Invite*.
- Every response received from the transfer target (C) is indicated in a *Notify* message and sent to B.
- The session with B is terminated.
- BorderNet SBC sends a *Re-Invite* to A to negotiate the Codecs received from C. It removes A from hold.
- A call is established between A and C.

This capability is often desired in Contact Centers and in hosted IP PBX 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.

## 6.9 Overload Management

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

The BorderNet SBC generates an alarm for each overload level, escalating the alarm as the overload increases. At the same time, the BorderNet 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 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 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 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 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 SBC parses the next header.
- If the message includes a resource-priority header, the response is parsed and handled.

## 6.10 Emergency Call Handling

The BorderNet 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 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.

### 6.10.1 SIP URN Routing for Emergency Services

The BorderNet SBC supports call routing based on service URN concept proposed in the RFC 5031 to handle emergency and other context sensitive scenarios.

Regulatory bodies and leading emergency associations such as **National Emergency Number Association (NENA)** have adopted use of 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 (e.g. 911 in US, 112 in Europe, 100 in India) by utilizing common naming conventions.

## 6.10.2 Border Control Function (BCF)

BorderNet SBC is typically deployed as a **Border Control Function (BCF)** in an **Emergency Service Network (ESINet)**. In this role, BorderNet SBC provides core SBC functions such as security, call routing, call prioritization.

The BorderNet 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. Further, the BorderNet SBC is also capable of modifying **ToS (Type of Service)** byte for emergency calls to ensure expeditious handling of emergency calls by network switching and routing infrastructure.

## 6.11 Local Ring Back Tone

The BorderNet SBC, during the call setup, can be provisioned to play a local Ring Back Tone (RBT), notifying the originator that the terminator's device is ringing.

The BorderNet SBC includes an LRBT sample package (non-licensed). The system operator can replace the sample tones with customized LRBT files. These files must include a default country-specific tone (defLRBT), and additional optional customized tones.

The BorderNet SBC management system provides a tool for ring back tones conversion (to appropriate Codecs and syntax), allows its upload to the system, and configuration.

For detailed provisioning information, see the *BorderNet SBC Provisioning Guide* document.

LRBT Flow is as follows:

- Upon receiving an *Invite*, with SDP from the originating peer, the BorderNet SBC generates *Invite* with SDP towards the destination. The destination responds with 180/183 without SDP.
- The BorderNet SBC checks the originating peer's configuration. If LRBT is disabled for this peer, then the BorderNet SBC proceeds with the call setup, and no LRBT is played.
- Otherwise the BorderNet SBC checks the LRBT folder, searching for the best Codec match with the offered *Invite*'s SDP Codec list. If no match found then the BorderNet SBC proceeds with the call setup, and no LRBT is played. If found then the decision is to play LRBT.

The BorderNet SBC sends a 180/183 (provisioned) with a locally generated SDP: the Codec is derived from the origination peer *Invite*, with send only.

Optionally if PRACK is configured then the BorderNet SBC waits for PRACK from the origination peer. Otherwise, it plays the provisioned RBT file for this peer.

The BorderNet SBC plays the tone in a loop until:

- The terminator sends a new *183* with SDP – the BorderNet SBC stops playing and sends *183* with SDP to the originating peer. The call setup then continues the regular procedure.
  - The BorderNet SBC receives *Cancel* from the originating peer - the BorderNet SBC stops playing the file and sends 200 OK to the originating after the *487* (Request Terminates). Upon approval *ACK* from the originating peer, the BorderNet SBC sends *Cancel* to the terminating peer.
    - Until the expiry of a pre-configured LRBT timeout, the BorderNet stops playing the file and sends *Cancel* to the terminating peer, and *487* to the originating peer.

## 6.12 UDP to TCP Automatic Transition

For large SIP messages (greater than the reported MTU or a default of 1,500 bytes), **RFC-3261** mandates to use a congestion control transport layer such as TCP, to improve the likelihood of the message to pass successfully.

When UDP is used by the BorderNet, and the message to be sent is too large, then a transition to TCP is applied. This means that a new TCP connection is established in order to send the large message. The maximum UDP MTU allowed is user configurable per provisioned peer or SIP interface, until a maximum of 9,000 bytes (which is the maximum allowed MTU for jumbo frames).

## 6.13 Trunk Authentication

SIP trunks create connections between SIP elements residing on different networks, and therefore security mechanisms should be deployed. One important security aspect is authentication, so a SIP trunk provider can make sure the call received on the connected SIP trunk is authorized.

In order to achieve trunk authentication on SIP trunks, the BorderNet utilizes the SIP registration process with its built-in authentication mechanism. Using this method, when the BorderNet connects via a SIP trunk to a SIP trunk provider, it will register and authenticate the trunk before any calls will be allowed to be sent using this trunk.

After an initial authentication with SIP registration, all subsequent calls do not need to authenticate. This means that a per call authentication for each initial *Invite* is not required.

The following figures depicts the trunk authentication scenario, as well as the implementation using the BorderNet.

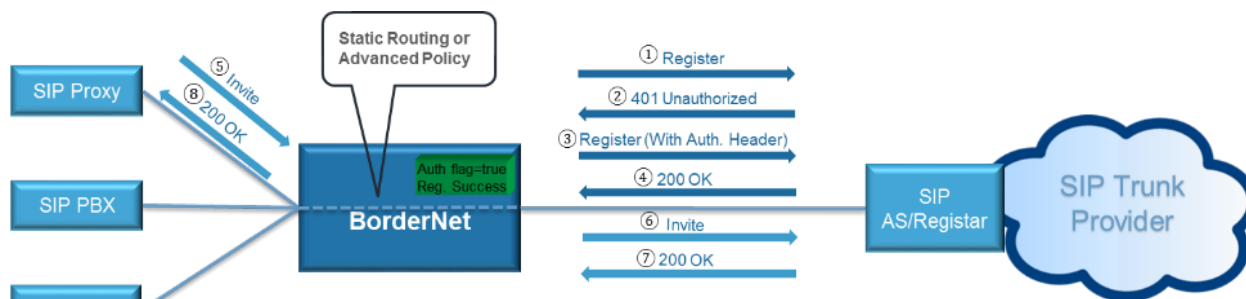


Figure 6-4: Trunk Authentication Scenario

If the authentication process is not successful, then the associated peer shall be marked as blocked for outgoing calls. In this case, no outgoing calls will be routed by the BorderNet to that peer.

Note that trunk authentication affects only outgoing calls via the associated peer, and not incoming calls towards the BorderNet peer. Accordingly, in the event of an unsuccessful authentication, incoming calls will still be allowed.

When the BorderNet constructs the **Authorization** header, it uses the user name and password as provisioned on the SIP peer configuration screen, for the trunk authentication options.

For additional information on trunk authentication configuration, see the *Dialogic® BorderNet™ SBC Configuration and Provisioning Guide*.

## 6.14 Number Translation

Number translation is a service enabling the calling/called party number of the call to be replaced with another number, before the call is sent out to the next hop.

The service is part of the Advanced Policy routing mechanism. It is applied as an action type which is available for either the called or calling number parameters. As a result, it ingrates with the routing decisions based on the original or translated numbers, allowing the number translation mechanism to have more flexibility.

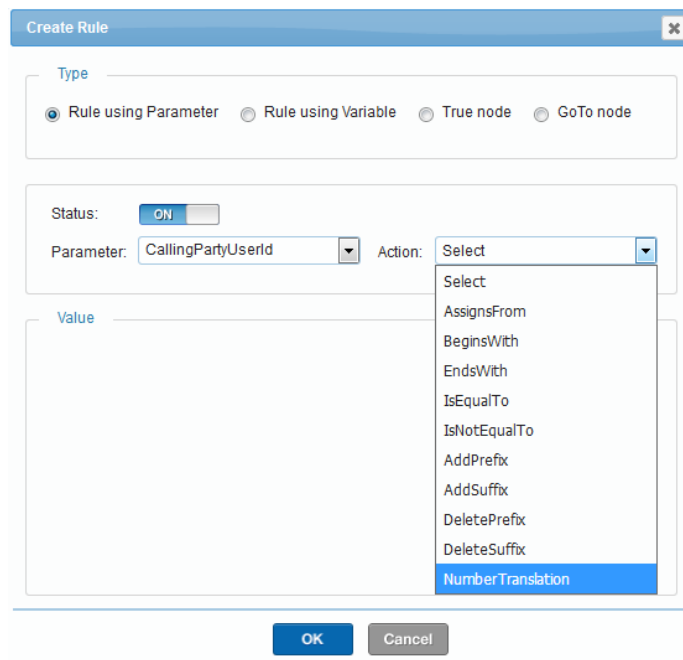


Figure 6-5: GUI Screen for Selecting Number Translation

The number translation action, as configured in the advanced policy, points to a table of numbers to be searched and replaced. Each such table, referenced as a number translation profile, is constructed from two columns – the first column includes the number to be searched (the original number), the second column includes the translated number to be reported back to the advanced policy process.

The following figure is an example of a number translation table.

Back

**Number Translation-To\_Carrier\_A** Add Translation Set

	Number	Translated Number
	<input type="text" value=""/>	<input type="text" value=""/>
	+12127773456	+12127771234
	+44223344550	+33223344550
	+55872456928	872456928
	039701234	9701234
	331029008001	443300537606
	82461085792	71342974692

Page 1 of 1 View 1 - 6 of 6

Figure 6-6: Number Translation GUI Screen

Each table can contain up to 100,000 records, and a maximum of 30 tables can be provisioned to the system.

When number translation is applied, the BorderNet SBC uses the following logic to find and replace the calling/called numbers.

- **CalledPartyUserId**
  - The searched number is extracted from the user part of the **Request-URI** (request-line)
  - The headers to be modified if the number is translated including the **Request-URI** and the **TO** header.
- **CallingPartyUserId**
  - The searched number is extracted from the user part of the **FROM** header.
  - The headers to be modified include only the **FROM** header.

## 6.15 Directory Lookup Service

**Directory Lookup** is a service enabling the parameters of the call to be matched/looked up with data in a directory list to determine if the call parameter belongs to that group. This lookup is performed as part of the policy execution.

This kind of lookup is extremely useful in the implementation of logic for functions such as subscriber checking, screening, whitelist, blacklist etc. that requires lookup of the call parameter in a directory list.

The policy lookup provides tools for the operator to lookup any call parameters into the directory list data, that would enable operators to reject the call, reject calls with announcements/tones, pick alternative routes, or in general for any policy decision.

New routable parameters “**BelongsTo**” and “**DoesNotBelongTo**” added in advanced policy for “**CalledpartyUserId**” and “**CallingpartyUserId**”.

Each table can contain up to 100,000 records, and a maximum of 30 tables can be provisioned to the system.

## 6.16 Criteria Set Service

The advanced policy routing mechanism is enhanced with a new criteria-set, allowing more flexibility and robustness in conditional routing.

Multiple tables containing multiple entries can be imported to the BorderNet criteria-set repository, later to be available as look-up tables for the parameters chosen as routing criteria on the advanced-policy.

When a rule parameter is chosen as a routing criterion, it can now search multiple tables for a match for this parameter.

The actions supported for the tables look-up are “**BeginWith**” and “**Contains**”, introduced as “**CriteriaBeginWith**” and “**CriteriaContains**” on the rule configuration screen of the advanced policy.

Each table can contain up to 100,000 records, and a maximum of 30 tables can be provisioned to the system.

This is an enhancement to the current support, allowing more flexibility and scalability of the routing process. Provisioned values are not required to be configured as single entries. They are easily imported via simple text files.

The criteria-set tables enable reuse of the rule data multiple times within or across multiple plans.



## 6.17 SIP-REC

SIP recording (**SIP-REC**) enables media recording of selected sessions, using a centralized and standardized environment. The IETF SIP-REC framework extends SIP to deliver RTP media and related information to a recording device using SIP, SDP and RTP.

SIPREC identifies two players involved in call recording – the **Session Recording Client (SRC)** and the **Session Recording Server (SRS)**.

The SRC is a SIP UA that acts as the source of the recorded media, and the SRS is a SIP UA that acts as the sink of the recorded media.

The BorderNet SBC acts as a SIP-REC SRC, allowing for the sessions traversing it to be sent to an external SRS for recording of the sessions and associated data.

An SRS is provisioned using a service profile. It is associated to a peer as a special peer type. It allows for multiple SRS servers to be configured and used for session recording, as well as for a single specific call to be sent for recording towards two different SRS elements. The first SRS is as provisioned for the ingress peer and the second SRS is as provisioned for the egress peer.

For additional information on SIP-REC configuration, see the *Dialogic® BorderNet™ SBC Configuration and Provisioning Guide*.

### 6.17.1 SIPREC extensions to SIP and SDP

As part of the SIP-REC framework support, the BorderNet SBC supports the following protocol extensions:

- ‘**siprec**’ option tag in the **Require** header field is used for requests to the SRS.
- ‘**+sip.src**’ feature tag added to the **Contact** header field in requests sent to the SRS. This indication signals that the BorderNet SBC is a SIP-Rec SRC and identifies a SIP dialog as a recording session. The Session Recording Server can tell it is talking to an SRC using this feature tag.
- ‘**a=record**’ SDP attribute as an indication if recording is **On**, **Off** or **Paused**. It is used by the BorderNet SBC for recording indication to the recording-aware UA (the actual record attribute is sent in a *re-Invite* or an *Update* message issued for the record indication to be sent).
- ‘**a=recordpref**’ SDP attribute, allowing a recording aware UA to inform the BorderNet SBC on its recording preference (**On**, **Off** or no preference).

### 6.17.2 Metadata

Metadata is used in SIP-REC to convey information about the session being recorded. It usually includes information such as the identity of the parties involved, label correlation and any other information required.

The metadata is formatted as an XML and is attached to the SIP requests as an XML attachment.

The BorderNet SBC uses the extended content-type and content-disposition defined for SIP-REC, namely ‘**Content-Type: application/rs-metadata**’ and ‘**Content-Disposition: recording-session**’

The BorderNet SBC generates a full metadata snapshot on session establishment, as well as partial metadata updates during the lifetime of the session.



## 7. IMS, VoLTE and IPX Support

### 7.1 IMS and VoLTE

The BorderNet SBC is suitable for deployment as an advanced SBC in the 3GPP IP Multimedia Subsystem (IMS) and the ETSI/TISPAN based network architecture.

The BorderNet SBC offers a best-of-breed border element for securing pure play 3GPP IMS and VoLTE-based modern telecom networks.

The BorderNet SBC is a key anchor for seamless delivery of IMS services across IMS, NGN and legacy TDM networks.

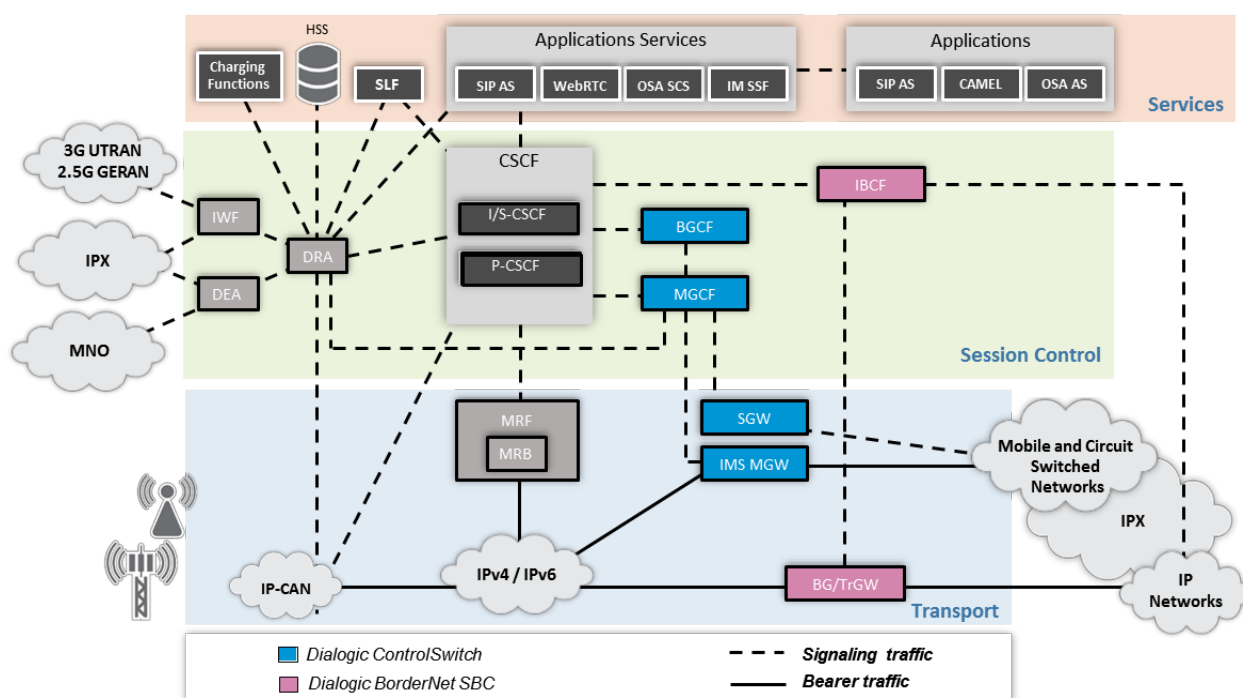


Figure 7-1: Dialogic IMS Elements

The BorderNet SBC offers comprehensive border control functionality for IMS access and interconnect deployments.

At the IMS interconnect, the BorderNet SBC can be deployed as an I-BCF, IWF or an integrated I-BGF/TrGW. IMS access scenario includes service interworking through the IMS core for services that include SIP trunking and real-time communication (RTC) service delivery to and from mobile user equipment (UE).

The Product Specifications table (see section 2 of this document) summarizes supported 3GPP network interfaces related to the IMS border functions.

### 7.2 Interworking Capabilities (I-BCF/TrGW)

The core I-BCF/TrGW border functions supported by the BorderNet SBC includes:

- Signaling
  - 3GPP SIP Call Handling
  - Authentication
  - Port Mapping
- Security and Encryption
  - Encryption (TLS, IPsec)
  - 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
  - Software Transcoding

## 7.3 Mobile Interconnect and IPX Support

The BorderNet SBC supports both 2G/3G Mobile interconnect and IPX market segments.

Example deployment configurations include:

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

- In particular, interworking between SIP-I and SIP has become a serious issue for mobile carriers as they connect their subscriber base to **Over the Top (OTT)** and IMS based network partners.
- Mobile carriers are relying more and more on border elements such as the BorderNet SBC to bridge the traditional MSC/MGW mobile cores with a variety of SIP based partner services.
- **SIP and SIP-I/SIP-T interworking** - The BorderNet SBC supports 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 **Session Detail Records (SDR)** for billing and analysis.

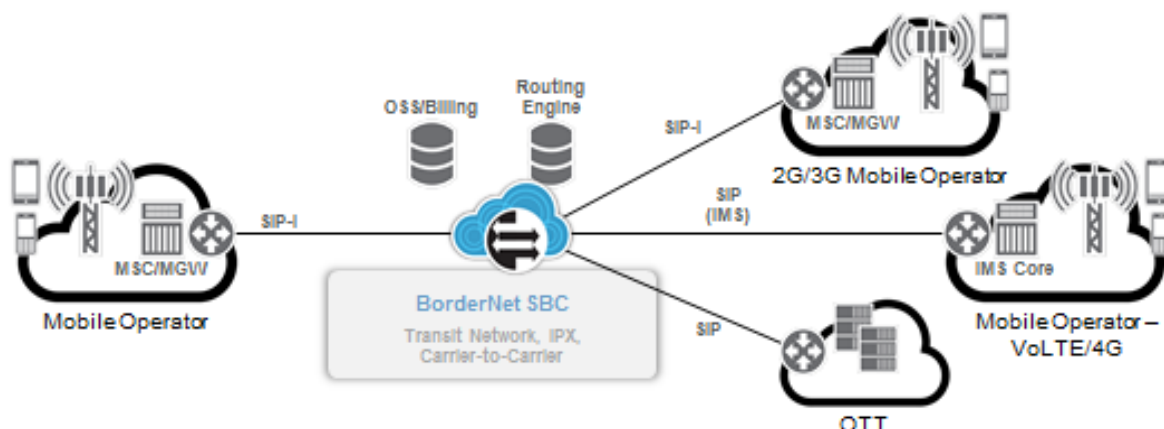


Figure 7-2: Mobile Interconnect and IPX Support

- **IPX Networks** – GSMA IPX networks are essentially like a clearing house for mobile operators. IPX operators typically have few additional requirements above and beyond the mobile interconnect deployments.
- Call routing and accounting are two essential pieces for any IPX services. The BorderNet SBC provides comprehensive on-board and external routing integration. Please see chapter 6 above (SIP Services) for a complete list of available routing and accounting capabilities.

## 7.4 Optimal Media Routing and Local Break Out

**Optimal Media Routing (OMR)** and **Local Break Out (LBO)** capabilities introduce mechanisms for providing an optimal media path between roaming users in IMS networks (based on 3GPP TS 29.079 specifications).

In case of the LBO, the signaling is sent to the home network for session control, and the media is handled locally by the visited network. For the LBO implementation, the **Transit & Routing Function (TRF)** entity is used. TRF is located in the visited network and performs the LBO. It is indicated in the *Invite* (sent from the visited to host network, and its confirmation is sent from the host to the visited network), using the following indicators of the **Feature-Capability** header.

- "TRF - Indicates that the visited network supports LBO and provides the TRF address.
- Example: Feature-Caps:\*;+g.3gpp.trf="< sip:trf-vA1.visited-A.net;lr>"
- "Loopback - Indicates that the home network supports LBO.
- Example: Feature-Caps:\*;+g.3gpp.loopback=<"homenetwork\_A">

The OMR mechanism uses the following OMR SDP attributes to detect the optimal path for the media, by bypassing relevant media functions and manipulating the SDP attributes:

Attribute	Syntax	Description
visited-realm	a=visited-realm: <instance> <realm> <addrtype> <addr> <port>	Used to bypass the allocated media functions. <ul style="list-style-type: none"> <li><i>Instance</i> is the sequence in which the visited-realm is added during the SDP offer forwarding.</li> <li><i>Realm</i> is the mutually connected networks identification, communicating this SDP attributes.</li> </ul>
secondary-realm	a=secondary-realm: <instance> <realm> <addrtype> <addr> <port>	The BorderNet SBC does not generate a secondary-realm attribute, but it validates and forwards it.
omr-Codecs	a=omr-Codecs: <instance>:<proto> 1*<Codec>	Captures 'm' line Codec information
omr-m-att	a=omr-m-att: <instance>:1* <attribute>	Captures media level attributes (is present after the 'm' line).
omr-s-att	a=omr-s-att: <instance>:1* <attribute>	Captures session level attributes (present before the 'm' lines).
omr-m-bw	a=omr-m-bw:<instance>: <bandwidth>	Captures media-level SDP bandwidth
omr-s-bw	a=omr-s-bw:<instance>: <bandwidth>	Captures session-level SDP bandwidth. <ul style="list-style-type: none"> <li>The "b=" bandwidth attribute can be present in both the session or media part.</li> <li>The OMR attributes distinguish between them and assign a different OMR attribute per level.</li> </ul>
omr-m-cksum	a=omr-m-cksum: <hexNumber>	Captures the <b>check-sum</b> calculated on all media level attributes, associated with a specified 'm' line.
omr-s-cksum	a=omr-s-cksum: <hexNumber>	Captures the <b>check-sum</b> calculated on all session level attributes, if exists. Both <b>omr-s-cksum</b> and <b>omr-m-cksum</b> are calculated after the modifications of the attributes by the BorderNet SBC.

Table 7-1: OMR SDP Attributes

The BorderNet SBC provides the role of the IBCF (IMS-ALG and TrGW), not using H.248 (as a result, it does not control different trunking gateways or secondary MRs).

If **Lawful Interception (LI)/SIP-REC/Local Ring-Back Tone (LRBT)/Transcoding** is activated for a call, then the intercept mode is used and OMR is not applied.

For details on provisioning, see the *BorderNet SBC Provisioning Guide* document.

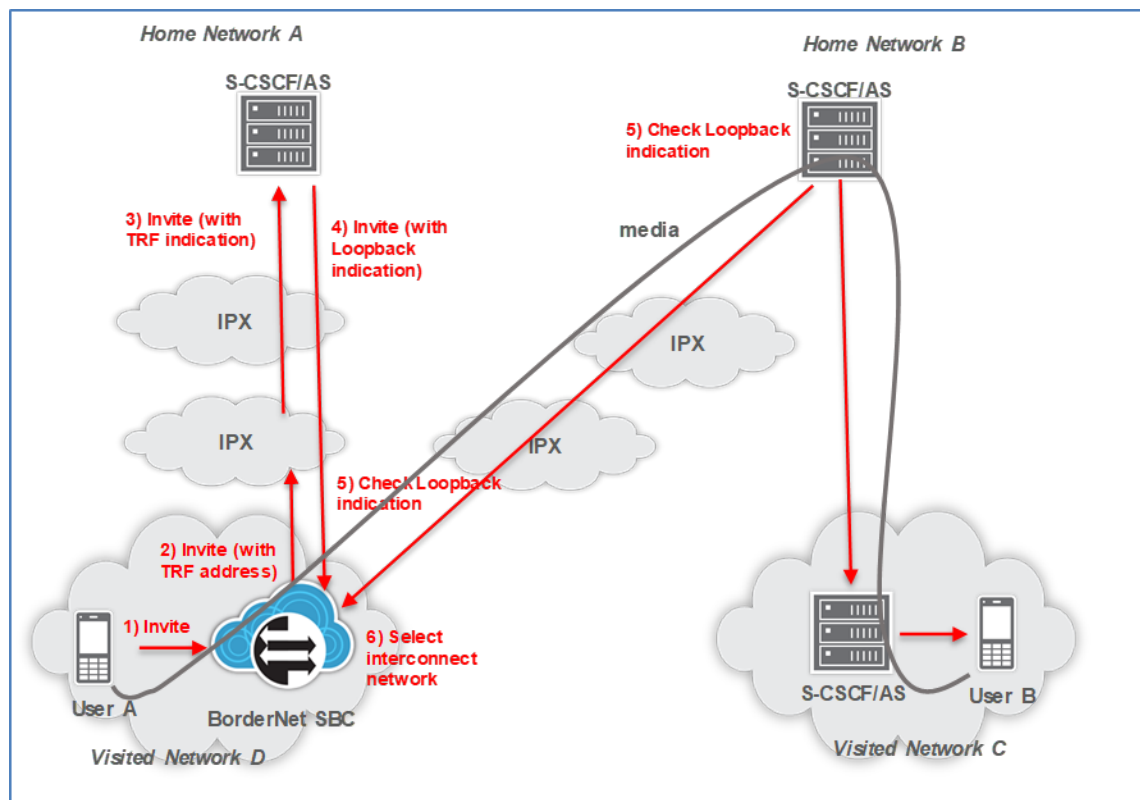


Figure 7-3: LBO and OMR flow

## 7.5 TRF - Transit & Routing Function

When Local Breakout with **VPMN Routed** calls is used, the BorderNet can act as the **TRF** for the call.

The TRF is located in the visited network and is used to receive the signaling from the home network, and then routes the call (signaling and voice) via the local network resources (via the visited network).

When the visited P-CSCF (or other entity in the visited network) decides to use a TRF, it adds the TRF indicator to the **Feature-Capability** header and assigns the TRF address/URI as the TRF indicator value.

Once the TRF indicator is received in the home network, and the home network confirms to use loopback routing, then the TRF address is copied from the **Feature-Capability** header and added as a Route header to the TRF. It also removes the TRF indicator and replaces it with a loopback indicator, to signal it approves and supports the loopback routing/Local Breakout.

When the BorderNet receives a SIP message with a single Route header having its own address (as extracted from the TRF indicator and added as a Route by the home network), and a feature-capability header having the loopback indicator, then it knows this message is destined to its own TRF functionality, hence it applies TRF handling.

---

### Note

The BorderNet SBC will invoke TRF handling only for Route headers containing the IP address of its SIP interface. Route headers with a **Domain/FQDN** will not trigger TRF handling.

---

When TRF functionality is invoked then the **IOTL** and **P-Charging-Vector** are manipulated, based on the TRF procedure as specified in 3GPP TS 24.229 section I.4.2.



## 8. Interworking Function (IWF)

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

BorderNet SBC B2BUA architecture supports the following IWF capabilities:

- **IPv4-IPv6 IWF/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.
- **RTP-SRTP:** BorderNet SBC provides SRTP to RTP, and SRTP to SRTP conversions, based on provisioning and a SIP offer-answer negotiation model.
- **Transcoding.** BorderNet SBC provides transcoding between different Codecs, packetization, DTMF transfer modes, and between T.38 and fax pass-through.

### 8.1 IPv4-IPv6 Interworking Function

The BorderNet SBC delivers enhanced connectivity through **IPv4-IPv6** interworking.

The BorderNet 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. Refer to Dialogic Technical Support for licensing information.

---

### 8.2 SIP, SIP-I, SIP-T Interworking

The BorderNet SBC supports 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 SBC includes a built-in ISUP stack which is capable of decoding ISUP content embedded in the SIP messages to extract various ISUP parameters.

The BorderNet SBC's SIP to ISUP interworking follows the recommendations defined in ITU-T's Q.1912.5 specification.

The BorderNet SBC's interworking is comprehensive by support for both SIP to SIP-I/SIP-T conversion as well as SIP-I/SIP-T to SIP conversion.

## 8.3 H.323-to-SIP Interworking Function

The BorderNet SBC supports an H.323 interworking gateway functionality by providing originating and terminating call services using the H.323 protocol with a remote gateway. H.323 calls are interworked to and from SIP calls.

The BorderNet SBC H.323-IWF can act as a direct gateway or a gatekeeper-managed gateway in an H.323 peering network.

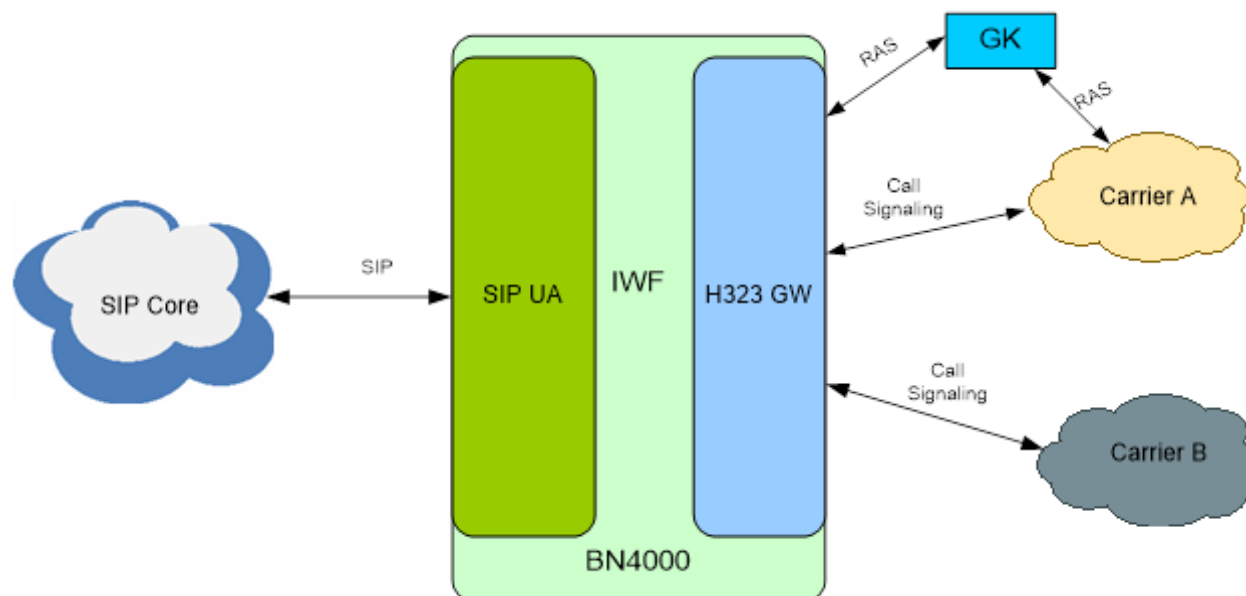


Figure 8-1: H.323 to SIP Interworking Function

The BorderNet SBC 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.

## 8.3.1 IWF Call Flow Support

The BorderNet SBC supports the following call flows:

Call Flow/Type	Description
SIP upstream, H.323 fast-start downstream	The offer received on the SIP <i>INVITE</i> is supported.
SIP upstream, H.323 slow-start downstream	After the offer is received on the SIP <i>INVITE</i> , the BorderNet SBC attempts an H.323 fast-start downstream. If the downstream endpoint does not support a fast-start, the SBC switches to a slow-start procedure.
SIP upstream, H.323 downstream (fast-start or slow-start)	No offer is received on the SIP <i>INVITE</i> .
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 but the H.323 fast-start response cannot. In this case, the BorderNet 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.711 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- <i>INVITE</i> 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 <b>UserInputIndication</b> .
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.

Table 8-1: Call Flow Support

## 8.3.2 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 SBC. A progress indicator with a value of 1 or 8 indicates that the H.323 endpoint will send early media.

The BorderNet 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 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 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 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**.

### 8.3.3 Response Code Mapping

The BorderNet 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.

### 8.3.4 Calling Line Identification

The BorderNet SBC supports mapping between H.323 message presentation indicators and **SIP Privacy** and **P-Asserted-Id** headers. **CLIP/CLIR** features are supported through this functionality.

## 8.4 Diameter Ro and Rf Interfaces

Diameter creates a framework for **Authentication, Authorization and Accounting (AAA)** transport. It details a base protocol that defines the minimum mandatory set of AAA operations, which can then be enriched with additional capabilities by using specific Diameter applications. These capabilities can be developed by extending existing applications or by creating new ones.

A **Diameter** message consists of a fixed-length header followed by a variable number of AVPs. The amount and type of AVPs attached to each message (**Request/Answer**) is dependent on the command associated with the message.

Diameter is a peer-to-peer protocol that uses a request-answer transaction format, in which any node can initiate a request.

Every request sent from a Diameter client must be replied with a Diameter answer from the server side.

- A Diameter client is a device at the edge of the network that performs access control and generates Diameter messages to request AAA services for the user.
- A Diameter server is a Diameter node that handles AAA requests from clients and also supports server initiated requests.

The **Rf** interface refers to situations of **Offline Charging** (see note below) and the **Ro** interface refers to situations of **Online Charging**.

---

**NOTES:**

**Offline Charging (Rf)** is a process where charging information for network resource usage is collected concurrently with that resource usage. The charging information is used to construct CDR files, which are then transferred to the network operator's billing domain (BD) for the purpose of subscriber billing and/or inter-operator accounting.

---

In the case of **Offline Charging (Rf)**, the DCS will be able to connect to more than a single peer, allowing it to overcome failures on its connected peers. In case of a detected failure in the primary peer, the DCS will send the messages to the secondary peer IP address.

In the case of **Online Charging (Ro)**, since this is used for real-time applications, the behavior of a possible fail detection and failover mechanism should be defined separately. A failover of an ongoing real-time session to a secondary server must incorporate a complex updating solution between the primary and secondary servers.

## 8.5 Diameter Rx Interface

The **Diameter Rx** reference point is used for policy control of sessions on the **IP Connectivity Access Network (IP-CAN)** and is operated between the **P-CSCF (Proxy-Call Session Control Function)** and the **PCRF (Policy and Charging Rule Function)**. The **PCRF** provides network control regarding service data flow detection, gating (blocking or allowing packets), QoS control and flow-based charging towards the **PCEF (Policy and Charging Enforcement Function)**.

When the **Policy and Charging Control (PCC)** is used in the network the **P-CSCF** sends information obtained from SIP/SDP session setup signaling to the **PCRF** via the **Rx reference point**.

This information enables the **PCRF** to form authorized IP QoS data (e.g. maximum bandwidth and QoS class) and charging rules that will be delivered to the access gateway via the **Gx reference point**.

The **P-CSCF** is tasked to send policy information to the **PCRF** about every SIP message that includes an SDP payload. This ensures that the **PCRF** passes the proper information to perform policy and charging control for all possible IMS session setup scenarios.

Similarly, the **PCRF** utilizes the **Rx reference point** to send notifications of bearer events to the **P-CSCF**. For passing the information, the **P-CSCF** and **PCRF** use a **Diameter protocol** as defined in **3GPP TS 29.214**.

The **Diameter Rx** interface therefore relies mainly on the following standards:

- **IETF rfc6733** - Diameter Base Protocol
- **IETF rfc7155** - Diameter Network Access Server Application
- **3GPP 29.214** - Policy and Charging Control over Rx reference point

The **Diameter Rx** properties use the existing Diameter profile configuration screen, which is available for **Rf & Ro**. An **Rx** interface activation checkbox is available in the SIP interface configuration screen.

The Rx uses message types as defined in **RFC6733 Diameter Base Protocol**, with the addition of the **AAR (Authentication Authorization Request)** message type defined in **RFC7155 Diameter NASREQ**.

The license for **Diameter Rx** is per Diameter feature. The entire feature is either enabled or disabled regardless of the number of concurrent sessions using it.

---

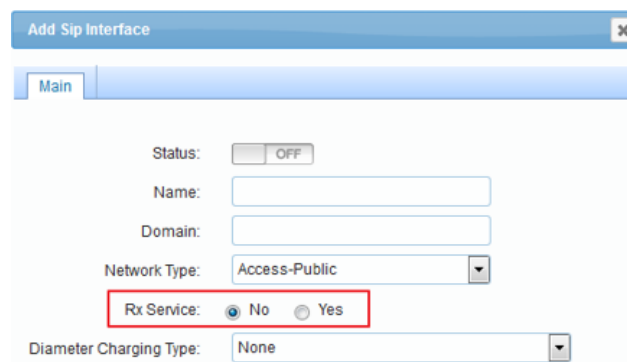
**NOTES:**

- **Rx** Diameter connections to the **PCRF** shall be independent of the **Ro** and **Rf** Diameter connections used for the **OCS/OCF** and the **CDF** accordingly.
- **Rx** user validation shall be enabled only for the **Access-Public** interface type.
- **Rx** validation shall be performed only if the **Rx Interface** parameter is set on the **SIP interface** configuration screen. Otherwise no **Rx** handling is required.
- **Rx** messages are sent by the BorderNet to the Diameter server (**PCRF**) only when the BorderNet receives a SIP message with SDP.
- **Rx** authorization process shall be performed before the call is routed, and before any **Rf** or **Ro** messages are sent.

---

The **Diameter Rx** interface:

- is not dependent on Rf/Ro
- is applied only on **Access Public** interfaces.
- sends an Rx message only when the BorderNet receives or sends a SIP message with SDP
- is handled per offer/answer, regardless of the message carrying it



The screenshot shows a configuration window titled "Add Sip Interface". It contains several fields: "Status" (OFF), "Name" (empty), "Domain" (empty), "Network Type" (Access-Public), "Rx Service" (radio buttons for No and Yes, with No selected), and "Diameter Charging Type" (None). A red box highlights the "Rx Service" section.

Figure 8-2: Activate Rx Service

## 9. Element Management System(EMS)

The BorderNet SBC **Element Management System (EMS)** was added to release 3.7.5 and is upgraded in release 3.8.0 to include Provisioning capability.

For further details please refer to the BorderNet EMS User Guide.

The EMS provides a simultaneous and comprehensive management tool for managing up to 100 (one hundred) BorderNet SBCs, distributed in various remote sites.

The EMS provides **Fault, Configuration, Accounting, Performance and Security (FCAPS)** which is the key concept used to define the overall functionality of an Enterprise Management System.

The EMS enables the operator with the following capabilities:

- Dashboard and Topology view, management and provisioning
- Fault management
- Reports and statistics
- User management
- Shortcut to access Analytic
- Debugging tool and call tracing
- License Management (NWL)

---

### Note

The EMS can manage BorderNet SBC with release 3.7.0 and onwards.

---

### 9.1 EMS Dashboard

The EMS Dashboard is the first screen that is displayed after logging into the BorderNet EMS.

The EMS Dashboard provides a global view of the BorderNet in the network.

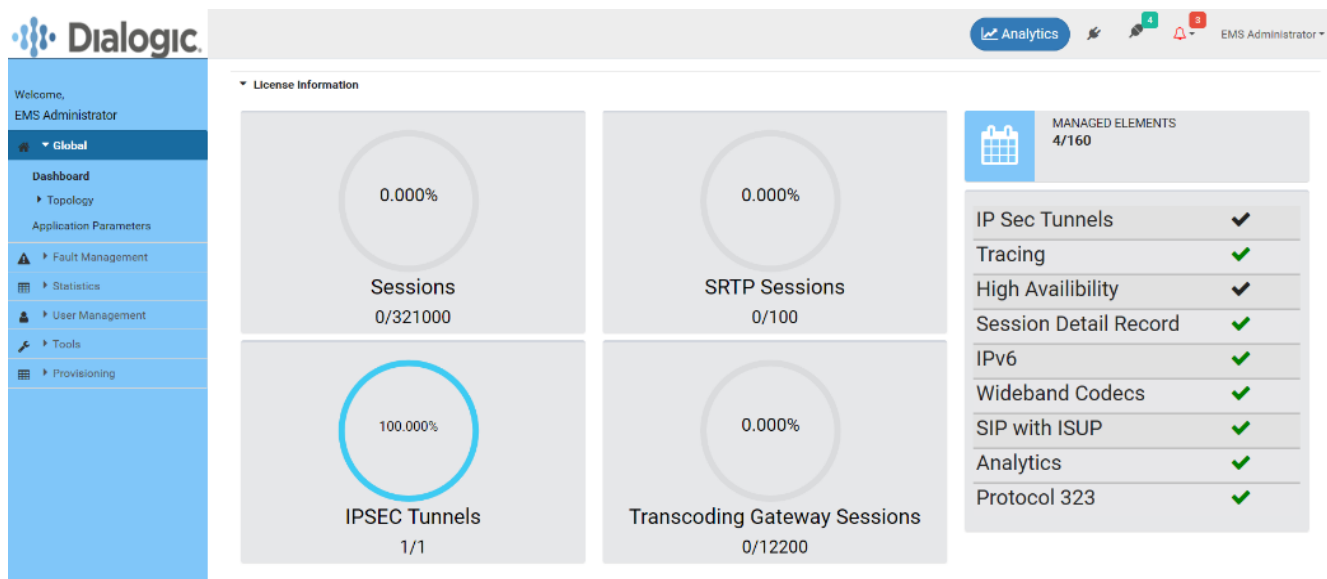


Figure 9-1: EMS Global Dashboard

The interface is divided into four parts: a common toolbar, navigation tree (left pane), middle pane and right pane

The Toolbar shows the following:

- Number of disconnected SBCs shown by icon
- Number of connected SBCs shown by icon
- Number of active alarms shown by bell icon
- Shortcut button to activate analytics

The Left pane shows a menu in the form of a tree (i.e. Navigation tree). This is a starting point to use the EMS functions.

The right pane displays the **Network Wide Licensing (NWL)** information.

At the uppermost right side, the licensed features are shown as follows:

Green Check mark 	All the BorderNet SBCs registered under the EMS have this license.
Black Check mark 	At least one BorderNet SBC has this license but not all of the BorderNet SBCs registered in the EMS have this license.
Red cross mark 	None of the BorderNet SBC registered under the EMS has this license.

The Middle pane shows the utilization of the BorderNet SBCs.



- The amount of purchased licensed resources vs. currently allocated resources.
- Here the percentage usage rates of the following are illustrated:
- Sessions
- SRTP Sessions
- IPSEC Tunnels
- Transcoding Gateway Sessions

Each connected BorderNet can be accessed from the Dashboard for information viewing and provisioning.

## 9.2 Topology View

The Topology View window displays a map of all the defined BorderNet SBCs

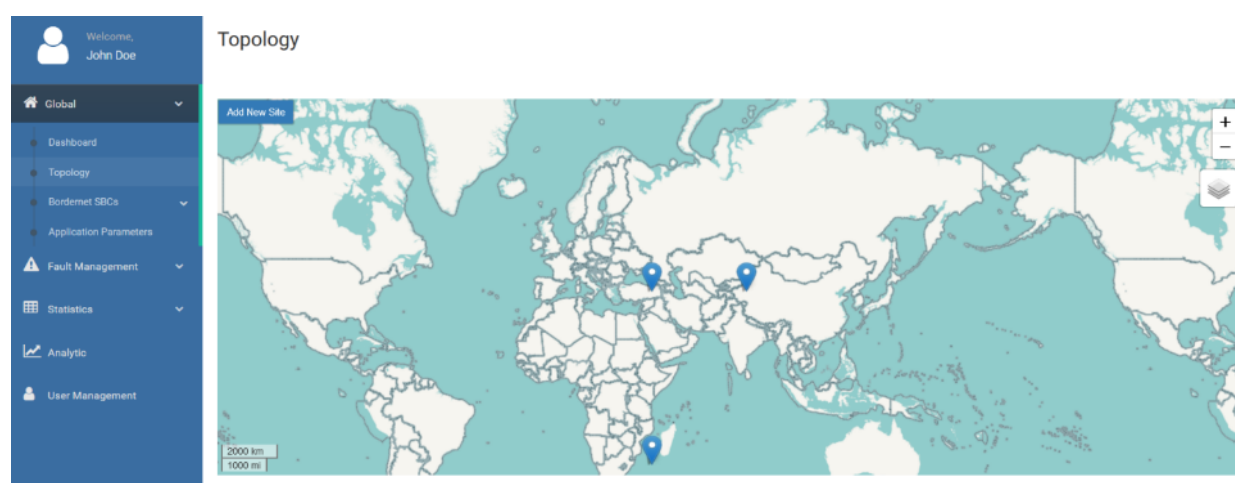


Figure 9-2: EMS Topology View

When in the Topology View screen, the user can add, edit, move or delete a site.

## 9.3 Application Parameters

These are part of the basic configuration of the EMS. The parameters allow you to view, change and set values to the following:

- Analytic access address
- Communication fine-tuning parameters
- LDAP access parameters for EMS user validation
- Log level to be captured and stored
- Purge set-up
- GUI update interval

## 9.4 Fault Management

The **Fault Management** window displays the BorderNet SBCs, under the control of the EMS alarms.

The user is able to export alarms, filter alarms, view alarms history and customize the alarm parameter view. It is possible to view the alarms of a specific BorderNet SBC or the alarms of the whole network.

## 9.5 User Management

The **User Management** GUI allows you to manage the login policy and the BorderNet SBC users.

The EMS comes with three pre-defined users:

- **EMS Admin** – The Administrator of the system. Has full management capabilities.
- **EMS User** – Normal user. Has full access except management of users.
- **EMS Query** – Read-only user. This user is unable to perform any changes in the system.

These users are defined internally and are not used for daily operations.

The EMS Admin user can add users that will operate the BorderNet SBC. For BorderNet SBC systems that are deployed with the BorderNet EMS, the users performing regular operations are provisioned in external servers, normally with LDAP access.

The EMS will access this server (e.g. via LDAP access) for authorizing them to login into the BorderNet.

## 9.6 Reports and Statistics

The **Statistics** window provides a global view of the whole network, and if selected through a specific BorderNet SBC menu, it displays the data of the selected BorderNet SBC.

The displayed information can be filtered per SBC and/or per SBC region.

The aggregate data is collected from all the processes and at a predefined interval it is forwarded to the EMS server database, and then displayed per user request.

The list of reports is dynamically built according to the server data, and can be displayed as a graphic chart or table. The charts of the tables can be exported and viewed by external applications.

## 9.7 Analytics

Please read chapter 12, Dialogic Analytics.

## 9.8 Network Wide License Management

Please refer to chapter 11 of this document.

## 9.9 Provisioning

# 10. Integrated Management

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

- Software Management for upgrades and releases.
- System Configuration to provision the BorderNet 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.

## 10.1 Dashboard

The dashboard management functionality is accessible through the Web UI.

Upon logging into the BorderNet 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.

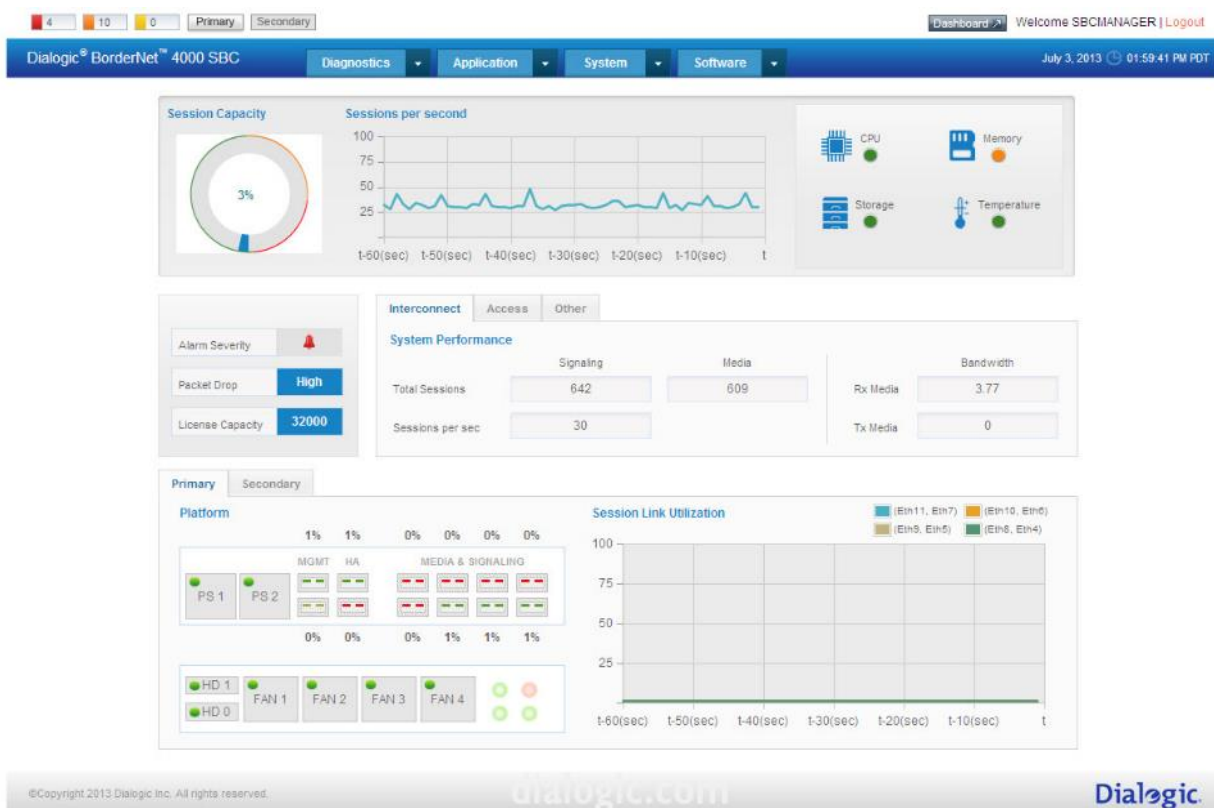


Figure 10-1: BorderNet SBC Dashboard

## 10.2 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, VLAN.
- Configure user authorization, authentication and access control.

## 10.3 System Audit

The BorderNet 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 secondary servers in a redundant (HA) BorderNet SBC system are coordinated to ensure a full history of events is available before and after a system switch-over.

## 10.4 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.

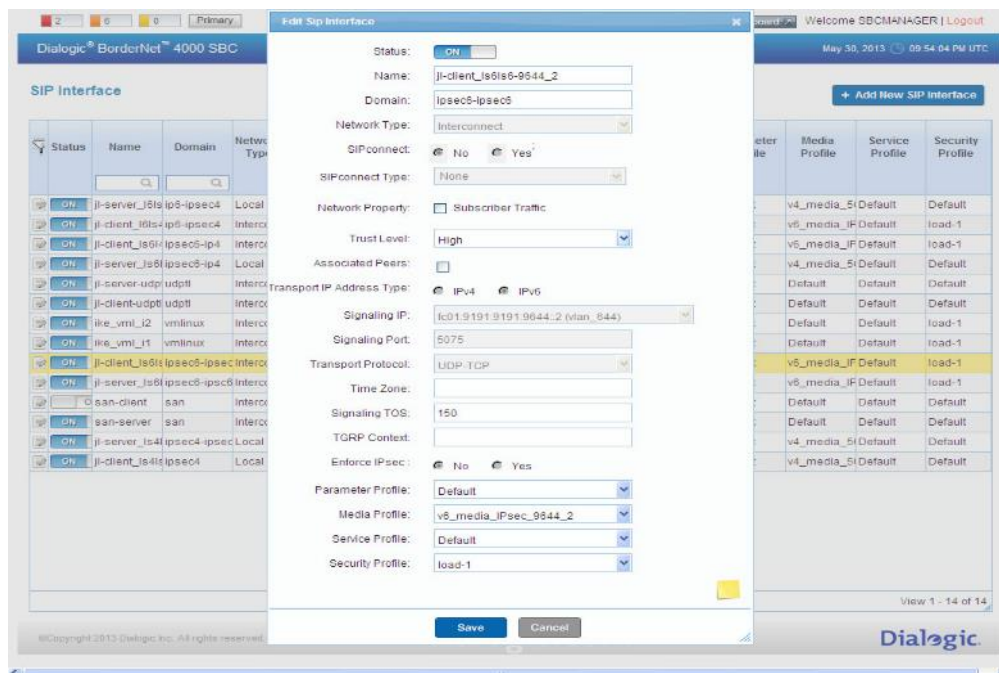


Figure 10-2: BorderNet SBC Configuration

## 10.5 SNMP Support

The BorderNet SBC uses **Simple Network Management Protocol (SNMP)** for sending alarm traps to external SNMP managers, and also for remote SNMP managers to retrieve limited information from the BorderNet via GET requests.

It supports SNMPv3, which enables each SNMP packet to be both authenticated and encrypted in a secure way.

SNMPv3 requires an application to know the identifier (snmpEngineID) of the remote SNMP protocol engine in order to retrieve or manipulate objects maintained on the remote SNMP entity. The EngineID is also one of the inputs used for key derivation of the authentication and privacy keys.

In order to learn the snmpEngineID of a remote SNMP protocol engine, a discovery mechanism is used.

For SNMPv3 traps there is no discovery process. Traps are also not acknowledged.

The authoritative SNMP engine for a trap packet is the sending SNMP agent. Since the generator of the message and the authoritative engine are one and the same, there is no need for the SNMPv3 discovery process. All the information is already inside the single trap message.

As mentioned, SNMPv3 traps use the engineID of the local application sending the trap rather than the engineID of the remote application (like in a GET request). This means that you have to create users in your remote user database (the SNMP trap server) for every engineID you wish to send traps from. Some servers allow all EngineIDs and identify the traps by their user-name.

For further details, refer to the *BorderNet SBC SNMP Guide*.

## 10.6 SOAP/XML API Interface

A **Service Oriented Application Programming (SOAP)** interface to the BorderNet SBC is supported from software Release 3.0 forward.

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.

The SOAP interface supports provisioning of peers, interfaces, peer-interface associations, advanced routing and local DNS.

To assist in deploying this feature, **Dialogic** provides the following for each of the interfaces:

- Sample code
- SOAP Request/Response formats
- Authentication scheme
- XSD schema
- Web Services Definition Language (WSDL)

## 10.7 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 SBC enables operators to change severity, generate an SNMP trap, or generate email notifications for each individual alarm.

## 10.8 Policy-Based Routing

The BorderNet 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 .

## 10.9 Trunk Group Routing/RFC 4904 Compliance

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

The BorderNet 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**

## 10.10 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 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.



Figure 10-3: Customized SDRs

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



## 10.11 Bulk Provisioning

The BorderNet SBC provides **Bulk Provisioning** to facilitate mass configuration of SIP data (Peer, Interface, Interface-Peer, Local DNS and Advanced Policies) via the Web UI.

Data can be updated or exported to a **.csv** or **.txt** file, and this feature provides M2M integration with external routing and billing engines.

## 10.12 Reports

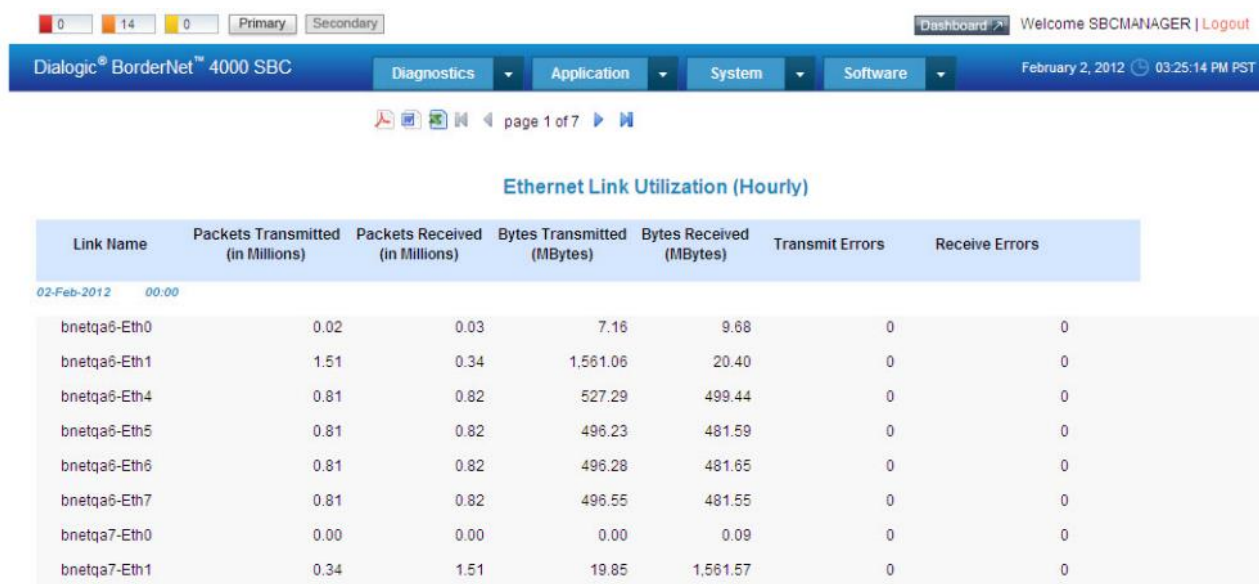
The BorderNet SBC generates reports to show traffic and operational information.

- Statistical data is stored locally on the BorderNet SBC for up to 1 week (7 days).
- Statistical reports are automatically calculated at defined intervals throughout the day.

The BorderNet SBC Web UI supports filtering based on date range and allows an operator to specify report intervals for data samples.

The BorderNet 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 Web UI.

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



Link Name	Packets Transmitted (in Millions)	Packets Received (in Millions)	Bytes Transmitted (MBytes)	Bytes Received (MBytes)	Transmit Errors	Receive Errors
02-Feb-2012 00:00						
bnetqa6-Eth0	0.02	0.03	7.16	9.68	0	0
bnetqa6-Eth1	1.51	0.34	1,561.06	20.40	0	0
bnetqa6-Eth4	0.81	0.82	527.29	499.44	0	0
bnetqa6-Eth5	0.81	0.82	496.23	481.59	0	0
bnetqa6-Eth6	0.81	0.82	496.28	481.65	0	0
bnetqa6-Eth7	0.81	0.82	496.55	481.55	0	0
bnetqa7-Eth0	0.00	0.00	0.00	0.09	0	0
bnetqa7-Eth1	0.34	1.51	19.85	1,561.57	0	0

Figure 10-4: Ethernet Link Utilization Report

The BorderNet SBC automatically generates the following reports:

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

## 10.13 Tracing

The BorderNet SBC includes a customized plug-in that works with the **Wireshark**<sup>®</sup> 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 SBC supports two types of tracing: IP level tracing and session level tracing.

### 10.13.1 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.

IP level tracing supports the following recording profiles:

- Signaling with media.
- Signaling without media (except UDP ports greater than 5100).
- Media drops (RTP packets dropped because of excessive rate, over-utilizing bandwidth etc.)
- Flow drops (advanced rate limit packet drops).

### 10.13.2 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**.

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**.

Session level tracing supports the following recording profiles:

- Signaling without media.
- Signaling with media.
- Media dropped.
- Flows dropped.

### 10.13.3 Media Capture

The BorderNet SBC supports media capture and recording.

The Web UI displays basic RTP stream characteristics, and multiple media streams can be selected and played back.

# 11. Network Wide Licensing (NWL)

The BorderNet SBC provides reliable licensing management.

There are three modes of licensing:

- Regular standalone licensing using a local license file on the BN
- EMS-based network licensing. The EMS retrieves an initial license from the Nalpeiron server using a DLGC interface and builds a local file. There is no on-going license enforcement through Nalpeiron, and only periodic usage updates are sent for statistical purposes. License refresh is triggered manually.

BorderNet has adopted a cloud-based **Network Wide Licensing (NWL)** solution, based on the following logical components, as shown in the figure below:

- Licensing Client - Installed on every BorderNet SBC.
- Licensing Server - Installed on the cloud.

NWL facilitates license sharing of multiple BorderNets. Licenses can be dynamically granted to the distributed BorderNets based on their momentary load. If some are not loaded, then others can utilize the unused license capacity.

The Nalpeiron is still used as the license generator, but after the initial license retrieval, it is not addressed anymore by the EMS or by the BorderNet.

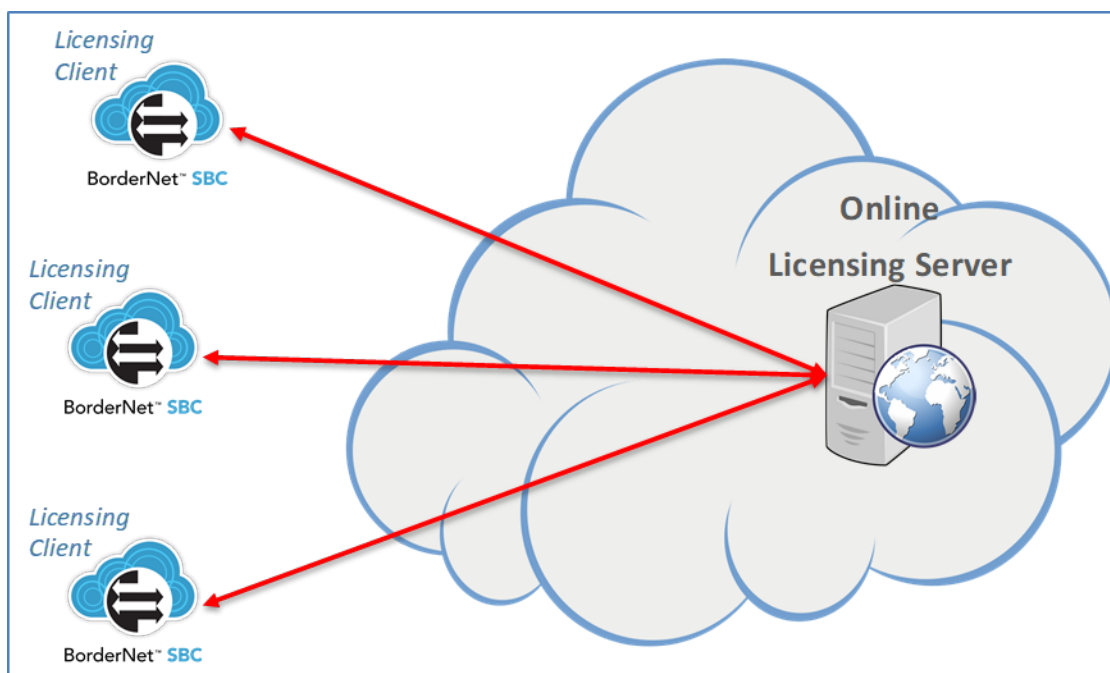


Figure 11-1: BorderNet SBC's Network Wide Licensing Architecture

The solution is agnostic to the deployment type (hardware, virtualized and cloud), and to the operating system (any Linux flavor supported by the BorderNet SBC).

When the NWL is activated:

- A code is created in the Licensing server per BorderNet SBC (or a group of BorderNet SBCs), together with the relevant feature list, and is provisioned in the EMS.
- The code is sent to each BorderNet SBC. The BorderNet SBC creates its own feature list.
- After the initialization, the BorderNet SBC (the licensing client) sends the **GetLicenseInfo** message and the license code to the Licensing server.
- The **GetLicenseInfo** message's response is sent back together with the feature list. Upon receiving the response, the BorderNet SBC populates the feature list and activates a timer using the **RefreshFeatureListtimer**'s value (see [Provisioning](#)).
- Upon the timer's expiration, the client periodically sends the **UpdateLicenseInfo** request and resets the timer each time.
- The **UpdateLicenseInfo** response contains the full list of features.
- For the **Yes/No** licenses, the feature list value is checked, the relevant action is taken accordingly, and for the **Quantitative** licenses, the feature's value is incremented per session, and is checked. If the value is larger than the value in the feature list, the session is rejected.
- The updates and steps that follow the update are provided periodically.

In the case of EMS-based NWL, the EMS creates a non-reproducible license and uses it locally. It then sends periodic usage reports as accumulated values only and not per BorderNet. This is illustrated in the figure below.

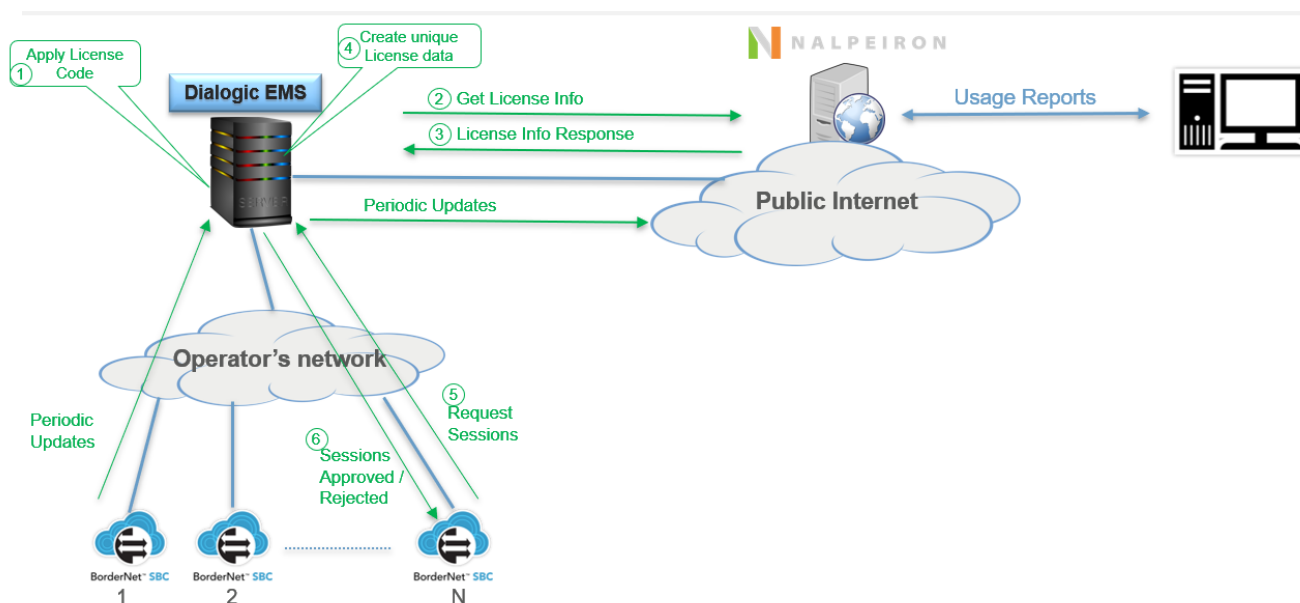


Figure 11-2: EMS-Based Network Wide Licensing

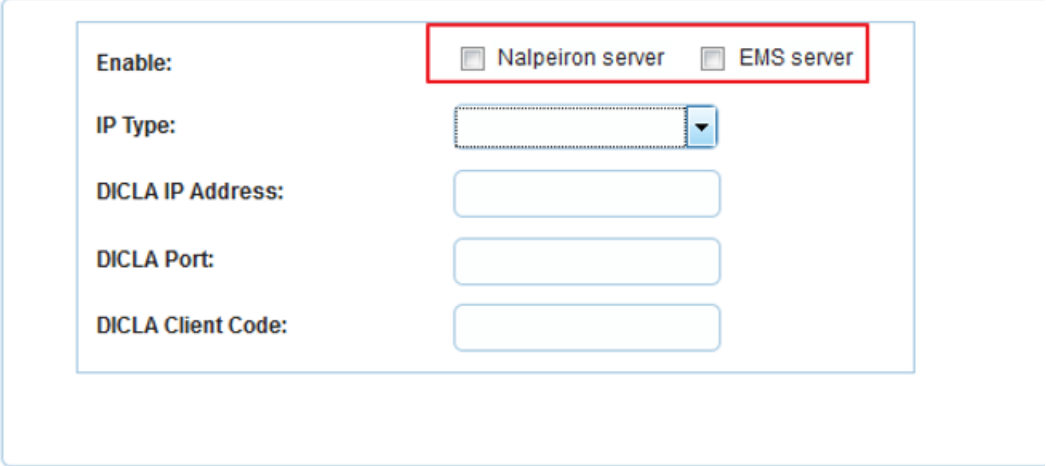
EMS to BorderNet communication is based on the current **RESTfull API** mechanism and all licensing messages are encrypted and authorized.

Message types include the following:

- **EMSGetLicense** – BorderNet to EMS: request for a new initial license, or a request for updating the existing license, if the license has been changed. If this request fails it is reattempted every 60 seconds.
- **EMSGetLicenseResponse** – EMS to BorderNet: list of full licenses and features.
- **EMSUpdate** – BorderNet to EMS: periodic updates on the amount of sessions and features used and requested. Used to both request and inform on current sessions usage.
- **EMSUpdateResponse** – EMS to BorderNet: The amount of sessions approved per each feature.

Network Wide Licensing configuration can be implemented directly from the BorderNet screen:

### Network Wide Licensing Configuration



The screenshot shows the Network Wide Licensing Configuration interface. It features the following elements:

- Enable:** Two checkboxes are present:  Nalpeiron server and  EMS server. These two checkboxes are enclosed in a red rectangular box.
- IP Type:** A dropdown menu with a blue arrow pointing downwards.
- DICLA IP Address:** A text input field.
- DICLA Port:** A text input field.
- DICLA Client Code:** A text input field.

Figure 11-3: NWL Configuration in BorderNet

## 12. Dialogic Analytics

Dialogic Analytics is based on the open source **Elastic Stack**, which takes data from any source, in any format, and enables an operator to search, analyze and visualize the data in real time.

The **DataForwarder** (Dialogic client - installed on the BorderNet SBC), gathers and forwards the performance and **Session Detail Record (SDR)** to a centralized analytics server that presents the processed information.

- The following figure displays the media statistics dashboard that contains the following information:
- "Audio/video/image jitter.
- "Latency.
- "Packet loss.
- "Ingress/Egress r-factor.
- "Audio Codecs Ingress vs. Egress.
- "Top Ingress/Egress peers.

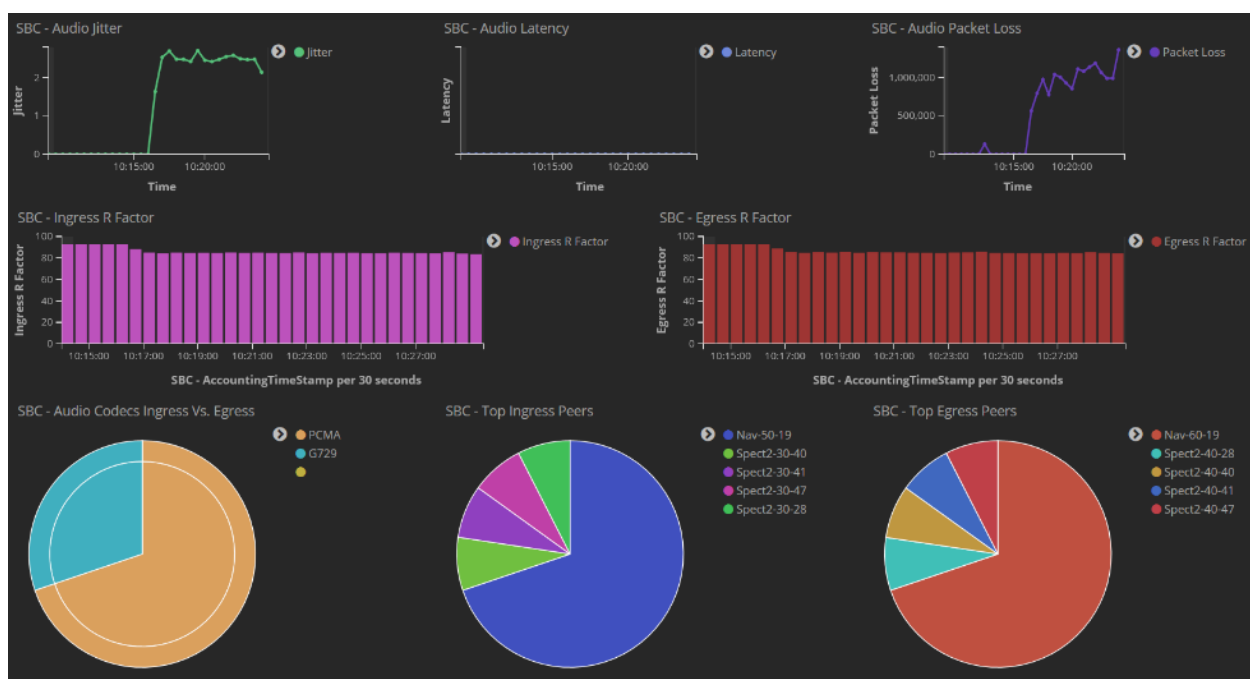


Figure 12-1: BorderNet SBC Media Statistics Dashboard

The **Dialogic Analytics** system is provided as a cluster architecture consisting of multiple **nodes**.

There are two types of node in an Analytic cluster:

- **Master.** Master nodes perform cluster-wide actions, such as managing indices and determining which data nodes should store specific data shards.
- **Data.** Data nodes hold shards of indexed documents and handle basic data operations such as **Create, Read, Update, and Delete (CRUD)**, search and aggregation operations.

A standard **Dialogic Analytics** High Availability cluster consists of a minimum three master nodes and two data nodes as illustrated in figure 12-2 below.

Dedicated master nodes are required to ensure that master nodes' stability cannot be compromised by intensive data node work.

The minimum three master nodes must be running for the cluster to function normally, which can be referred to as **quorum**. This is to ensure data consistency in the event that one or more master nodes lose connectivity to the rest of the cluster, preventing what is known as a "split-brain" situation. This is where the single cluster of nodes gets divided (or partitioned) into smaller clusters of equal numbers of nodes, each of which believes it is the only active cluster.

The minimum two data nodes must be running for data redundancy.

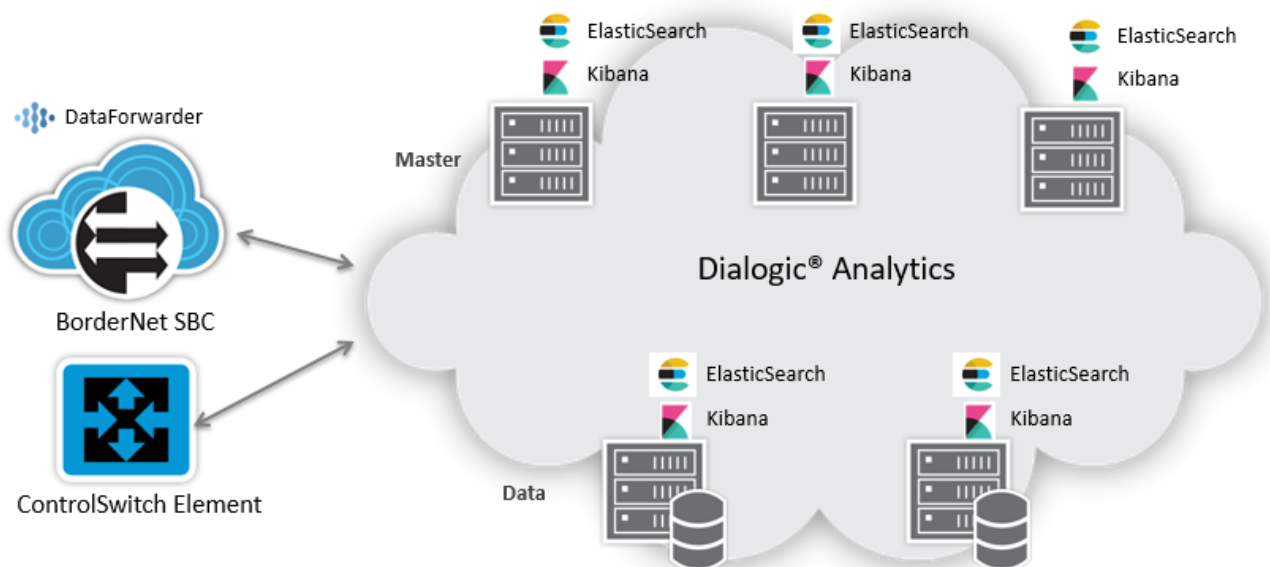


Figure 12-2: Dialogic Analytic Cluster Architecture



## 13. Lawful Interception (LI)

The BorderNet SBC forks (duplicates), and forwards the targets' signaling and media information over the IP network to a third-party **Mediation Device (MD)**, which provides the interface towards the **Legal Enforcement Agency (LEA)**.

The following figure depicts the LI architecture:

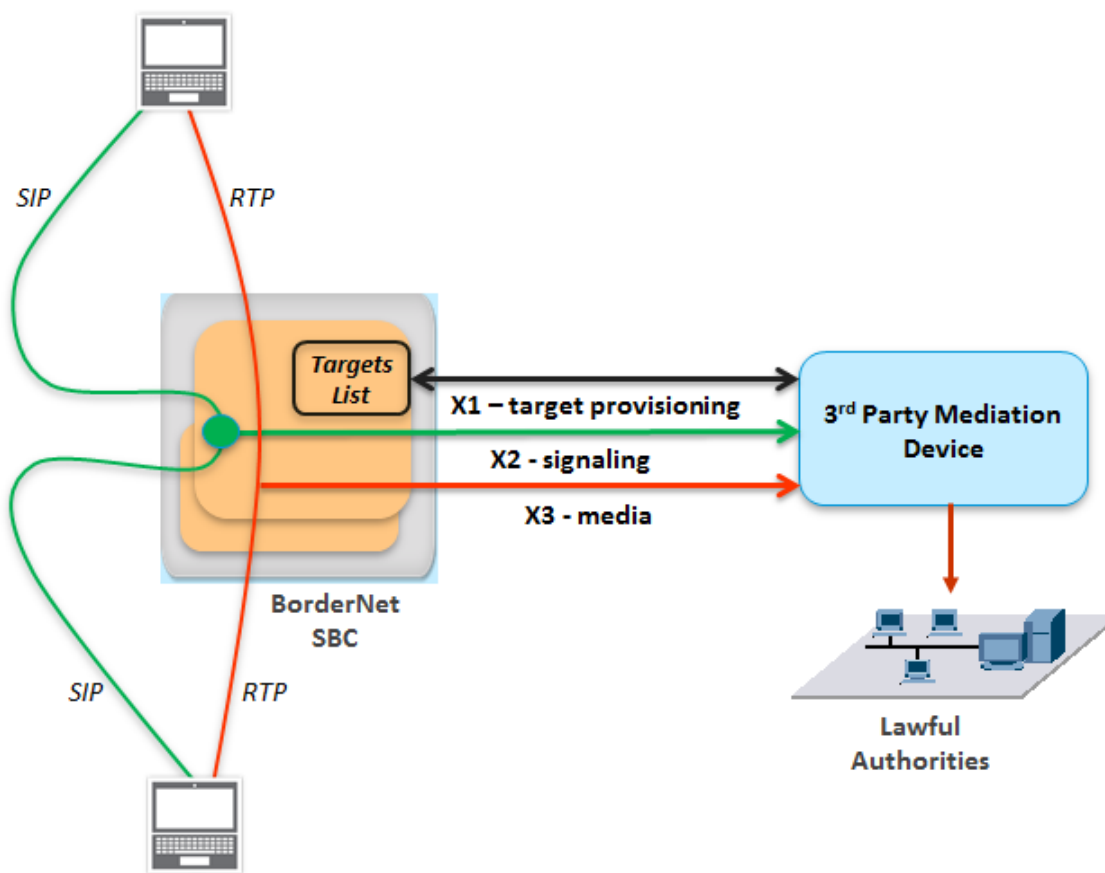


Figure 13-1: LI Architecture

The MD provisions the target information to the BorderNet SBC's memory (via the X1 interface). Based on a query to the provisioned list of targets, BorderNet SBC decides if the target is involved in the session.

- **X2 interface.** The signaling information (encapsulated in TCP packets).
- **X3 interface.** The media (encapsulated RTP in UDP packets).

The LI operation is fully transparent, with no impact on the BorderNet SBC's services.

The interception sessions are not recorded in the regular session's traces, logs and SDRs. Only the LI\_Admin user is allowed to view the LI logs, traces and events (not including the target information).

# 14. Compliances and Certifications

## 14.1 Specifications Compliance

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

Specification	Details
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 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	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

Specification	Details
RFC 3389	Real-Time Transport Protocol (RTP) Payload for Comfort Noise (CN)
RFC 3427	Change Process for the Session Initiation Protocol (SIP)
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

Specification	Details
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 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

Specification	Details
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 5069	Security Threats and Requirements for Emergency Call Marking and Mapping
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

Table 14-1: Compliances with Specifications

## 14.2 Certifications of Compliance

### 14.2.1 BroadSoft BroadCloud R22 Certification

The BorderNet SBC is certified for interoperability with BroadSoft **BroadCloud Release 22**, which encompasses the basic and advanced Class 5 feature set.

Please refer to the *BroadWorks Session Controller Interoperability Test Report* for additional information.

[https://www.broadsoft.com/technology-innovation-blog/broadcloud\\_release\\_22\\_22.1\\_make\\_sure\\_you\\_are\\_ready](https://www.broadsoft.com/technology-innovation-blog/broadcloud_release_22_22.1_make_sure_you_are_ready)

## 14.2.2 SIPconnect 1.1 Compliance

The BorderNet 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 Two-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.

END OF DOCUMENT