



Maintenance Guide

Dialogic[®] BorderNet[™] Session Border Controller (SBC)

Release 3.8.1

June 2019

Table of Contents

1. Introduction
 - 1.1 Purpose of this Document
 - 1.2 Glossary
 - 1.3 Contact Us
2. Alarms
 - 2.1 Categories
 - 2.2 Pending
 - 2.3 Alarm History
 - 2.4 Customization
3. Reports
 - 3.1 System Performance
 - 3.2 Traffic Statistics
 - 3.3 System Statistics
 - 3.3.1 Summary
 - 3.3.2 Packet Statistics
 - 3.3.3 Incoming Sessions
 - 3.3.4 Outgoing Sessions
 - 3.4 Interface Statistics
 - 3.4.1 Summary
 - 3.4.2 Packet Statistics
 - 3.4.3 Incoming Sessions
 - 3.4.4 Outgoing Sessions
 - 3.5 Peer Statistics
 - 3.5.1 Summary
 - 3.5.2 Packet Statistics
 - 3.5.3 Incoming Sessions
 - 3.5.4 Outgoing Sessions
4. Trace
 - 4.1 Downloading the Trace Plug-in
 - 4.2 Connecting to the BorderNet SBC from Wireshark
 - 4.3 Recording Profiles
 - 4.4 Message Based Capture Filters
 - 4.5 Interface Based Capture Filters
 - 4.6 Session Tracing
 - 4.7 Media Capture
 - 4.8 SIP Capture
5. Dashboard
6. System Status
 - 6.1 ACL Status
 - 6.2 DNS Cache
 - 6.3 Registration Cache
 - 6.4 IP Route Status

- 6.5 IPsec Policy Status
- 6.6 IPsec Security Association Status
- 6.7 Black List Entries
- 7. Analytic Configuration
- 8. Software Management
 - 8.1 Displaying Software Information
 - 8.2 Uploading a New Software Release
 - 8.3 Upgrading Software
 - 8.4 Software Roll Back
 - 8.5 Restoring and Backing up Configuration Data
 - 8.5.1 Starting the Backup
 - 8.5.2 Uploading the Backup
 - 8.5.3 Restoring the Backup
 - 8.5.4 Downloading the Backup
 - 8.5.5 Deleting the Backup
 - 8.6 Upgrade / Rollback Update
 - 8.7 Generating LRBT Package and Provisioning
- 9. Audit Logs
- 10. Additional Diagnostics Tools
 - 10.1 Logged In Users
 - 10.2 Remove Older Builds
 - 10.3 Cores
 - 10.4 BorderNet SBC Dump
- 11. Troubleshooting
 - 11.1 Alarms
 - 11.2 SCS Resources

Copyright and Legal Notice

Copyright © 2016-2019 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.

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.

Revision History

Revision	Release Date	Notes
1.0	February 2016	Release 3.3 - editing and formatting
1.1	February 2016	Release 3.4 - HP platform
1.2	November 2016	Release 3.5.0 - Updated statistical reports, added an update to the upgrade/rollback procedure
1.3	March 2017	Updated for released 3.6.0: Added: -Media Inactivity Call Disconnection alarm added to the alarms' list -DNS Cache window -Analytic Configuration -Alarms' list is updated
1.4	May 2017	Added description to SDR Extremely Low Disk & SDR Low Disk alarms.
2.0	September 2017	Updated for released 3.7.0: -Added a new tab: Tools, in Software menu, to support the LRBT capability -Added SIP Capture capability -Removed <i>CPU Utilization Reached Overload Level</i> alarm -The following alarms have been added: <ul style="list-style-type: none"> • CPUmng Utilization Reached Overload Level • CPUmedia Utilization Reached Overload Level • Memory Utilization Reached Overload Level • Root Extremely Low Disk • Root Low Disk alarms.
2.1	October 2017	Added the LRBT filename 's format rules
2.2	March 2018	Release 3.7.5
2.3	August 2018	Updates for release 3.7.6
2.4	December 2018	Updates for release 3.8.0
2.5	May 2019	Updates for release 3.8.1

1. Introduction

1.1 Purpose of this Document

This document provides the information needed to maintain the BorderNet Session Border Controller (SBC) after it is installed, deployed and configured.

The BorderNet SBC's Web GUI presents the **Monitor and Diagnostics** plus **Software and Management** windows, which facilitate system maintenance and details on [Audit Logs](#) and [Troubleshooting](#).

The following procedures are available from the **Monitor and Diagnostics** menu:

- [Alarms](#)
- [Reports](#)
- [Tracing](#)
- [System Status](#)
- [Real-Time Status and Performance](#)

The [Software Management](#) module enables the software upgrade, uploading new releases of software.

This document includes the following sections:

1.2 Glossary

For the purposes of this document the following abbreviations apply:

Abbreviation	Meaning
ACL	Access Control List
HA	High Availability
LRBT	Local Ring Back Tone
NAPTR	Name Authority Pointer
QoS	Quality of Service
RR	Resource Record
SBC	Session Border Controller
SRV	Service Record
TTL	<ul style="list-style-type: none">• Time to Live

Table 1: Glossary

1.3 Contact Us

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

2. Alarms

The Web GUI collects and displays the following categories of alarms:

- **Pending Alarm.** Allows operators to filter and view all pending alarms based on severity, category, time and name.
- **Alarm History.** Allows operators to filter and view all historical alarms based on severity, name, category, time, reported object type and FDN.
- **Alarm Customization.** Enables operators to customize severity, to set whether to generate an SNMP trap, or send an email notification for each individual alarm.

See also the [Alarms](#) section in the [Troubleshooting](#) chapter for the alarms list and corrective actions.

2.1 Categories

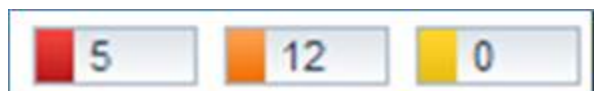
BorderNet SBC supports the following alarm categories:

- QoS
- Configuration
- HA
- License
- Peer
- Overload
- Hardware
- Network
- System
- Security
- Session

The following are the severity levels and the corresponding icon:

- **Critical** 🚨. Critical alarms are a subgroup of the major alarms. Critical alarms are issued when service has stopped and an immediate corrective action is required.
- **Major** 🚩. Raised when a service-affecting condition has developed and an immediate corrective action is required.
- **Minor** 🟡. Raised due to the existence of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious fault.

In the **Alarms** window, three color coded boxes at the top display the number of current alarms in three categories:



Each of these boxes represents the numbers of outstanding alarms by severity.

Periodic refreshing of these alarm numbers indicates ongoing alarm notification for operator visibility. See the [Troubleshooting](#) chapter for an explanation of alarms and corrective actions.

2.2 Pending

Pending alarms are alarms that are currently reported on the BorderNet SBC that have not been cleared.

The alarm history shows cleared alarms.

→ To report the pending alarms:

1. From the **Diagnostics** menu, under the **Alarms** section, select **Pending**.
2. The **Pending Alarm Summary** window opens.

Severity	Category	Time	Name	Reported Type	Reported FQDN	Content
Warning	Network	2011-10-12+08:39:58	Physical Interface Failed	interface	PlatformMainut.InterfaceEtn3	Etn3 Physical interface has failed
Warning	Network	2011-10-12+08:39:58	Physical Interface Failed	interface	PlatformMainut.InterfaceEtn6	Etn6 Physical interface has failed
Warning	Network	2011-10-12+08:39:58	Physical Interface Failed	interface	PlatformMainut.InterfaceEtn10	Etn10 Physical interface has failed
Warning	Network	2011-10-12+08:39:58	Physical Interface Failed	interface	PlatformMainut.InterfaceEtn7	Etn7 Physical interface has failed
Warning	Network	2011-10-12+08:39:58	Physical Interface Failed	interface	PlatformMainut.InterfaceEtn11	Etn11 Physical interface has failed
Warning	Network	2011-10-12+08:39:58	Physical Interface Failed	interface	PlatformMainut.InterfaceEtn8	Etn8 Physical interface has failed
Warning	Network	2011-10-12+08:39:58	Physical Interface Failed	interface	PlatformMainut.InterfaceEtn5	Etn5 Physical interface has failed
Warning	Network	2011-10-12+08:39:58	Physical Interface Failed	interface	PlatformMainut.InterfaceEtn9	Etn9 Physical interface has failed
Critical	Network	2011-10-12+08:39:58	Link Failed	Link	PlatformMainut.LinkSession1 3	Failure in Ethernet Link on interface Sess
Critical	Network	2011-10-12+08:39:58	Link Failed	Link	PlatformMainut.LinkSession1 4	Failure in Ethernet Link on interface Sess
Critical	Network	2011-10-12+08:39:58	Link Failed	Link	PlatformMainut.LinkSession1 2	Failure in Ethernet Link on interface Sess
Warning	Network	2011-10-12+07:22:49	Physical Interface Failed	interface	PlatformCashes.InterfaceEtn3	Etn3 Physical interface has failed
Warning	Network	2011-10-12+07:22:50	Physical Interface Failed	interface	PlatformCashes.InterfaceEtn6	Etn6 Physical interface has failed
Warning	Network	2011-10-12+07:22:50	Physical Interface Failed	interface	PlatformCashes.InterfaceEtn10	Etn10 Physical interface has failed
Warning	Network	2011-10-12+07:22:50	Physical Interface Failed	interface	PlatformCashes.InterfaceEtn7	Etn7 Physical interface has failed
Warning	Network	2011-10-12+07:22:50	Physical Interface Failed	interface	PlatformCashes.InterfaceEtn11	Etn11 Physical interface has failed
Warning	Network	2011-10-12+07:22:50	Physical Interface Failed	interface	PlatformCashes.InterfaceEtn8	Etn8 Physical interface has failed
Warning	Network	2011-10-12+07:22:50	Physical Interface Failed	interface	PlatformCashes.InterfaceEtn5	Etn5 Physical interface has failed
Warning	Network	2011-10-12+07:22:50	Physical Interface Failed	interface	PlatformCashes.InterfaceEtn9	Etn9 Physical interface has failed
Critical	Network	2011-10-12+07:22:50	Link Failed	Link	PlatformCashes.LinkSession1 3	Failure in Ethernet Link on interface Sess

3. Click the filter button to further refine the results.



4. Edit the alarm reporting criteria in the screen below.

alarm filter

Name:

Severity: Critical Major Minor

Category: SDR Session Qos Peer

License Configuration Security HA

Overload Network Hardware System

Date (YYYY-MM-DD) and Time (HH:MM:SS)

Start Date:

End Date:

Start Time: End Time:

Reported

Type:

FQDN:

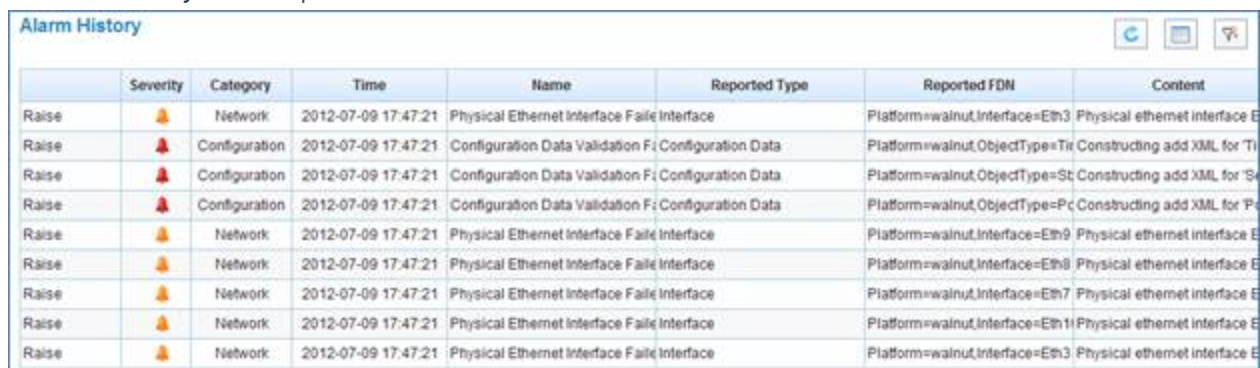
5. Click **OK**.

2.3 Alarm History

Alarms from the last 7 days are retained in the system by default. Non-pending alarms older than 7 days are purged every 24 hours.

→ To report the history of alarms on the BorderNet SBC:

1. From the **Diagnostics** menu, under the **Alarms** section, select **History**.
2. The **Alarm History** window opens.

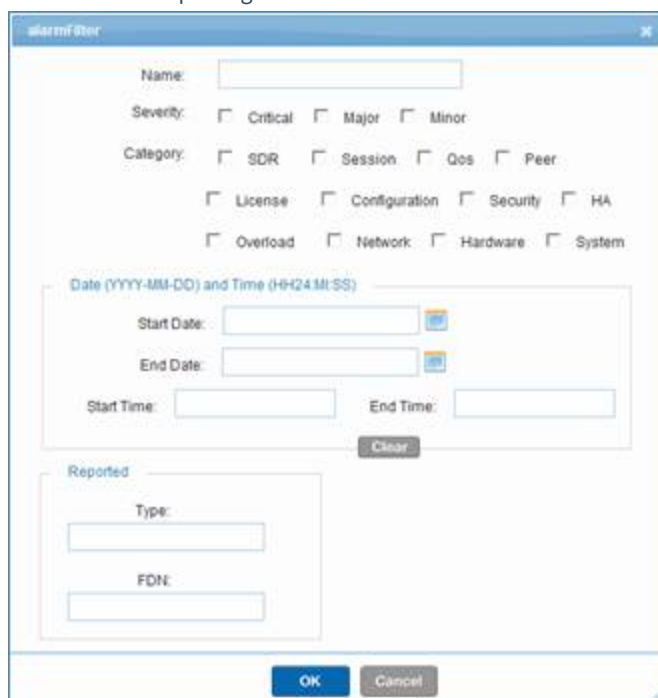


	Severity	Category	Time	Name	Reported Type	Reported FDN	Content
Raise	🚨	Network	2012-07-09 17:47:21	Physical Ethernet Interface Failure Interface		Platform=walnut,Interface=Eth3	Physical ethernet interface E
Raise	🚨	Configuration	2012-07-09 17:47:21	Configuration Data Validation Failure Configuration Data		Platform=walnut,ObjectType=Tr	Constructing add XML for Ti
Raise	🚨	Configuration	2012-07-09 17:47:21	Configuration Data Validation Failure Configuration Data		Platform=walnut,ObjectType=St	Constructing add XML for 'S
Raise	🚨	Configuration	2012-07-09 17:47:21	Configuration Data Validation Failure Configuration Data		Platform=walnut,ObjectType=Pe	Constructing add XML for 'P
Raise	🚨	Network	2012-07-09 17:47:21	Physical Ethernet Interface Failure Interface		Platform=walnut,Interface=Eth9	Physical ethernet interface E
Raise	🚨	Network	2012-07-09 17:47:21	Physical Ethernet Interface Failure Interface		Platform=walnut,Interface=Eth8	Physical ethernet interface E
Raise	🚨	Network	2012-07-09 17:47:21	Physical Ethernet Interface Failure Interface		Platform=walnut,Interface=Eth7	Physical ethernet interface E
Raise	🚨	Network	2012-07-09 17:47:21	Physical Ethernet Interface Failure Interface		Platform=walnut,Interface=Eth11	Physical ethernet interface E
Raise	🚨	Network	2012-07-09 17:47:21	Physical Ethernet Interface Failure Interface		Platform=walnut,Interface=Eth3	Physical ethernet interface E

3. Click the filter button to further refine the results.



4. Edit the alarm reporting criteria in the screen below.




alarm filter


Name:

Severity: Critical Major Minor

Category: SDR Session Qos Peer
 License Configuration Security HA
 Overload Network Hardware System

Date (YYYY-MM-DD) and Time (HH:MM:SS)

Start Date: 

End Date: 

Start Time: End Time:

Reported

Type:

FDN:

5. Click **OK**.

2.4 Customization

→ To customize an alarm:

1. From the **Diagnostics** menu, under the **Alarms** section, select **Customization**.
2. The **Alarm Customization** window opens.

Severity	Category	Name	Severity Editable	Operator Clearable	Logging Enabled	SNMP Traps	Email
Critical	Configuration	Interface Creation Failed	Yes	No	Yes	No	No
Critical	Overload	Bandwidth Limit Reached at Interface	Yes	No	Yes	Yes	Yes
Warning	Security	TLS Connectivity to Un-Configured Peer Failed	Yes	No	Yes	No	No
Warning	Security	TLS Connectivity to Configured Peer Failed	Yes	No	Yes	No	No
Critical	Overload	Session License Limit Reached	Yes	No	Yes	No	Yes
Critical	Overload	System Session Limit Reached	Yes	No	Yes	No	Yes
Warning	Overload	Approaching Session License Limit	Yes	No	Yes	No	Yes
Warning	Overload	Approaching System Session Limit	Yes	No	Yes	No	Yes
Warning	Session	Connectivity Failure with Peer	Yes	No	Yes	No	No
Critical	Configuration	Interface Activation Failed	Yes	No	Yes	No	No
Critical	Configuration	Registration with Gatekeeper failed	Yes	No	Yes	No	No
Warning	QoS	Packet Rate Limit exceeded at Peer	Yes	No	Yes	No	No
Warning	QoS	Packet Rate Limit exceeded at Interface	Yes	No	Yes	No	No
Warning	Security	Excessive Packet Drops	Yes	No	Yes	No	No
Warning	Security	Peer Backstited	Yes	No	Yes	No	No
Warning	QoS	Maximum Active Sessions reached on Peer	Yes	No	Yes	No	No
Warning	QoS	Maximum Active Sessions reached on Interface	Yes	No	Yes	No	No
Warning	QoS	Maximum Outgoing Active Sessions reached	Yes	No	Yes	No	No
Warning	QoS	Maximum Outgoing Active Sessions reached	Yes	No	Yes	No	No
Warning	QoS	Maximum Incoming Active Sessions reached	Yes	No	Yes	No	No

3. Click the edit button for an alarm that you want to edit.



4. The **Customize Alarm** window opens.

Customize Alarm

Event Display Name:

Category:

Severity Editable:

Severity: ▼

Operator Clearable: Yes No

Logging Enabled: Yes No

Generate SNMP Trap: Yes No

Generate Email: Yes No

5. Modify the alarm definition including the severity.
6. Click on **Save** to keep the changes.

3. Reports

BorderNet SBC generates reports on traffic and operational information. Statistical data is stored locally on the BorderNet SBC for up to 7 days, calculated as average values of the terminated calls' data, for a selected time interval (5 min, 1 hour etc.).

To generate and view a report, the time intervals should be defined to either 5 minutes or 1 hour. The reports can be exported to PDF, Word or Excel formats, using the Web GUI.

This section provides the following:

- System Performance
- Traffic Statistics
- System Statistics
- Interface Statistics
- Peer Statistics

The **Chart** and **Table** buttons enable the users to display the data as a table or as a graphic chart:

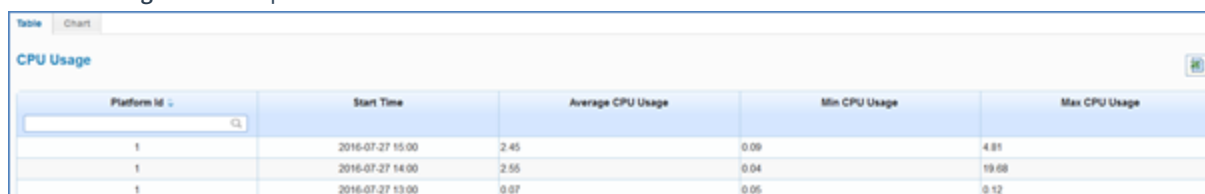
- **Chart.** Enables the user to view each parameter as a chart. To view a parameter in a graphic format, select it first using the drop-down menu.
- **Table.** Enables the user to view the parameters in table format.

3.1 System Performance

CPU Usage

→ To display the CPU usage reports:

1. Select **Diagnostics à System Performance à CPU Usage**.
2. The **CPU Usage** window opens.



Platform Id	Start Time	Average CPU Usage	Min CPU Usage	Max CPU Usage
1	2016-07-27 15:00	2.45	0.09	4.81
1	2016-07-27 14:00	2.55	0.04	19.68
1	2016-07-27 13:00	0.07	0.05	0.12

- 3.
4. Select the following criteria for filtering:

§ **Hourly.** Set to select an hourly interval for the CPU usage report.

§ **Five Minutes.** Set to select a 5-minute interval for the CPU usage report.

§ **Time Range.** Select the start date/time and end date/time of the report period.

1. Click the **Filter** button, to display the statistics for the selected interval:


§ **Platform ID.** The identification number of the platform.

§ **Start Time.** The start time of the calculations.

§ **Average CPU Usage.** The percentage of the average CPU usage in the selected interval.

§ **Min CPU Usage.** The minimum CPU usage percentage in the selected interval.

§ **Max CPU Usage.** The maximum CPU usage percentage in the selected interval.

1. Click on the **Export** icon  to export the display data to a CSV file.
2. Click on **Chart** to see the graphic presentation of the statistics.

3.2 Traffic Statistics

Ethernet Links

→ To display the ethernet links reports:

1. Select **Diagnostics à Traffic Statistics à Ethernet Links.**
2. The **Ethernet Link** window opens.

Link Name	Start Time	Packets Transmitted	Packets Received	Bytes Transmitted (MBytes)	Bytes Received (MBytes)	Transmit Errors	Receive Errors
abc10g/0-Eth0	2016-07-27 15:00	0.0	0.0	2.84	0.72	0	0
abc10g/0-Eth0	2016-07-27 14:00	0.01	0.02	7.74	3.9	0	0
abc10g/0-Eth4	2016-07-27 14:00	2.1	1.21	996.17	529.41	0	0
abc10g/0-Eth5	2016-07-27 14:00	1.07	1.21	693.27	640.14	0	0

3. Select the following criteria for filtering:

§ **Hourly.** Set to select an hourly interval for the CPU usage report.

§ **Five Minutes.** Set to select a 5-minute interval for the CPU usage report.

§ **Time Range.** Select the start date/time and end date/time of the report period.

- Click the **Filter** button, to display the statistics for the selected interval.

§ **Link Name.** The identification number of the platform.

§ **Start Time.** The start time of the calculations.

§ **Packets Transmitted.** The number of transmitted packets per a specified link, in Mbytes.

§ **Packets Received.** The number of received packets per a specified link.

§ **Bytes Transmitted (Mbytes).** The total number of transmitted data in MB.

§ **Bytes Received (Mbytes).** The total number of received data in MB.

§ **Transmit Errors.** Number of transmitted errors.

§ **Receive Errors.** Number of received errors.

1. Click on the **Export** icon  to export the display data to a CSV file.
2. Click on **Chart** to see the graphic presentation of the statistics.

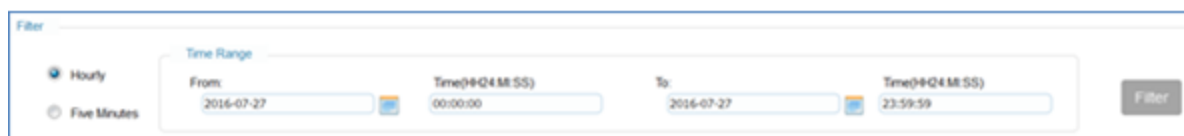
3.3 System Statistics

3.3.1 Summary

→ To display the system statistics summary reports:

1. Select **Diagnostics** à **System Statistics** à **Summary**.

1. The **System Statistics Summary** window opens.



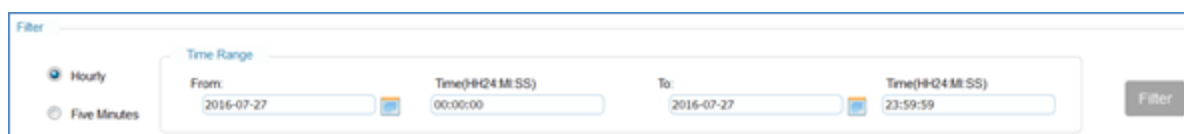
The screenshot shows the 'Filter' section of the 'System Statistics Summary' window. It includes a 'Time Range' section with 'From' and 'To' date/time pickers. The 'From' date is set to 2016-07-27 and the 'To' date is set to 2016-07-27. The time is set to 00:00:00. There are radio buttons for 'Hourly' (selected) and 'Five Minutes'. A 'Filter' button is visible on the right.

- 2.
3. Select the following criteria for filtering:

§ **Hourly.** Set to select an hourly interval for the CPU usage report.

§ **Five Minutes.** Set to select a 5-minute interval for the CPU usage report.

§ **Time Range.** Select the start date/time and end date/time of the report period.



The screenshot shows the 'Filter' section of the 'System Statistics Summary' window. It includes a 'Time Range' section with 'From' and 'To' date/time pickers. The 'From' date is set to 2016-07-27 and the 'To' date is set to 2016-07-27. The time is set to 00:00:00. There are radio buttons for 'Hourly' (selected) and 'Five Minutes'. A 'Filter' button is visible on the right.

- Click the **Filter** button, to display the statistics for the selected interval:

§ **Start Time.** The start time of the calculations.

§ **Incoming Attempts.** Number of incoming sessions attempts.

§ **Outgoing Attempts.** Number of outgoing sessions attempts.

§ **Answered.** Number of sessions answered.

§ **Highest Active.** The total number of active calls.

§ **With Media.** The total number of sessions which their media traverses the BorderNet SBC.

§ **Emergency.** Number of emergency sessions.

§ **Secure.** The total number of secured sessions (with TLS).

§ **Total SIP-I Calls.** The total number of SIP-I sessions.


§ **Transcoded.** The total number of transcoded sessions.

§ **Peak.** Number of peak session rate.

§ **ASR (%).** The Answer Seizure Rate ((answered calls #/call attempts #)/100)

§ **ACD (sec).** The Average Call Duration in seconds.

§ **R-Factor.** Based on delay, and packet loss parameters, the quality of the voice is calculated, and presented as R-Factor in range [0-5], where the highest value presents the highest quality.

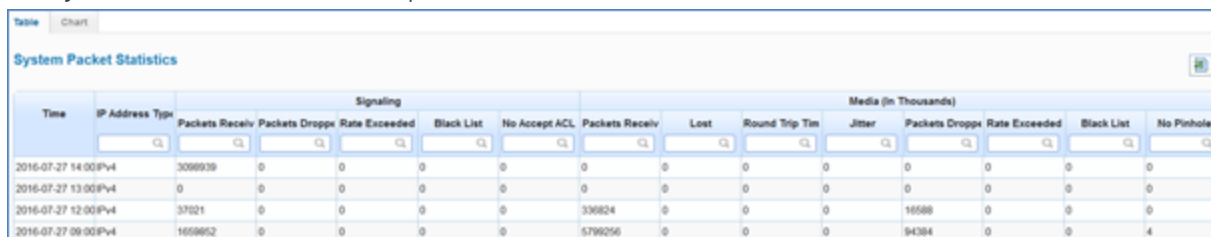
1. Click on the **Export** icon  to export the display data to a CSV file.
2. Click on **Chart** to see the graphic presentation of the statistics.

3.3.2 Packet Statistics

→ To display the system's packet statistics:

1. Select **Diagnostics** à **System Statistics** à **Packet Statistics**.
2. The **System Packet Statistics** window opens.

Time	IP Address Type	Signaling					Media (in Thousands)								
		Packets Receiv	Packets Dropp	Rate Exceeded	Black List	No Accept ACL	Packets Receiv	Lost	Round Trip Tim	Jitter	Packets Dropp	Rate Exceeded	Black List	No Pinhole	
2016-07-27 14:00Pv4		308939	0	0	0	0	0	0	0	0	0	0	0	0	0
2016-07-27 13:00Pv4		0	0	0	0	0	0	0	0	0	0	0	0	0	0
2016-07-27 12:00Pv4		37021	0	0	0	0	336824	0	0	0	16589	0	0	0	0
2016-07-27 09:00Pv4		1659852	0	0	0	0	5796256	0	0	0	94364	0	0	0	4

3. 
4. Select the following criteria for filtering:

§ **Hourly.** Set to select an hourly interval for the CPU usage report.

§ **Five Minutes.** Set to select a 5-minute interval for the CPU usage report.

§ **Time Range.** Select the start date/time and end date/time of the report period.

1. Click the **Filter** button, to display the statistics for the selected interval:

§ **Time.** The start time of the calculations.

§ **IP Address Type.** Type of IP address (IPv4, IPv6)

§ **Packets Received.** The total number of the received signaling packets.

§ **Packets Dropped.** The total number of the dropped signaling packets.

§ **Rate Exceeded.** Signaling packets rate exceeded the maximum limit.

§ **Black List.** The total number of the blacklisted signaling packets.

§ **No Accept ACL.** The total number of signaling packets that did not pass the access list.

§ **Packets Received.** The total number of the received media packets.

§ **Lost.** The total number of the lost media packets.

§ **Round Trip Time.** RTT is calculated based on the RTCP packets, by measuring the delay between the packet's sending and receiving times minus the delay experienced in the remote side. This is calculated only on the Rx, and per peer (calculated in milliseconds).


§ **Jitter.** Jitter is calculated based on a function described in RFC 3550, using the RTP stream's timestamps (calculated in milliseconds).

§ **Packets Dropped.** The total number of the dropped media packets.

§ **Rate Exceeded.** Signaling packets rate exceeded the maximum limit.

§ **Black List.** The total number of the blacklisted media packets.

§ **No Pinhole.** The total number of media packets that did not pass the BorderNet SBC, as a result of pinholes that did not open.

1. Click on the **Export** icon  to export the display data to a CSV file.
2. Click on **Chart** to see the graphic presentation of the statistics.

3.3.3 Incoming Sessions

→ To display the system's incoming statistics:

1. Select **Diagnostics** à **System Statistics** à **Incoming Sessions**.
2. The **System Statistics - Incoming Sessions** window opens.

Time	Type	Sessions							Average	Peak
		Attempted	Answered	Rejected	Highest Active	With Media	Emergency	Dropped Messages(b)		
2016-07-27 14:00	IPv4	537136	450726	0	97091	537136	0	0	162.54545454545453	980
2016-07-27 13:00	IPv4	0	0	0	614	0	0	0	0.0	0
2016-07-27 12:00	IPv4	0	0	0	13421	0	0	0	0.0	0
2016-07-27 09:00	IPv4	165032	112993	0	31090	165033	0	0	137.0	288

- 3.
4. Select the following criteria for filtering:

§ **Hourly**. Set to select an hourly interval for the CPU usage report.

§ **Five Minutes**. Set to select a 5-minute interval for the CPU usage report.

§ **Time Range**. Select the start date/time and end date/time of the report period.

Filter

Hourly
 Five Minutes

Time Range

From: 2016-07-27 00:00:00 To: 2016-07-27 23:59:59

Filter

1. Click the **Filter** button, to display the statistics for the selected interval:

§ **Time**. The start time of the calculations.

§ **Type**. Type of IP address (IPv4, IPv6)

§ **Attempted**. The total number of the incoming session attempts.

§ **Answered**. The total number of the incoming sessions answered.

§ **Rejected**. The total number of the incoming rejected sessions.

§ **Highest Active**. The total number of active calls.


§ **With Media**. The total number of sessions which their media traverses the BorderNet SBC.

§ **Emergency**. The maximum number of incoming emergency sessions.

§ **Dropped Messages**. The total number of dropped incoming messages.

§ **Average**. The average number of the incoming sessions.

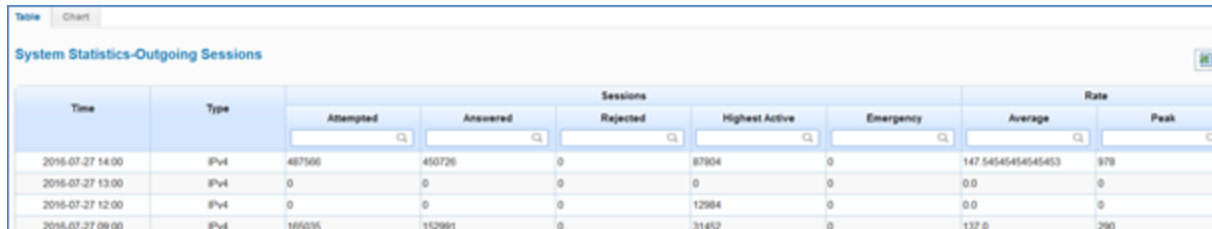
§ **Peak**. Number of peak session rate.

1. Click on the **Export** icon  to export the display data to a CSV file.
2. Click on **Chart** to see the graphic presentation of the statistics.

3.3.4 Outgoing Sessions

→ To display the system's outgoing statistics:

1. Select **Diagnostics** à **System Statistics** à **Outgoing Sessions**.
2. The **System Statistics - Outgoing Sessions** window opens.



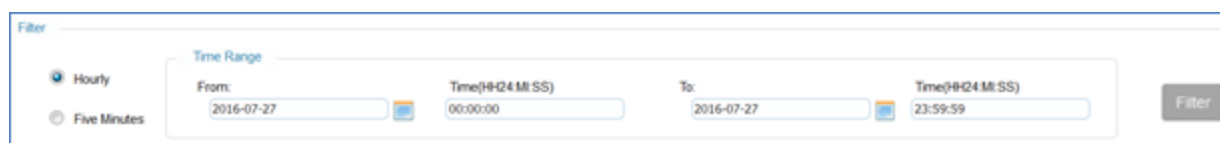
Time	Type	Sessions					Rate	
		Attempted	Answered	Rejected	Highest Active	Emergency	Average	Peak
2016-07-27 14:00	IPv4	487566	450726	0	87804	0	147.54545454545453	978
2016-07-27 13:00	IPv4	0	0	0	0	0	0.0	0
2016-07-27 12:00	IPv4	0	0	0	12984	0	0.0	0
2016-07-27 09:00	IPv4	165035	152991	0	31452	0	137.0	290

3. Select the following criteria for filtering:

§ **Hourly**. Set to select an hourly interval for the CPU usage report.

§ **Five Minutes**. Set to select a 5-minute interval for the CPU usage report.

§ **Time Range**. Select the start date/time and end date/time of the report period.



Filter

Hourly
 Five Minutes

Time Range

From: 2016-07-27 Time(##Q24MISS) 00:00:00 To: 2016-07-27 Time(##Q24MISS) 23:59:59

Filter

1. Click the **Filter** button, to display the statistics for the selected interval:

§ **Time**. The start time of the calculations.

§ **Type**. Type of IP address (IPv4, IPv6)

§ **Attempted**. The total number of the outgoing session attempts.

§ **Answered**. The total number of the outgoing sessions answered.


§ **Rejected**. The total number of the outgoing rejected sessions.

§ **Highest Active**. The total number of active calls.

§ **Emergency**. The maximum number of outgoing emergency sessions.

§ **Average**. The average number of the outgoing sessions.

§ **Peak**. Number of peak session rate.

1. Click on the **Export** icon  to export the display data to a CSV file.
2. Click on **Chart** to see the graphic presentation of the statistics.

3.4 Interface Statistics

3.4.1 Summary

1. Select **Diagnostics** à **Interface Statistics** à **Summary**.
2. The **Interface Statistics Summary** window opens.

- 3.
4. Select the following criteria for filtering:
 - § **Hourly**. Set to select an hourly interval for the CPU usage report.
 - § **Five Minutes**. Set to select a 5-minute interval for the CPU usage report.
 - § **Time Range**. Select the start date/time and end date/time of the report period.

1. Click the **Filter** button, and the following appears.

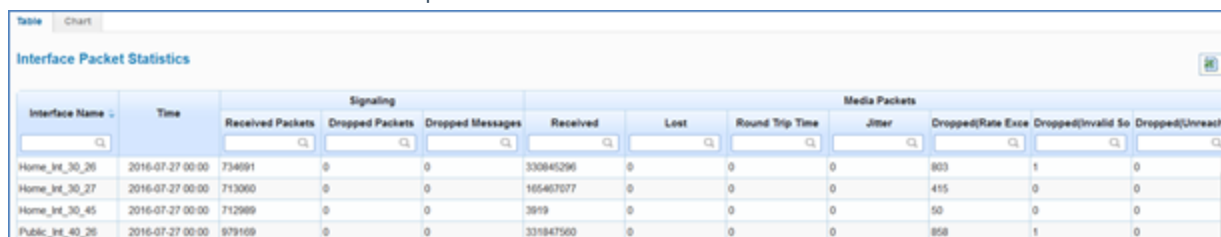
- § **Interface Name**. The name of the interface.
- § **Start Time**. The start time of the calculations.
- § **Attempted**. Total number of attempted sessions per the specified interface.
- § **Answered**. Number of sessions answered.
- § **With Media**. The total number of sessions which their media traverses the BorderNet SBC.
- § **Emergency**. Number of emergency sessions.
- § **Received Packets**. Number of received packets.
- § **Dropped Packets**. Number of packets dropped.
- § **Dropped Messages**. Number of messages dropped.
- § **Total SIP-I Calls**. The total number of SIP-I sessions.
- § **Transcoded**. The total number of transcoded sessions.
- § **ASR (%)**. The Answer Seizure Rate ((answered calls #/call attempts #)/100)
- § **ACD (sec)**. The Average Call Duration in seconds.

§ **R-Factor**. Based on delay, and packet loss parameters, the quality of the voice is calculated, and presented as R-Factor in range [0-5], where the highest value presents the highest quality.

1. Click on the **Export** icon  to export the display data to a CSV file.
2. Click on **Chart** to see the graphic presentation of the statistics.

3.4.2 Packet Statistics

1. Select **Diagnostics** à **Interface Statistics** à **Packet Statistics**.
2. The **Interface Packet Statistics** window opens.



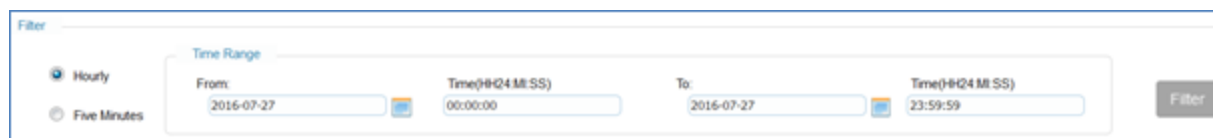
Interface Name	Time	Signaling			Media Packets							
		Received Packets	Dropped Packets	Dropped Messages	Received	Lost	Round Trip Time	Jitter	Dropped(Rate Exce	Dropped(Invalid So	Dropped(Unreachal	
Home_int_30_26	2016-07-27 00:00	734891	0	0	300845296	0	0	0	803	1	0	
Home_int_30_27	2016-07-27 00:00	713060	0	0	165407077	0	0	0	415	0	0	
Home_int_30_45	2016-07-27 00:00	712989	0	0	3919	0	0	0	50	0	0	
Public_int_40_26	2016-07-27 00:00	979169	0	0	331947560	0	0	0	858	1	0	

- 3.
4. Select the following criteria for filtering:

§ **Hourly**. Set to select an hourly interval for the CPU usage report.

§ **Five Minutes**. Set to select a 5-minute interval for the CPU usage report.

§ **Time Range**. Select the start date/time and end date/time of the report period.



1. Click the **Filter** button to display the signaling and media packet statistics reports per each interface:

§ **Interface Name**. The name of the interface.

§ **Time**. The start time of the calculations.

§ **Received Packets**. The total number of the received signaling packets.

§ **Dropped Packets**. The total number of the dropped signaling packets.

§ **Dropped Messages**. The total number of the dropped messages.

§ **Received**. The total number of the received media packets.

§ **Lost**. The total number of the lost media packets.

§ **Round Trip Time**. RTT is calculated based on the RTP packets, by measuring the delay between the packet's sending and receiving times minus the delay experienced in the remote side. This is calculated only on the Rx, and per peer (calculated in

milliseconds).

§ **Jitter**. Jitter is calculated based on a function described in RFC 3550, using the RTP stream's timestamps (calculated in milliseconds).

§ **Dropped Rate Exceeded**. Number of dropped packets that exceeded the bandwidth limit.

§ **Dropped Invalid Source**. Number of dropped packets with invalid source (at the receive side).

§ **Dropped Unreachable**. Number of dropped packets that could not be transmitted.



1. Click on the **Export** icon to export the display data to a CSV file.
2. Click on **Chart** to see the graphic presentation of the statistics.

3.4.3 Incoming Sessions

1. Select **Diagnostics** à **Interface Statistics** à **Incoming Sessions**.
2. The **Interface Statistics - Incoming Sessions** window opens.

Interface Name	Time	Sessions				Rate		Rejected Sessions				Bandwidth		
		Attempted	Answered	Max Active	Emergency	Average	Peak	Rate Exceeded	Active Limit	Incoming Limit	Overload	Bandwidth Lim	Usage (mbps)	Relative Usage
Home_Int_30_26	2016-07-27 15:00:17974	17793	17792	0	59.0	324	0	0	0	0	0	0	2 084 984.00	0
Home_Int_30_27	2016-07-27 15:00:17970	17790	17793	0	59.0	325	0	0	0	0	0	0	2 084 520.00	0
Home_Int_30_45	2016-07-27 15:00:18520	18318	18327	0	61.0	335	0	0	0	0	0	0	2 148 320.00	0

3. Select the following criteria for filtering:

§ **Hourly**. Set to select an hourly interval for the CPU usage report.

§ **Five Minutes**. Set to select a 5-minute interval for the CPU usage report.

§ **Time Range**. Select the start date/time and end date/time of the report period.

Filter

Hourly
 Five Minutes

Time Range

From: 2016-07-27 Time(H:Q4 M:SS) 00:00:00 To: 2016-07-27 Time(H:Q4 M:SS) 23:59:59

Filter

1. Click the **Filter** button to display the selected interface's incoming statistics reports:

§ **Interface Name**. The name of the interface.

§ **Time**. The start time of the calculations.

§ **Attempted**. The total number of the incoming session attempts.

§ **Answered**. The total number of the incoming sessions answered.

§ **Max Active**. The total number of incoming active calls.

§ **Emergency**. The maximum number of incoming emergency sessions.

§ **Average.** The average rate of the incoming sessions.

§ **Peak.** Number of incoming peak session rate.

§ **Rate Exceeded.** Number of incoming rejected sessions. If the current rate (session per second), exceeds the session rate and the burst rate (the percentage allowed to pass the session rate for cases of temporary load), then the call is rejected. The session rate and burst rate are configured in the security profile.

§ **Active Limit.** Number of rejected sessions. The calls are rejected when the number of active calls exceeds the maximum active sessions (configured in security profile).


§ **Incoming Limit.** Number of rejected incoming sessions. The incoming calls are rejected when the number of incoming sessions exceeds the maximum incoming sessions (configured in security profile).

§ **Overload.** Number of rejected sessions due to overload (i.e. CPU overload...).

§ **Bandwidth Limit.** Total number of rejected calls due to full use of the bandwidth, allocated for this interface (configured in media profile).

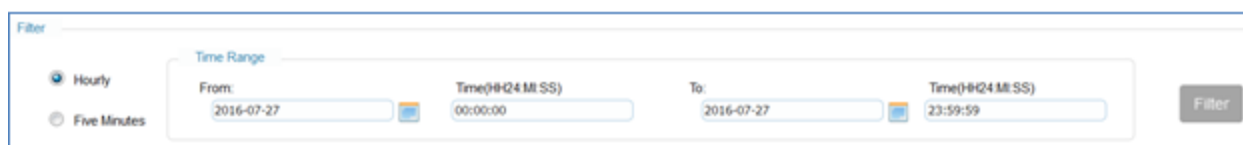
§ **Usage (mbps).** Bandwidth utilization in MB/sec.

§ **Relative Usage.** The bandwidth utilization based on the configured total bandwidth.

1. Click on the **Export** icon  to export the display data to a CSV file.
2. Click on **Chart** to see the graphic presentation of the statistics.

3.4.4 Outgoing Sessions

1. Select **Diagnostics** à **Interface Statistics** à **Outgoing Sessions**.
2. The **Interface Statistics - Outgoing Sessions** window opens.



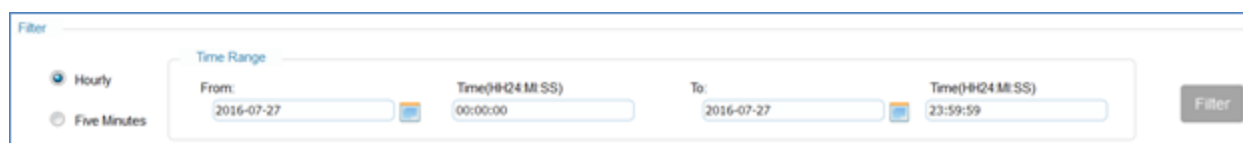
3.

1. Select the following criteria for filtering:

§ **Hourly.** Set to select an hourly interval for the CPU usage report.

§ **Five Minutes.** Set to select a 5-minute interval for the CPU usage report.

§ **Time Range.** Select the start date/time and end date/time of the report period.



1. Click the **Filter** button to display the selected interface's outgoing statistics reports:

§ **Interface Name.** The name of the interface.

§ **Time.** The start time of the calculations.

§ **Attempted.** The total number of the outgoing session attempts.

§ **Answered.** The total number of the outgoing sessions answered.

§ **Max Active.** The total number of outgoing active calls.

§ **Emergency.** The maximum number of outgoing emergency sessions.

§ **Average.** The average rate of the outgoing sessions.

§ **Peak.** Number of outgoing peak session rate.

§ **Rate Exceeded.** Number of outgoing rejected sessions. If the current rate (session per second), exceeds the session rate and the burst rate (the percentage allowed to pass the session rate for cases of temporary load), then the call is rejected. The session rate and burst rate are configured in security profile.

§ **Active Limit.** Number of rejected sessions. The calls are rejected when the number of active calls exceeds the maximum active sessions (configured in security profile).


§ **Outgoing Limit.** Number of rejected outgoing sessions. The incoming calls are rejected when the number of outgoing sessions exceeds the maximum incoming sessions (configured in security profile).

§ **Overload.** Number of rejected sessions due to overload (i.e. CPU overload...).

§ **Bandwidth Limit.** Total number of rejected calls due to full use of the bandwidth, allocated for this interface (configured in media profile).

§ **Usage (mbps).** Bandwidth utilization in MB/sec.

§ **Relative Usage.** The bandwidth utilization based on the configured total bandwidth.

1. Click on the **Export** icon  to export the display data to a CSV file.
2. Click on **Chart** to see the graphic presentation of the statistics.

3.5 Peer Statistics

3.5.1 Summary

1. Select **Diagnostics** à **Peer Statistics** à **Summary**.
2. The **Peer Statistics Summary** window opens.

3.

1. Select the following criteria for filtering:

§ **Hourly**. Set to select an hourly interval for the CPU usage report.

§ **Five Minutes**. Set to select a 5-minute interval for the CPU usage report.

§ **Time Range**. Select the start date/time and end date/time of the report period.

1. Click the **Filter** button, and the following appears.

§ **Peer Name**. The name of the peer.

§ **Time**. The start time of the calculations.

§ **Attempted**. Total number of attempted sessions per the specified peer.

§ **Answered**. Number of sessions answered.

§ **With Media**. The total number of sessions which their media traverses the BorderNet SBC.

§ **Emergency**. Number of emergency sessions.


§ **Total SIP-I Calls**. The total number of SIP-I sessions.

§ **Transcoded**. The total number of transcoded sessions.

§ **ASR (%)**. The Answer Seizure Rate ((answered calls #/call attempts #)/100)

§ **ACD (sec)**. The Average Call Duration in seconds.

§ **R-Factor**. Based on delay, and packet loss parameters, the quality of the voice is calculated, and presented as R-Factor in range [0-5], where the highest value presents the highest quality.

1. Click on the **Export** icon  to export the display data to a CSV file.

2. Click on **Chart** to see the graphic presentation of the statistics.

3.5.2 Packet Statistics

1. Select **Diagnostics** à **Peer Statistics** à **Packet Statistics**.
2. The **Peer Packet Statistics** window opens.

Peer Name	Time	Signaling			Media Packets							
		Received Packets	Dropped Packets(R)	Dropped Messages	Received	Lost	Round Trip Time	Jitter	Dropped/Rate Exce	Dropped/Invalid So	Dropped/Unreachal	
Spect2-30-28	2016-07-27 15:00	23206	0	0	0	0	0	0	0	0	0	0
Spect2-30-40	2016-07-27 15:00	23207	0	0	0	0	0	0	0	0	0	0
Spect2-30-41	2016-07-27 15:00	23901	0	0	0	0	0	0	0	0	0	0
Spect2-40-28	2016-07-27 15:00	34906	0	0	0	0	0	0	0	0	0	0

- 3.
4. Select the following criteria for filtering:

§ **Hourly**. Set to select an hourly interval for the CPU usage report.

§ **Five Minutes**. Set to select a 5-minute interval for the CPU usage report.

§ **Time Range**. Select the start date/time and end date/time of the report period.

Filter

Hourly
 Five Minutes

Time Range

From: 2016-07-27 [Calendar Icon] Time(##Q4 M:SS) 00:00:00

To: 2016-07-27 [Calendar Icon] Time(##Q4 M:SS) 23:59:59

Filter

1. Click the **Filter** button to display the signaling and media packets' statistics reports:

§ **Peer Name**. The name of the peer.

§ **Time**. The start time of the calculations.

§ **Received Packets**. The total number of the received signaling packets.

§ **Dropped Packets**. The total number of the dropped signaling packets.

§ **Dropped Messages**. The total number of the dropped messages.

§ **Received**. The total number of the received media packets.

§ **Lost**. The total number of the lost media packets.


§ **Round Trip Time**. RTT is calculated based on the RTCP packets, by measuring the delay between the packet's sending and receiving times minus the delay experienced in the remote side. This is calculated only on the Rx, and per peer (calculated in milliseconds).

§ **Jitter**. Jitter is calculated based on a function described in RFC 3550, using the RTP stream's timestamps (calculated in milliseconds).

§ **Dropped Rate Exceeded**. Number of dropped packets that exceeded the bandwidth limit.

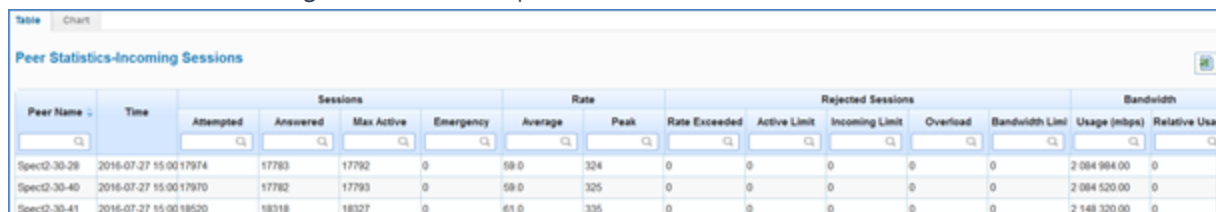
§ **Dropped Invalid Source**. Number of dropped packets with invalid source (at the receive side).

§ **Dropped Unreachable**. Number of dropped packets that could not be transmitted.

1. Click on the **Export** icon  to export the display data to a CSV file.
2. Click on **Chart** to see the graphic presentation of the statistics.

3.5.3 Incoming Sessions

1. Select **Diagnostics** à **Peer Statistics** à **Incoming Sessions**.
2. The **Peer Statistics - Incoming Sessions** window opens.



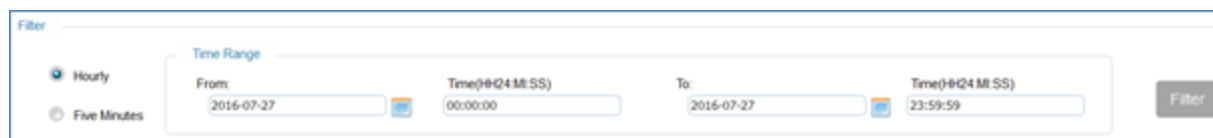
Peer Name	Time	Sessions				Rate			Rejected Sessions			Bandwidth	
		Attempted	Answered	Max Active	Emergency	Average	Peak	Rate Exceeded	Active Limit	Incoming Limit	Overload	Bandwidth Limit	Usage (mbps)
Spect2-30-28	2016-07-27 15:00:17974	17783	17792	0	59.0	324	0	0	0	0	0	2 084 984.00	0
Spect2-30-40	2016-07-27 15:00:17970	17782	17793	0	59.0	325	0	0	0	0	0	2 084 520.00	0
Spect2-30-41	2016-07-27 15:00:18520	18318	18327	0	61.0	335	0	0	0	0	0	2 148 320.00	0

3. Select the following criteria for filtering:

§ **Hourly**. Set to select an hourly interval for the CPU usage report.

§ **Five Minutes**. Set to select a 5-minute interval for the CPU usage report.

§ **Time Range**. Select the start date/time and end date/time of the report period.



Filter

Hourly
 Five Minutes

Time Range

From: 2016-07-27 00:00:00 To: 2016-07-27 23:59:59

Filter

1. Click the **Filter** button to display the incoming packets' statistics reports:

§ **Peer Name**. The name of the peer.

§ **Time**. The start time of the calculations.

§ **Attempted**. The total number of the incoming session attempts.

§ **Answered**. The total number of the incoming sessions answered.

§ **Max Active**. The total number of outgoing active calls.

§ **Emergency**. The maximum number of incoming emergency sessions.

§ **Average**. The average rate of the incoming sessions.

§ **Peak**. Number of incoming peak session rate.

§ **Rate Exceeded**. Number of incoming rejected sessions. If the current rate (session per second), exceeds the session rate and the burst rate (the percentage allowed to pass the session rate for cases of temporary load), then the call is rejected. The session rate and burst rate are configured in security profile.

§ **Active Limit.** Number of rejected sessions. The calls are rejected when the number of active calls exceeds the maximum active sessions (configured in security profile).


§ **Incoming Limit.** Number of rejected incoming sessions. The incoming calls are rejected when the number of incoming sessions exceeds the maximum incoming sessions (configured in security profile).

§ **Overload.** Number of rejected sessions due to overload (i.e. CPU overload...).

§ **Bandwidth Limit.** Total number of rejected calls due to full use of the bandwidth, allocated for this interface (configured in media profile).

§ **Usage (mbps).** Bandwidth utilization in MB/sec.

§ **Relative Usage.** The bandwidth utilization based on the configured total bandwidth.

1. Click on the **Export** icon  to export the display data to a CSV file.
2. Click on **Chart** to see the graphic presentation of the statistics.

3.5.4 Outgoing Sessions

1. Select **Diagnostics** à **Peer Statistics** à **Outgoing Sessions**.
2. The **Peer Statistics - Outgoing Sessions** window opens.



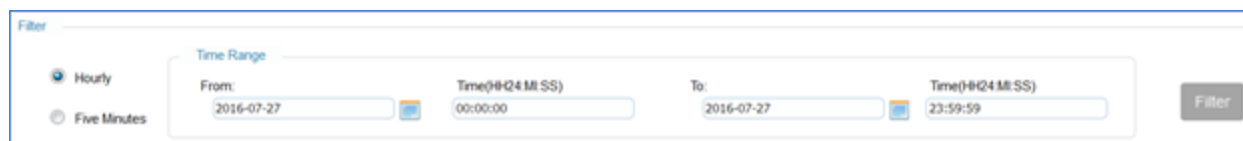
Peer Name	Time	Sessions				Rate			Rejected Sessions			Bandwidth	
		Attempted	Answered	Max Active	Emergency	Average	Peak	Rate Exceeded	Active Limit	Outgoing Limit	Overload	Bandwidth Limit	Usage (mbps)
Spec12-30-28	2016-07-31 11:00:00	0	0	0	0	0.0	0	0	0	0	0	2 853 745.00	0
Spec12-30-40	2016-07-31 11:00:00	0	0	0	0	0.0	0	0	0	0	0	2 859 458.00	0
Spec12-30-41	2016-07-31 11:00:00	0	0	0	0	0.0	0	0	0	0	0	2 948 488.00	0
Spec12-40-28	2016-07-31 11:00:318600	314872	29268	0	0	265.25	1500	0	0	0	0	3 395 088.00	0

3. Select the following criteria for filtering:

§ **Hourly.** Set to select an hourly interval for the CPU usage report.

§ **Five Minutes.** Set to select a 5-minute interval for the CPU usage report.

§ **Time Range.** Select the start date/time and end date/time of the report period.



Filter

Hourly
 Five Minutes

Time Range

From: 2016-07-27 00:00:00 To: 2016-07-27 23:59:59

Filter

1. Click the **Filter** button to display the outgoing packets' statistics reports:

§ **Peer Name.** The name of the peer.

§ **Time.** The start time of the calculations.

§ **Attempted.** The total number of the outgoing session attempts.

§ **Answered.** The total number of the outgoing sessions answered.

§ **Max Active.** The total number of outgoing active calls.

§ **Emergency.** The maximum number of outgoing emergency sessions.

§ **Average.** The average rate of the outgoing sessions.

§ **Peak.** Number of outgoing peak session rate.

§ **Rate Exceeded.** Number of outgoing rejected sessions. If the current rate (session per second), exceeds the session rate and the burst rate (the percentage allowed to pass the session rate for cases of temporary load), then the call is rejected. The session rate and burst rate are configured in security profile.


§ **Active Limit.** Number of rejected sessions. The calls are rejected when the number of active calls exceeds the maximum active sessions (configured in security profile).

§ **Outgoing Limit.** Number of rejected outgoing sessions. The incoming calls are rejected when the number of outgoing sessions exceeds the maximum incoming sessions (configured in security profile).

§ **Overload.** Number of rejected sessions due to overload (i.e. CPU overload...).

§ **Bandwidth Limit.** Total number of rejected calls due to full use of the bandwidth, allocated for this interface (configured in media profile). Usage (mbps). Bandwidth utilization in MB/sec.

§ **Relative Usage.** The bandwidth utilization based on the configured total bandwidth.

1. Click on the **Export** icon  to export the display data to a CSV file.
2. Click on **Chart** to see the graphic presentation of the statistics.

4. Trace

BorderNet SBC supports **Wireshark** remote tracing, enhancing the remote trace functionality of Wireshark with a custom **wpcap.dll**.

The custom plug-in supports additional message-based filters along with the existing IP level filters. All messages that match the filter are streamed to Wireshark client in **pcap** format.

Note:

The Wireshark application is not included with the BorderNet SBC. See the link on the screen below to download the application from wireshark.org. Once you have downloaded Wireshark and installed it, you can download the plug-in also from the screen below.

Wireshark uses remote tracing to capture the trace messages. You can also store the messages. By default, the BorderNet SBC streams to the Wireshark client. The custom plug-in allows profile-based traces and interface traces.

4.1 Downloading the Trace Plug-in

→ To download the Trace Plug-in:

1. From the **Diagnostics** menu, under the **Trace** section, select **Plugin**.
2. Follow the instructions from the screen below.

Download Page for BorderNet 4000 Trace

This page will allow you to download and install BorderNet 4000 Trace plug-in. BorderNet 4000 allows tracing using Wireshark, a popular network protocol analyzer. You need to download Wireshark from [here](#) and install it on your client platform before downloading and installing this plug-in. Minimum version of Wireshark must be 1.6.

System Requirements:
Wireshark plug-in supports the following configurations:

Platform	Wireshark version
Windows 98 / NT / 2000 / XP / 2003	1.6 or higher
Windows 7*	1.6 or higher (32-bit version)

Steps to download and install Wireshark plug-in

- Click on the download link below and save the file wpcap.dll to your local files system.

When download finishes, copy wpcap.dll to c:\windows\system32 directory
For Windows 7 (64 bit), copy wpcap.dll to c:\windows\system32\win64 directory.
If the file already exists, overwrite it with downloaded file.

[Download Plug-in](#)

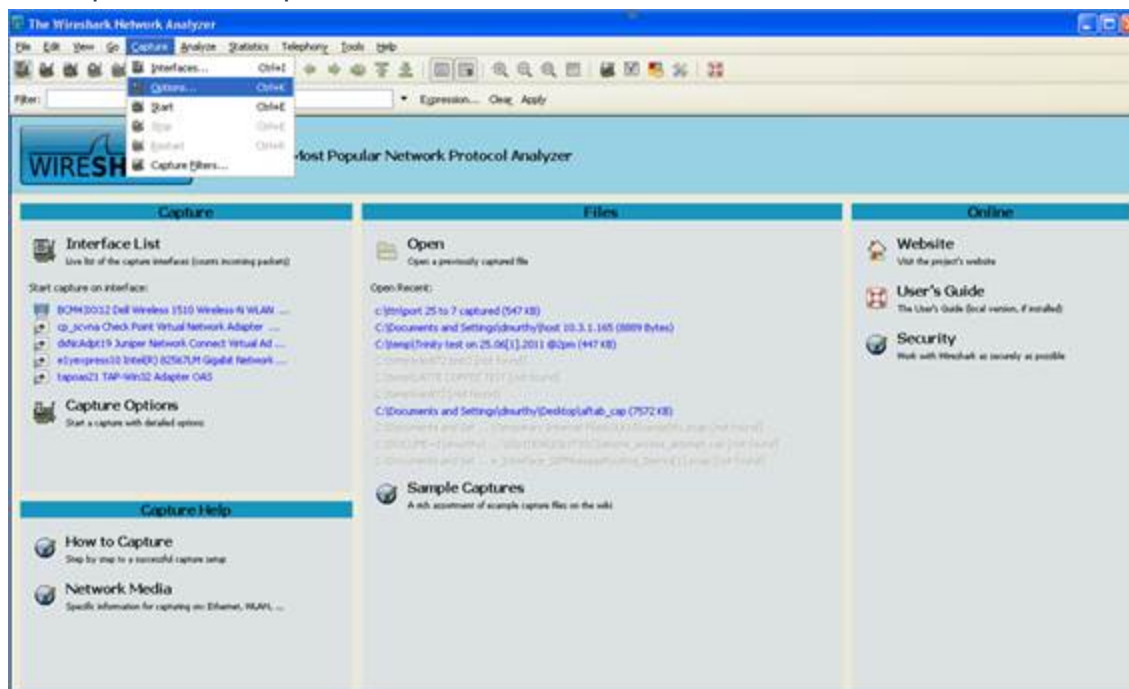
Caution:

If you have previously downloaded another plug-in named wpcap.dll for a different device, do not overwrite it. Rename it before downloading this wpcap.dll.

4.2 Connecting to the BorderNet SBC from Wireshark

→ To connect to the BorderNet SBC from Wireshark:

1. Select **Options** from the **Capture** menu.



2. The **Capture Options** window opens.



3. Select **Remote** from the **Interface** drop down box.
4. Enter the management IP address of the BorderNet SBC system for the **Host**.
5. The port number for the **Port** is 2010.

Note:

The host IP address from which the trace request is triggered must be entered in the ACL without which the trace requests coming into the BorderNet SBC will be dropped. This is a security feature. Also, remote tracing as a service should be enabled on the BorderNet SBC. See the *BorderNet SBC Provisioning Guide* for instructions on how to create ACL entries.

1. Select **Password** authentication.
2. Enter the **Username** and **Password**.

3. The user must have the "tracing role" assigned. Without it, the trace requests cannot be initiated. See the *BorderNet SBC Provisioning Guide*.
4. Click **OK**.
5. If the connection is successful, the system shows the following capture options including session interfaces and recording profiles:
6. Session Interface:

§ **SessionIf1**

§ **SessionIf2**

§ **SessionIf3**

§ **SessionIf4**

1. Recording Profiles:

§ **SignalingNoMedia**

§ **SignalingWithMedia**

§ **MediaDropped**

§ **FlowsDropped**

1. To start a trace request choose from one of the options above.
2. Based on the option selected you can either enter an interface level capture filter or a message level capture filter to narrow down the trace criteria.
3. The list below gives the valid combinations of options and filter criteria that are supported.

Option	Description
SessionIf1 - SessionIf4	All IP based capture filters are supported. These are default Wireshark capture filters. For example, IP, host, port, TCP, UDP ... A combination of these filters are also supported using the logical operators 'and', 'or' and 'not'
SignalingWithMedia	Message-based capture filters. For example, CallingPartyUserPart , CalledPartyDomainName , IncomingInterface , IncomingPeer . Multiple Call trace criteria can be combined using a logical operator 'and.'
SignalingNoMedia	Message-based capture filters. For example, CallingPartyUserPart , CalledPartyDomainName , IncomingInterface , IncomingPeer . Multiple Call trace criteria can be combined using a logical operator 'and.'
MeidaDropped, FlowsDropped	No Filter required. All the dropped packets are captured even if a filter is specified.

Table 2: Filter Criteria

4.3 Recording Profiles

Recording profiles help to trace sessions based on message-specific filter criteria. Each profile has a specific type of message to trace.

- **SignalingNoMedia.** Traces all the signaling messages that match the message specific capture filter.
- **SignalingWithMedia.** Traces all the signaling messages and RTP (media) that match the message specific capture filter.
- **MediaDropped.** Traces all the media packets that are dropped in the kernel. It does not require a filter.
- **MediaDropped.** Traces all the non-media packets that are dropped in the kernel. It does not require a filter.

4.4 Message Based Capture Filters

The custom Wireshark plug-in supports message-based capture filters. The following message-based capture filters are supported.

- **CallingPartyUserPart**
- **CallingPartyDomain**
- **CallingPartyURIScheme**
- **CallingPartyNumber**
- **CalledPartyUserPart**
- **CalledPartyDomain**
- **CalledPartyURIScheme**
- **DialedNumber**
- **IncomingInterface**
- **IncomingPeer**

Three operators are supported for matching the filters:

- **BeginsWith** - for example, `CalledPartyUserPart=408%`. This filter will trace all the sessions whose `CalledPartyUserPart` begins with 408.
- **EndsWith** - for example, `CalledPartyUserPart=%9000`. This filter will trace all the sessions whose `CalledPartyUserPart` ends with 900.
- **IsEqualTo** - for example, `CalledPartyUserPart=4087509000`. This filter will trace all the sessions whose `CalledPartyUserPart` equals 4087509000.

The operators can be used with all the message-based capture filters. To narrow down the traces further, any capture filters can be combined using a logical 'and' operation. For example, `CalledPartyUserPart=408%` and `IncomingInterface=SIPIntf1`. This will capture all the messages that arrive on SIPInterface SIPIntf1 and whose `CalledPartyUserPart` begins with 408.

Note:

Message-Based Capture filters are case sensitive. The filter should exactly match the specified syntax with case.

4.5 Interface Based Capture Filters

Interface based capture filters are used with the session options. Though Wireshark supports several interface based capture filters, only the following capture filters are qualified with the BorderNet SBC:

- IP
- TCP
- UDP
- Host
- Port
- Arp

The remaining Wireshark filters can be used to narrow down the traces. The operators and logical operations follow the Wireshark syntax.

Note:

Tracing may not capture all the packets when the traffic is too high on the interface or when the system is processing a high amount of traffic. It recommends to use specific capture filters (instead of display filters which are applied on the captured messages) to narrow down the packet traffic of interest.

4.6 Session Tracing

The current sessions, connected from Wireshark (Trace Sessions) can be displayed. The following data is displayed:

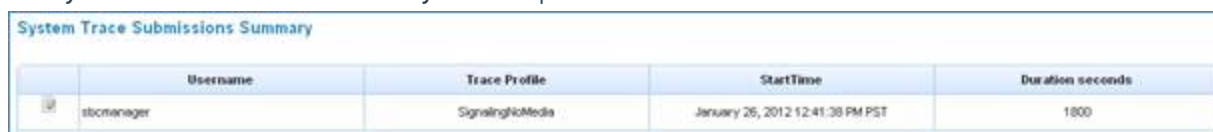
- Wireshark trace requests in progress
- Trace Profile used for tracing
- Start time of the trace

For session traces, the **Trace Profile** shows the Interface and for recording profiles the trace profile shows the actual profile used. You can stop each of these traces from the Web GUI.

- Click the **Edit** button to see the options to stop the trace.
- Double-click on the entry to show a detailed view of the trace request.

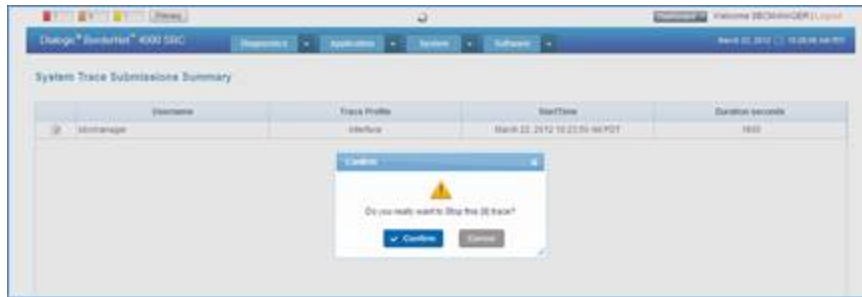
→ To activate a session trace:

1. From the **Diagnostics** menu, select **Sessions under Trace**.
2. The **System Trace Submissions Summary** window opens.



Username	Trace Profile	StartTime	Duration seconds
stcmanager	SignalingMedia	January 26, 2012 12:41:38 PM PST	1800

3. To stop the session trace, select **Stop** from the edit button.
4. Click **Confirm**.



5.

4.7 Media Capture

BorderNet SBC supports media capture and recording from any connection point on the network. The GUI displays basic RTP stream characteristics, and multiple media streams can be selected and played back at any given time (see [Connecting to the BorderNet SBC from Wireshark](#)).

4.8 SIP Capture

BorderNet SBC can be provisioned to record all the system's incoming and outgoing SIP messages. The SIP messages are recorded in **pcap** format (a format that is used in the Wireshark application) to assure the offline opening of the Wireshark files, saved in **.pcap.gz** format.

If this capability is enabled and the system is in an overload state, the open files are closed and the SIP message recording temporarily stops. It is resumed when this state is cleared.

Note:

This capability is available to *System_Admin* role.

→ To provision the SIP Capture capability:

1. Select **Diagnostics** → **SIP Capture**.
2. The **SIP Capture Configuration** window opens:

The 'SIP Capture Configuration' dialog box has the following elements:

- Enable:** A checkbox that is checked.
- Warning:** A red text message: "System performance degradation of up to 10% is expected!"
- Parameters:** A section with two input fields:
 - File creation interval [1 to 30 minutes]:** The value is 10.
 - File maximum size [10 to 100 MB]:** The value is 15.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

3. Enter the following parameters:

4. **Enable.** If checked, this capability is enabled, enabling the user to provision the following two additional parameters.
5. **File creation interval** [1 to 30 minutes]. The file duration in minutes (the file starts recording and is closed at this specified time duration) - default: 10 minutes.
6. **File maximum size** [10 to 100 MB]. The file-size limit (the file starts recording and is closed when the size of the file reaches the specified size) - default: 15MB.
7. Select **Save** to keep the entered values.

5. Dashboard

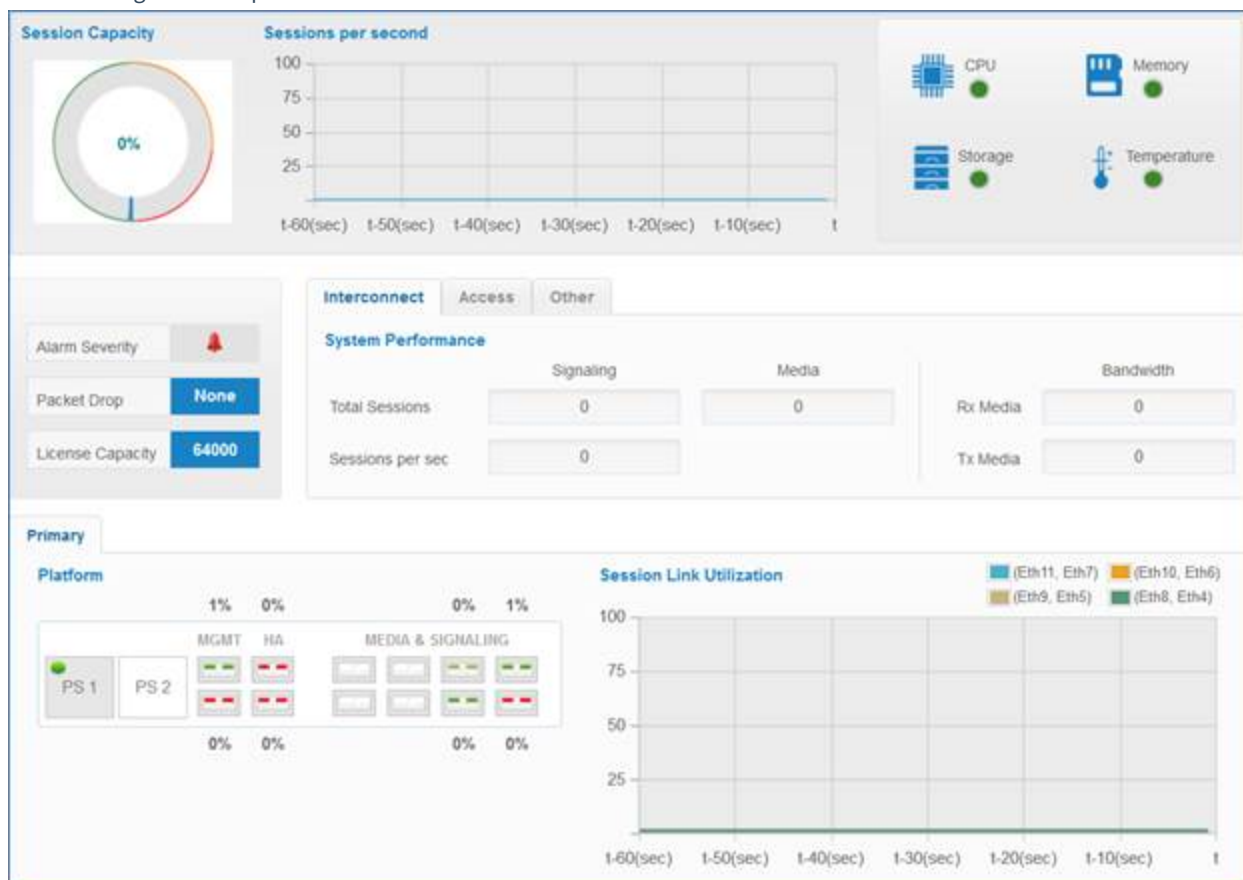
The dashboard provides real-time information on how BorderNet SBC is functioning including the platform status and system performance.

→ To display the dashboard information:

1. Click the **Dashboard** button from the Web GUI.



2. The following window opens:

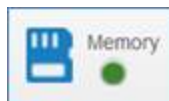


3. **Session Capacity.** Displays the percentage of the total number of ongoing sessions per the maximum number of allowed sessions in the system.
4. **Sessions per second.** The session's percentage (in a graph), displayed every 100 milliseconds.
5. **CPU.** Displays the last 60 seconds of the CPU's activity and bandwidth.
6. To view this value, point on the circle: [green: normal, orange: warning, red: critical]



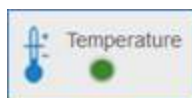
7. **Memory.** Displays the percentage of the total memory allocated to the application. Memory is statically allocated in BorderNet SBC which means that application memory consumption does not increase drastically as an increasing number of calls flow through the BorderNet SBC. Similarly, there is memory allocation even when the system is not experiencing any traffic flow. When utilization goes beyond 90% or if the utilization is varying in real time, then the operator needs to run other diagnostics to find out the cause.

8. To view this value, point on the circle: [green: normal, orange: warning, red: critical]



9. **Temperature.** Shows the system's temperature (in Centigrade and Fahrenheit).

10. To view these values, point on the circle: [green: normal, orange: warning, red: critical]



11. **Storage.** Indicates the disk space usage.

12. To view this value, point on the circle: [green: normal, orange: warning, (above 70%), red: critical (above 85%)]



13. **Alarm Severity.** Indicates the highest level of alarm found in the system. For example, if there are zero outstanding critical alarms (red), two major alarms (orange) and five minor alarms (yellow), then the dashboard will show an orange alert.

14. **Packet Drop.** Indicates the level of discarded Ethernet packets in the system. It has the following three levels.

§ **None** - 0-10 percent packets being dropped

§ **Low** - 10-25 percent packets being dropped

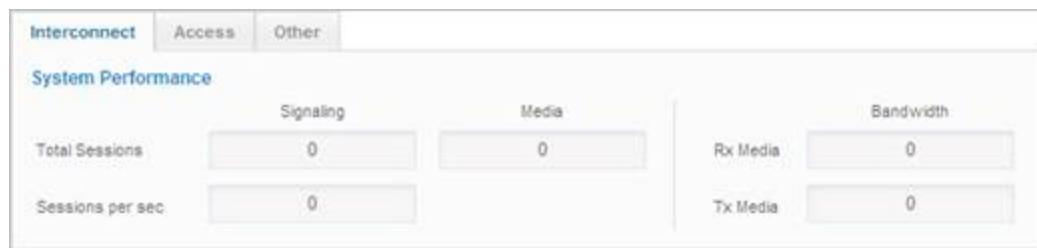
§ **High** - greater than 25 percent being dropped

- **License Capacity.** Indicates the number of sessions licensed. When the number of concurrent sessions in the system exceeds 80% of license capacity, this number turns to orange. When the threshold increases beyond 90%, the License Capacity turns red.



- **System Performance.** The system reports the real-time performance information for the active platform at the following levels:

§ **Interconnect.** Signaling, media, and bandwidth information, of the interconnect traffic:



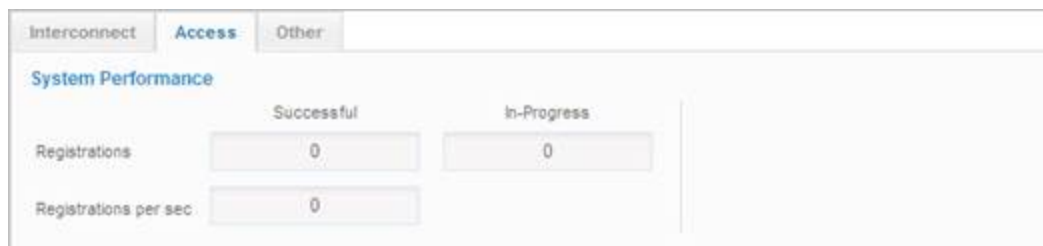
Total Sessions Signaling represents the count of all attempted calls.

Total Sessions Media represents all answered calls for which the BorderNet SBC does media interception.

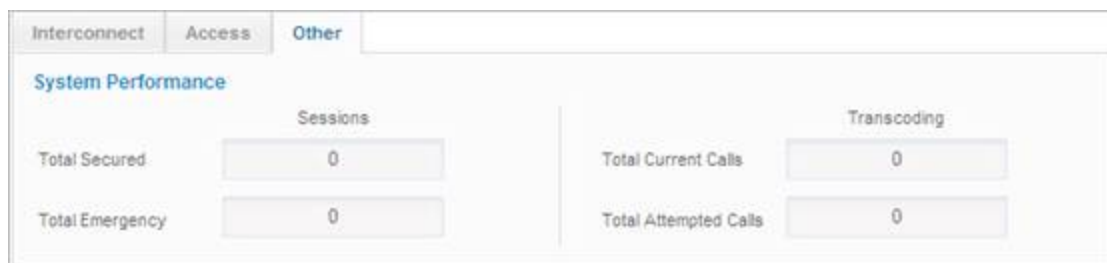
Sessions/sec is the number of new incoming session attempts per second across all session interfaces.

Media Bandwidth (in Mbps) indicates system level media bandwidth utilization (transmit and receive) across all session interfaces. For example, on a system with 4 GigE interfaces in Full Duplex mode, Rx and Tx can each show values closer to 4096 Mbps. However, signaling packets and other dropped packets are not considered for this usage representation. As stated, it is representative of RTP stream only.

§ **Access.** The number of successful registrations, the number of registrations in progress on the system, and the number of registrations per second processed by the BorderNet SBC.



§ **Other.** The number of secured sessions, total number of emergency sessions, and the total concurrent and attempted transcoding calls.



- **Platform Status.** The real-time platform status information for the active platform, as shown in the table below (this section is available only for appliance configuration based on HP DL360/DL380 servers):

Note:

You can toggle the view between the Active and Secondary platforms.

The color coding for the LEDs is as follows:

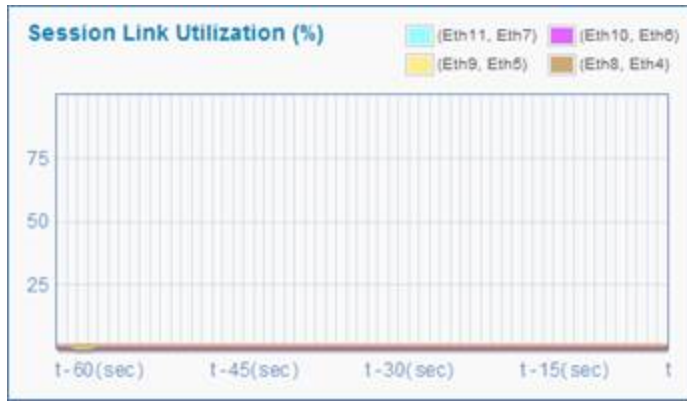
- **Red** - Down
- **Gray** - Not configured or disabled
- **Green** - Up or active

Component	Supported Status
Management, High Availability, and Media and Signaling Links .	Dark green: Active Pale Green: Standby Red: Down Gray: Not Configured
Power Supplies .	Green: Functional Red: Non-functional or down White: Not installed

Table 3: Components and Supported Status

- **Session Link Utilization.** The Session Link Utilization percentage provides a graphical representation of all four session interfaces in the system. It captures utilization every second and graphs it over a 1 minute time interval. If a session link is set

to 1 Gbps and if it carries traffic of 500 Mbps, the utilization is represented as 50%.



6. System Status

This section covers the e System Status information for the active platform.

6.1 ACL Status

Access Control Lists (ACLs) selectively allow or deny traffic from specified remote entities.

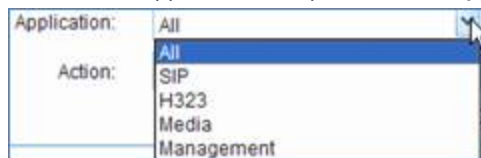
You can create a set of static filtering rules to accept or block traffic, and BorderNet SBC creates service specific ACLs based on other configurations. These service-aware ACLs enable fine-grain control over BorderNet SBC traffic and prevent DoS attacks from random sources.

→ To report the security Access Control List (ACL) Status summary:

1. Select **Diagnostics** à **System Status** à **ACL Status**.
2. The **Security ACL Status Filter** window opens.



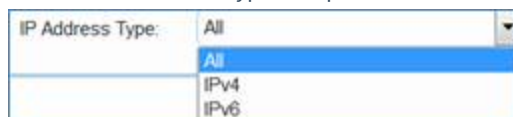
3. Select which application to report from the **Application** dropdown list.



4. Select the type of ACL to report from the **Action** dropdown list:
5. All ACLs
6. Drop ACLs
7. Accept ACLs



8. Select the IP Address type to report from the **IP Address Type** dropdown list:



9. Click **OK**.

1. The **Security Access Control List Status Summary** window opens.

Security Access Control List Status Summary									
Application	Action	Configured By	IP Address Type	Local IP	Local Port	Transport	Remote IP	Remote Netmasl	Remote Port
Management	Accept	User	IPv4	192.168.57.57	443	TCP	0.0.0.0	0	0
Management	Accept	User	IPv4	192.168.57.57	80	TCP	0.0.0.0	0	0
Management	Accept	User	IPv4	192.168.57.57	2010	TCP	0.0.0.0	0	0
Management	Accept	User	IPv4	192.168.57.55	21	TCP	0.0.0.0	0	0
Management	Accept	User	IPv4	192.168.57.55	22	TCP	0.0.0.0	0	0
Management	Accept	System	IPv4	192.168.57.57	443	TCP	192.168.57.0	24	0
Management	Accept	System	IPv4	192.168.57.57	80	TCP	192.168.57.0	24	0
Management	Accept	System	IPv4	192.168.57.57	22	TCP	192.168.57.0	24	0
Management	Accept	System	IPv4	192.168.57.57	500	UDP	192.168.57.0	24	0
Management	Accept	System	IPv4	192.168.57.55	22	TCP	192.168.57.0	24	0
Management	Accept	System	IPv4	192.168.57.55	500	UDP	192.168.57.0	24	0
SIP	Accept	System	IPv4	192.168.58.56	5060	UDP	192.168.58.0	24	0
SIP	Accept	System	IPv4	192.168.58.55	5060	UDP	192.168.58.0	24	0

6.2 DNS Cache

To reduce the number of DNS queries to external DNS servers, BorderNet maintains a DNS cache of the **Resource Records (RRs)** list (periodically removed based on TTL expiry).

BorderNet first tries to resolve the domain name's address, by querying the DNS cache. Upon a negative response from the cache, the query is sent to provisioned DNS servers. The returned result and the associated TTL are recorded in the cache, for future use.

The **DNS Cache** window enables the user to view and refresh the list of the cached DNS, clean the cache, and export the information to a CSV file.


→ To view and refresh the list of the cached DNS:

1. Select **Diagnostics à System Status à DNS Cache**.
2. The **DNS Cache Records** window opens, presenting the cached-DNS list, and the parameters of each entry.

3. **TTL**. Time to Live (TTL) is the time interval (seconds), in which the record in the cache is relevant. Upon the expiration of this value the record is deleted
4. **Resource Record Type**. Resource Record (RR) displays the network's entity name that is returned by the DNS. The table below lists the RR types' possible values:

Type	Description	Function
A	Address record	DNS returns a 32-bit IPv4 address.
AAAA	IPv6 Address record	DNS returns a 128-bit IPv6 address
CNAME	Canonical name record	Another Alias is returned: DNS retries a lookup with the new name.

Type	Description	Function
NAPTR	Naming Authority Pointer	Regular-expression-based rewriting of domain names which can be used as URIs .
SRV	Service locator	Generalized service location record, used for newer protocols instead of creating protocol-specific records such as MX.
URI	Uniform Resource Identifier	Can be used for publishing mappings from hostnames to URIs.

- **Host.** Host's name and address, where the content depends on the RR type. For example, for the Name=sbc1.green.dialogic.com, if RR=A, then the Address is an IPv4 address. If RR=AAAA, then the Address is an IPv6 address.
- **NAPTR** (Name Authority Pointer DNS RR type, widely used for SIP) parameters.
- **SRV** (Service Record, DNS RR type) parameters
- **CNAME** parameters
- To clear the DNS cache, press the **Clear DNS cache** button, and confirm the operation.
- To refresh the screen, press the **Refresh screen** button.
- To export the information to a CSV file, click on the **Export** icon .

6.3 Registration Cache

The **Registration Cache** window enables the user to view and refresh the list of the cached IDs, clean the cache, and export the information to a CSV file.

→ To view and refresh the list of the cached Registration Cache data:

1. Select **Diagnostics à System Status à Registration Cache**.
2. Edit the fields.
3. The **Registration Cache Data** window opens, presenting the data of successful call registrations.

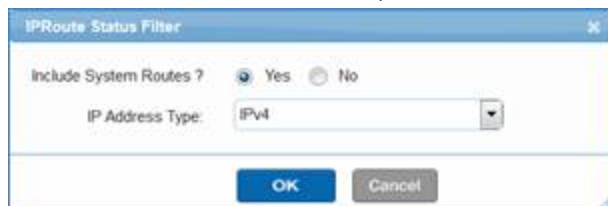


Registration Cache ID	To Header	Contact Header	Expires (secs)	Bulk Registration	Incoming Peer ID	IMPI	IMPU	Outgoing Peer ID	P Charging vector	Call ID

4. **Registration Cache ID** - ID number.
5. **To Header** - Presents the 'to header' of the subscriber.
6. **Contact Header** - Presents the header including the IP address.
7. **Expires (secs)** - Expiration time, usually 60 secs.
8. **Bulk Registration** - Registration including several individual registrations in a bulk package.
9. **Incoming Peer ID** - ID of the incoming subscriber.
10. **IMPI** - IMS Private User Identity - the means by which a subscriber of an IMS service is identified by other users of the service.
11. **IMPU** - IMS Public User Identity - the means by which a subscriber of an IMS service is identified by other users of the service.
12. **Outgoing Peer ID** - ID of the outgoing subscriber.
13. **P Charging Vector** - Charging data relating to the registration.
14. **Call ID** - ID of last call which was made.

6.4 IP Route Status

1. From the **Diagnostics** menu, under **System Status**, select **IP Route Status**.
2. The **IP Route Status Filter** window opens.



3. Select whether to report system routes or not by selecting **Yes/No** in the **Include System Routes?** field.

§ Routes that are automatically added by the system (for example, when VLAN Access IP addresses are configured on the system) are referred to as **system-added routes**. This option allows you to see the routing table entries existing in the system.

§ Routes that are explicitly provisioned by the operator are referred to as **non-system routes**.

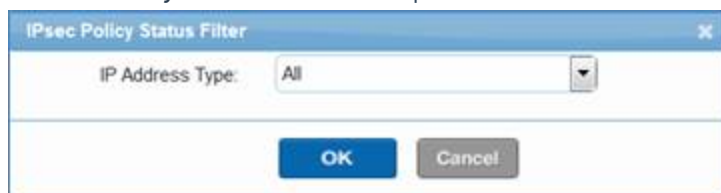
1. Select the **IP Address Type**.
2. Possible Values: **IPv4, IPv6**.
3. Click **OK**.
4. The **IP Route Status Summary** window opens.

IP Route Status Summary						
Destination IP Address	Subnet Mask	Gateway IP Address	TOS	Metric	Interface	
192.168.55.0	24			0.0	eth1	
192.168.58.0	24			0.0	eth2	
192.168.58.0	24			0.0	eth3	
192.168.57.0	24			0.0	eth0	
default	0	192.168.57.250		0.0	eth0	

6.5 IPsec Policy Status

→ To view the IPsec Policy Status summary:

1. Select **Diagnostics** à **System Status** à **IPsec Policy Status**.
2. The **IPsec Policy Status Filter** window opens.



- 3.
4. Select the **IP Address Type** as the filter criteria.
5. Possible values: **All, IPv4, IPv6**.
6. Click **OK**.

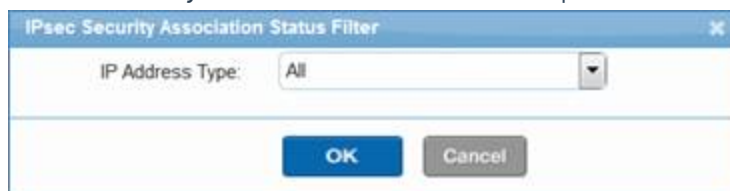
7. The following information is displayed:

IPsec Policy Status Summary							
IP Address Type	Local IP	Local Port	Remote IP	Remote Port	Transport	Mode	Protocol
<input type="text"/>	<input type="text"/>		<input type="text"/>				

6.6 IPsec Security Association Status

→ To view the IPsec Security Associations summary:

1. Select **Diagnostics** à **System Status** à **IPsec Security Association Status**.
2. The **IPsec Security Association Status Filter** window opens.



The dialog box titled "IPsec Security Association Status Filter" has a close button (X) in the top right corner. It contains a label "IP Address Type:" followed by a dropdown menu currently set to "All". At the bottom, there are two buttons: "OK" and "Cancel".

- 3.
4. Select the **IP Address Type** as the filter criteria.
5. Possible values: **All**, **IPv4**, **IPv6**.
6. Click **OK**.
7. The following information is displayed:

IPsec Security Association Status Summary								
IP Address Type	Local IP	Local Port	Remote IP	Remote Port	Status	Transport	Mode	Protocol
<input type="text"/>	<input type="text"/>		<input type="text"/>					

6.7 Black List Entries

→ To view the Black List Entries:

1. Select **Diagnostics** à **System Status** à **Black List Entries**.
2. The **Black List Entries Filter** window opens.



The dialog box titled "Black List Entries Filter" has a close button (X) in the top right corner. It contains a label "IP Address Type:" followed by a dropdown menu currently set to "All". At the bottom, there are two buttons: "OK" and "Cancel".

- 3.
4. Select the **IP Address Type** as the filter criteria.
5. Possible values: **All**, **IPv4**, **IPv6**.
6. Click **OK**.

7. The following information is displayed:

Black List Entries Summary					
Application	Local IP	Local Port	Transport	Remote IP	Remote Port

7. Analytic Configuration

Elasticsearch Logstash Kibana (ELK) is an industry analytic infrastructure tool, which collects raw data (**Logstash**) and sends it to a central database (**Elasticsearch**). The central server (**Kibana**) calculates, and presents a comprehensive graphic presentation for all kinds of resources and data.

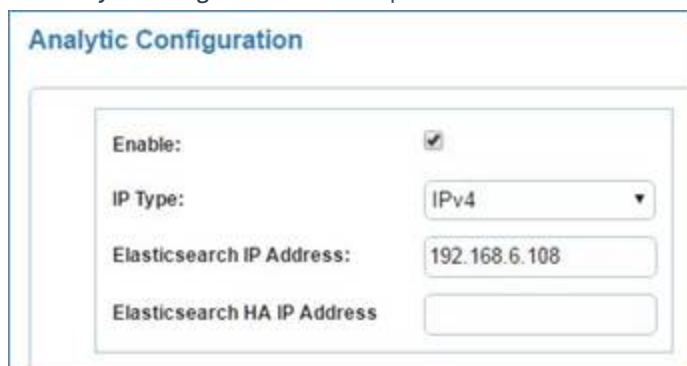
The Analytic solution has been integrated in the BorderNet, when Logstash (client- installed on the BorderNet), retrieves the performance and SDR information from the BorderNet, and forwards it to a centralized, and separate Analytic server.

The collected performance information includes:

- CPU per process/core/system
- Memory per process/system
- Network per interface/system (Incoming/Outgoing)

→ To set the analytic information:

1. Select **Diagnostics à Analytic Configuration**.
2. The **Analytic Configuration** window opens.



The screenshot shows a configuration window titled "Analytic Configuration". It contains the following fields:

- Enable:** A checkbox that is checked.
- IP Type:** A dropdown menu with "IPv4" selected.
- Elasticsearch IP Address:** A text input field containing "192.168.6.108".
- Elasticsearch HA IP Address:** An empty text input field.

3. Enter the following information:
4. **Enable.** If checked, the Analytic capability is enabled.
5. **IP Type.** Select IPv4/IPv6 from the dropdown list.
6. **Elasticsearch IP Address.** The IP address of the Analytic server (mandatory), used to enter to the Analytic platform.
7. **Elasticsearch HA IP Address.** The IP address of the standby Analytic server (optional).
8. Click **Save**.

For more information on this capability, and for installation details, see *Analytic Platform User's Manual*, and *Analytic Installation Guide*.

8. Software Management

This section explains how to perform the following:

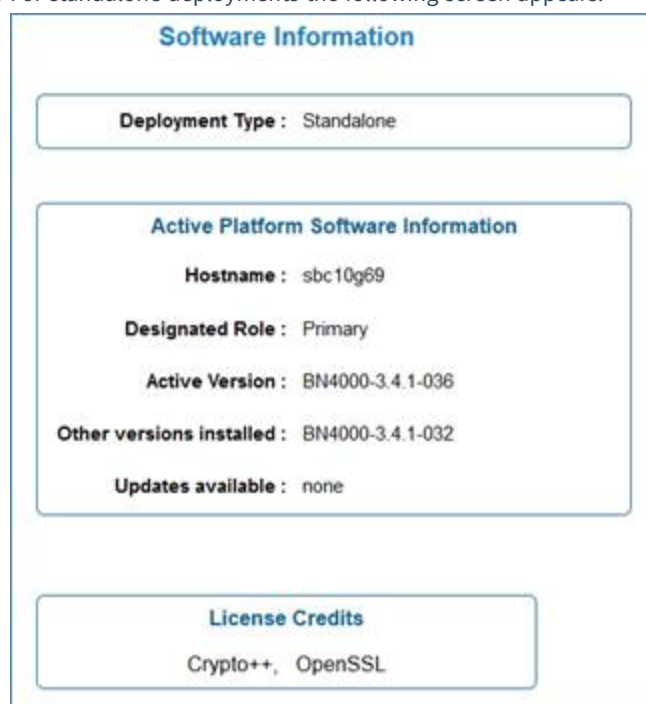
- Displaying software information
- Uploading new software
- Upgrading software
- Rolling back software
- Backing up and restoring configuration data

8.1 Displaying Software Information

There can be a maximum of five versions installed on the platform.

→ To display software information:

1. From the **Software** menu, select **About**.
2. For standalone deployments the following screen appears:



For an HA system, the same information appears for both primary and secondary platforms.

8.2 Uploading a New Software Release

You can upload a new release to the system. In an HA deployment, the software upload is performed only once and it is synced automatically to the standby platform.

Uploaded software releases are cleaned up automatically. Only the last three releases are kept on the system.

→ To upload a new software release:

1. From the **Software** menu, select **Upload New Release**.



2. The **Upload Software** window opens.
3. Click **Browse...** to select the file for upload.
4. Click **Upload** to upload the software.

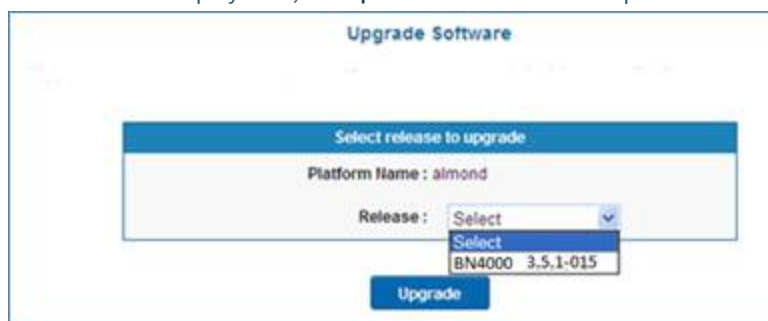
8.3 Upgrading Software

The following criteria apply to upgrading software:

- In a standalone deployment, you must upgrade software during a maintenance window because it affects traffic.
- All application processes are shutdown during the upgrade process.
- Application services are started as soon as the upgrade is completed.
- In an HA deployment, the upgrade is allowed only on the standby platform.
- The following operations should be done for HA deployment upgrade:
 - Upgrade current standby platform
 - Failover
 - Upgrade current standby platform

→ To upgrade the current software version:

1. From the **Software** menu, select **Upgrade**.
2. In a standalone deployment, the **Upload Software** window opens.



3. Select the software release from the dropdown list.
4. Click **Upgrade**.

8.4 Software Roll Back

→ To roll back the software to a previous release:

1. From the **Software** menu, select **Rollback**.
2. The **Software Rollback** window opens.



3. Select the software version to roll back to from the dropdown list.
4. Click **Rollback**.

8.5 Restoring and Backing up Configuration Data

Backing up software from a standalone system differs from an HA system.

- On a standalone system, when you back up the configuration data, the provisioning process is shut down. It is started up once the backup is completed.
- On an HA system, configuration data backup is taken on a standby platform and is also transferred to the active platform automatically.

→ To back up and restore configuration data:

1. From the **Software** menu, select **Backup & Restore** under **Data Management**.
2. The **Configuration Data Management** window opens.



3. Select one of the **Backup** options available:
4. Start Backup
5. Upload Backup
6. Restore Backup
7. Download Backup
8. Delete Backup

8.5.1 Starting the Backup

→ To start a backup:

1. Click **Start Backup** to back up the configuration data.
2. Click **Confirm**.

8.5.2 Uploading the Backup

→ To upload a backup:

1. Click the **Upload Backup** button to upload the configuration data backup file from the local machine to the BorderNet SBC application platform.
2. Click **Confirm**.

8.5.3 Restoring the Backup

Note:

Restoring configuration data is a service impacting action.


The process for restoring configuration data differs on a standalone system and an HA system as follows:

- On a standalone system, when you are restoring data, application services are shutdown and started once the backup restoration is complete.
- On an HA system, you restore data on the standby platform and then the automatic failover happens. You do not have to restore data on both platforms.

Note:


The system that you are restoring the data to has to be on the same version as the one backed up to. In addition, the filename has to be the same as the original filename that was downloaded.

→ To restore a backup:

1. Click the **Restore** icon  to restore the configuration data backup.
2. Click **Confirm**.


8.5.4 Downloading the Backup

→ To download a backup:

1. Click the **Download** icon  to download the configuration data to the local machine.
2. Click **Confirm**.

8.5.5 Deleting the Backup

→ To delete a backup:

1. Click the **Delete** icon  to delete the configuration data backup.
2. Click **Confirm**.

8.6 Upgrade / Rollback Update

Follow the below steps, after the **Upgrade/Rollback** procedure has been finalized.

→ To perform an upgrade and/or rollback update:

1. Before upgrade, backup the `/etc/sysctl.conf` file of each BorderNet SBC machine/platform.
2. In case of rollback to the previous release, after running the rollback procedure restore `/etc/sysctl.conf` on each machine.
3. Run `sysctl -p` after restoring the file.


8.7 Generating LRBT Package and Provisioning

Prior to configuring **Local Ring Back Tone (LRBT)** and uploading the LRBT files to the BorderNet SBC (from the local terminal), these files should be prepared to comply with the selected BorderNet SBC codecs and an appropriate syntax.

The below window provides a tool that assists the user to prepare the files.

→ To generate an LRBT package:

1. Select **Software** → **LRBT Tools**.
2. The following window opens.



- 3.
4. Select the buttons according to the following order:
5. **Provide input (wav file)**. Enables the user to select a **wav** file from the local terminal (in 8000/6000 sample rate, and **PCM Alaw** format).

Note:

-The filename should not contain #,%,&,{,},\, <, >, *, ?, /, back space, \$, !, ', " , : , and @

-Don't start the filename with space/period/hyphen/underline.

-Make sure that the filename length is less than 31 characters.

-Always use lowercase letters.

-Avoid using space and underscore (use a hyphen instead).

- **Upload.** Enables the user to upload the **wav** file to the BorderNet SBC tool.

The tool prepares a **tar** file (with the original file name), including files per codec, and **wav** files per codec. The **tar** file is downloaded back to the user's local terminal to: `c:\Users\<User name>\Download`.

1. Prepare a zip file from the files with the selected codecs.
2. Select the created zip file, using the **Customize LRBT** tab (see *BorderNet SBC Provisioning Guide, Customized LRBT*).
3. Create a **Parameter Profile**, with **Initiate Reliable Provisional Responses** set to **Yes** (see *BorderNet SBC Provisioning Guide*)
4. Configure the **LRBT** service (see *BorderNet SBC Provisioning Guide, LRBT*).
5. Select the relevant **Parameter Profile** and **Service Profile** for the originating peer.

Note:

To use the LRBT capability: Update, Prack, and 100Rel must be supported on the originating peer.

9. Audit Logs

The **Audit Log** functionality audits every data change happening in the system and writes the information into an audit record file. The system maintains the file for one year.

The following audit records are recorded into the file:

Parameter	Type	Mandatory	Description
<ul style="list-style-type: none">• Time	<ul style="list-style-type: none">• Date-time	<ul style="list-style-type: none">• N	<ul style="list-style-type: none">• Date+Time in seconds when the audit trail is generated.
<ul style="list-style-type: none">• Username	<ul style="list-style-type: none">• String	<ul style="list-style-type: none">• N	<ul style="list-style-type: none">• Name of the user who requested the change.
<ul style="list-style-type: none">• Device	<ul style="list-style-type: none">• String	<ul style="list-style-type: none">• Y	<ul style="list-style-type: none">• IP address or device name from where Web GUI was accessed.
<ul style="list-style-type: none">• Event	<ul style="list-style-type: none">• String	<ul style="list-style-type: none">• N	<ul style="list-style-type: none">• CREATE, UPDATE, DELETE
<ul style="list-style-type: none">• Resource	<ul style="list-style-type: none">• String	<ul style="list-style-type: none">• N	<ul style="list-style-type: none">• Name of the resource/filename that was modified.
<ul style="list-style-type: none">• Result	<ul style="list-style-type: none">• String	<ul style="list-style-type: none">• N	<ul style="list-style-type: none">• SUCCESS/FAILURE

Table 4: Audit Log

Note:

You must have Security Auditor privileges to view the audit records.

→ To view audit logs:

1. From the **System** menu, select **Audit Logs** under **Administration**.

2. The **Audit Logs** window opens.

	Time	User	Event	Device	Resource	Result
🔍	2016-05-31 13:33:22	A	UPDATE	172.29.9.71	NpVarfCtg_3.xml	Success
🔍	2016-05-31 13:33:12	A	CREATE	172.29.9.71	NpVarfCtg_Lxml	Success
🔍	2016-05-31 13:33:12	A	CREATE	172.29.9.71	NpCtg_3.xml	Success
🔍	2016-05-31 13:32:55	A	UPDATE	172.29.9.71	NpVarfCtg_1.xml	Success
🔍	2016-05-29 09:42:19	A	UPDATE		License_insl.xml	Success
🔍	2016-05-25 14:21:08	A	UPDATE	172.29.9.71	SbcSipCtg_21.xml	Success
🔍	2016-05-25 12:45:55	A	UPDATE	172.29.9.71	StaticRouting_3st.xml	Success
🔍	2016-05-25 12:45:30	A	UPDATE	172.29.9.71	StaticRouting_3st.xml	Success
🔍	2016-05-25 12:45:20	A	CREATE	172.29.9.71	SbcSipPeerCtg_2.xml	Success
🔍	2016-05-25 12:45:00	A	CREATE	172.29.9.71	SbcSipPeerCtg_1.xml	Success
🔍	2016-05-25 12:44:42	A	CREATE	172.29.9.71	SbcSipPeerCtg_21.xml	Success
🔍	2016-05-25 12:43:50	A	CREATE	172.29.9.71	SbcSipPeerCtg_11.xml	Success
🔍	2016-05-25 12:41:39	A	CREATE	172.29.9.71	SbcSipCtg_21.xml	Success
🔍	2016-05-25 12:40:50	A	UPDATE	172.29.9.71	SbcSipCtg_11.xml	Success
🔍	2016-05-25 12:40:40	A	CREATE	172.29.9.71	SbcSipCtg_11.xml	Success
🔍	2016-05-25 12:39:20	A	CREATE	172.29.9.71	SbcSocProfile_2.xml	Success
🔍	2016-05-25 12:37:06	A	CREATE	172.29.9.71	SbcSipMediaProfCtg_3.xml	Success
🔍	2016-05-25 12:37:06	A	CREATE	172.29.9.71	SbcSipMediaProfCtg_2.xml	Success
🔍	2016-05-25 12:36:39	A	CREATE	172.29.9.71	SbcSipMediaProfCtg_2.xml	Success
🔍	2016-05-25 12:36:39	A	CREATE	172.29.9.71	SbcSipMediaProfCtg_1.xml	Success

3. Click the **Filter** button to refine the results:



4. Enter the filtering criteria from the **Audit Filter** window as below:

Audit Filter

User Name:

Event: ▼

Resource:

Date (YYYY-MM-DD) and Time (HH:MM:SS)

Start Date: 📅

End Date: 📅

Start Time: End Time:

Clear

OK Cancel

Note:

The User Name and Resources fields are case-sensitive.

1. To display the details on a record, select the record and click **Audit**.



2. You can also double-click any record to display the **Audit Details**.

4. Click OK.

The screenshot shows a dialog box titled "Audit Details" with a close button (X) in the top right corner. It contains several input fields with the following values:

- Time: 2016-05-25 14:21:58
- User Name: A
- Device: 172.29.8.71
- Event: UPDATE
- Resource: SbcSipIcfig_21.xml
- Result: Success

Below these fields is a section titled "Details" with a "Content:" label and a text area containing XML data:

```
Content: <id>21</id>
- <CfgStatus>No</CfgStatus>
+ <id>21</id>
+ <CfgStatus>Yes</CfgStatus>
<Time>2016-05-25 14:21:58</Time>
```

An "OK" button is located at the bottom center of the dialog box.


10. Additional Diagnostics Tools

10.1 Logged In Users


→ To view the logged-in users:

1. Select **Diagnostics à Logged In Users**.
2. The **Logged-In Users** window opens.



	User Name	Device	Login Time	Last Access Time
	John	172.29.8.51	2016-11-09 09:32:38	2016-11-09 10:03:46
	Mathew	172.29.8.162	2016-11-08 17:25:01	2016-11-09 10:03:40

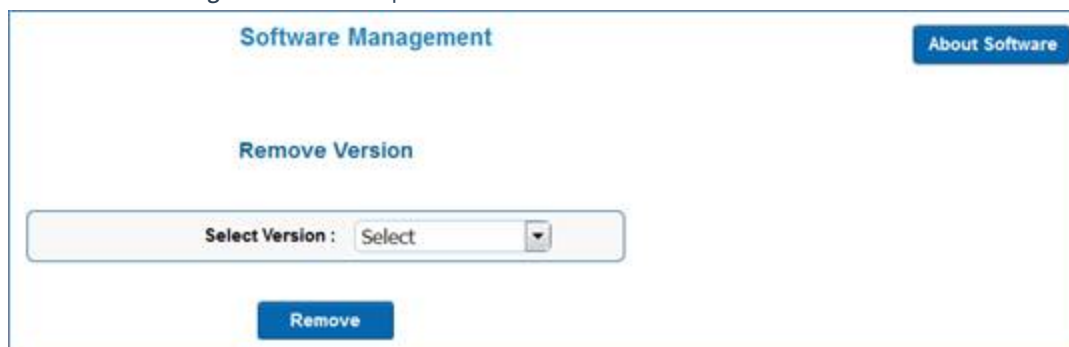
→ To end a user's login:

1. Select the user.
2. Click the **Edit**  icon and select **End**.

10.2 Remove Older Builds

→ To remove the older versions from the local storage of the platform:

1. Select **Diagnostics à Remove older Builds**.
2. The **Software Management** window opens.



Software Management About Software

Remove Version

Select Version :

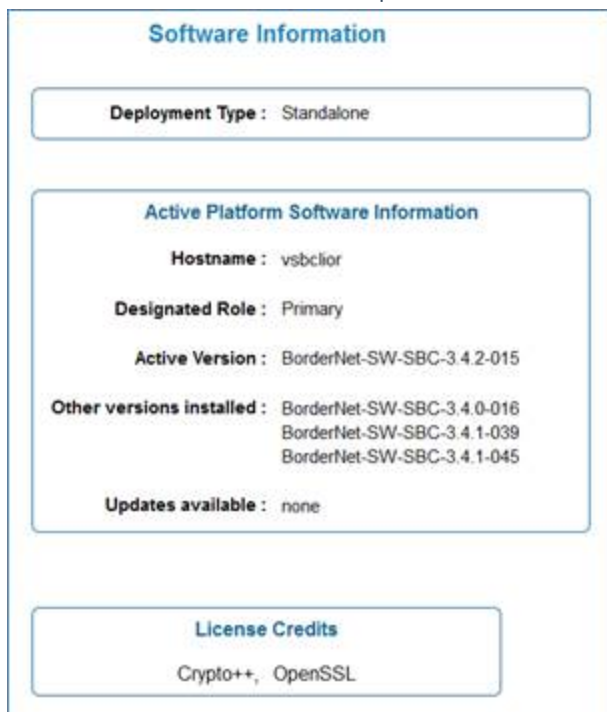
Remove

3. Select the version to be removed, using the dropdown menu.
4. Click **Remove**.

→ To view information on the current software:

1. Click **About Software**.


2. The **Software information** window opens.




10.3 Cores

→ To view all the system's cores (failures):

1. Select **Diagnostics à Cores**.
2. The **Cores** window opens.

	name	time	Platform
	core-bnetics-v3.4.2-015-11-0-0-2641-1475082626	Wed Sep 28 17 13 46 2016	Active

→ To delete a core's record:

1. Select a core.
2. Click the **Edit**  icon, and select **Delete**.

10.4 BorderNet SBC Dump

→ To download the BorderNet SBC logs as a zip file:

1. Select **Diagnostics à BorderNet SBC Dump**.

2. The list of available files is displayed.



1. Click on **Create Dump File**.
2. The following window opens.



3. Click on **Start Download** to download the logs' zip file.

11. Troubleshooting

This section will help you determine the cause of a problem with the BorderNet SBC and indicate corrective actions to follow.

11.1 Alarms

The table below lists each alarm that the BorderNet SBC produces along with descriptions and corrective actions.

Name	Category	Severity	Description	Corrective Actions
Approaching Session License limit	Overload	Major	System rejects calls due to exceeding the maximum amount of calls allowed according to the license.	The alarm is cleared when the percentage falls below 90%.
Approaching System License limit	Overload	Major		
Bandwidth usage approaching configured limit for interface	Overload	Minor	Bandwidth at the SIP interface is over 95% of the configured bandwidth limitation.	The alarm will be cleared when bandwidth usage is below 90% of the configured bandwidth limitation. To configure a new bandwidth limitation go to the Media Profile.
Bandwidth usage approaching configured limit for peer	Overload	Minor	Bandwidth at the SIP peer is over 95% of the configured bandwidth limitation.	The alarm will be cleared when bandwidth usage is below 90% of the configured bandwidth limitation. To configure new bandwidth limitation go to the Media Profile.
Communication Lost with Paired Platform	Hardware	Critical	Raised when the platform deployed in HA configuration detects communication failure with paired platform.	Check the connectivity between the paired platforms of the HA configuration. Also verify that the paired platform with which the communication failure is reported, is up and running BorderNet SBC software.

Name	Category	Severity	Description	Corrective Actions
Configuration Data is not in sync	Configuration	Major	When the Standby platform of the HA system is upgraded/rollback to a different software version of the Active platform, it will raise this alarm to indicate to users that any configuration changes made through the GUI will be lost, if the system is in failover.	Failing over to Standby platform and upgrading the other platform so that both platforms will have the same software version. This alarm will be cleared once the software versions on both platforms are the same.
Configuration Data Validation Failure	Configuration	Critical	When the platform becomes active from standby, the configuration data is validated. If the validation fails then this alarm is raised.	Follow the detail error message in the alarm, delete the objects that caused the validation to fail, and restart the platform. Delete the object that caused the problem. Then restart the platform.
Connectivity Failure with Peer	QoS	Major	A configured peer fails to respond to OPTIONS sent by the system.	If calls can be sent over that peer regardless then turn off connectivity for that peer. If the peer is supposed to respond verify if there are routes to the peer. See if routes to that peer need to be determined. Verify that what is configured from the Web GUI has made it properly to the internal components by another debug mechanism. See if there are any configuration errors if any. See if there are internal configuration errors by intrusive debugging into the platform such as debug access on process, and logs.
CPUmng Utilization Reached Overload Level	Overload	Major, Minor, Critical	CPU usage crossed the following predefined thresholds: o 75%-minor o 85%-major o 95%-critical	This alert refers to CPU0 that handles the management, high availability and platform management.
CPUmedia Utilization Reached Overload Level	Overload	Major, Minor, Critical	CPU usage crossed the CPU usage crossed the following predefined thresholds: o 75%-minor o 85%-major o 95%-critical	This alert refers to the CPU1 to CPU _n that handle the media

Name	Category	Severity	Description	Corrective Actions
DB Operation Failed	Configuration	Major	Raised if attempting to insert/delete an entry to/from the report DB fails.	Cleared when the next operation on the same DB is successful.
DNS queries to External DNS server failed	Configuration	Minor	Raised when the DNS query to the DNS server is failed.	The alarm is operator clearable only.
Essential System Component Failed	HA	Critical	The system detects the failure of some critical system component in the platform that affects the system functionality. If this failure was detected on the platform that is serving the ACTIVE role, the system may decide to failover to the paired-platform if one is available. The system continues to provide the desired functionality.	The operator should review the available diagnostics to understand what component failed and the reason. If the issue persists the operator may contact support for further troubleshooting.
Ethernet Link Administratively Disabled	Configuration	Minor	Raised when the Ethernet link is administratively "disabled". The alarm gets cleared when this Ethernet link is administratively "Enabled".	The alarm is the result of user action disabling the link. User can enable the link from the Ethernet Links Screen.
Ethernet Link Failed	Network	Critical	Raised when the system detects the Ethernet link (both Primary and Secondary Ethernet links of the link pair) to have failed.	Check both the physical interfaces for the given Ethernet link and ensure they are properly connected to the switch. If the problem persists check the cables and the Ethernet properties such as speed, duplex, auto negotiation are configured the same on both ends of the Ethernet link.
Excessive Packet Drops	Security	Minor	Too many packets are being dropped in the system.	Verify the System Statistics. This is an indicative alarm and no correction is required.

Name	Category	Severity	Description	Corrective Actions
Fan Speed Sensor Reached Threshold (not relevant for Virtualized SBC)	Hardware	Major	The Fan speed sensors detect that the fan failed or is operating below configured fan speed thresholds indicating potential mechanical failures.	Check the platform fan.
Interface Activation Failed	Configuration	Critical	The system failed to open up a listening ip:port for the configured interfaces.	Check the interface configuration on the Web GUI. Turn-off and Turn-on the configuration. Remove Associations. Clone and delete old....rename the clone to the previous one (source). On the interface screen, sort on the IP and ensure the same IP and port does not exist. Restart IBCF service.
IP Address Configuration Failure	Configuration	Minor	The received configuration failed to get configured/applied on the BorderNet SBC platform. Configuration failure examples that could result in this alarm include IP Address assignment/un-assignment failure. The FDN and additional alarm details contains the information for the object type (for example, VLAN, IP and IPRROUTE) and the object identified (for example ID or the Name of the object) that failed to get configuration on the platform.	The operator provided a configuration of the IP Address, IP Route etc. that was rejected by the underlying OS layer. This may happen when the given configuration is either not valid or already exists or conflicts with another configuration on the platform. The additional detail string in the alarm usually provides the error not received from the operating system which can be used to further debug the issues with the configuration data. The operator should check and correct/remove invalid configuration data from the provisioning system and manually clear the alarm.

Name	Category	Severity	Description	Corrective Actions
IP Route Configuration Failure	Configuration	Minor	The received configuration failed to get configured/ applied on the BorderNet SBC platform. The following are the Configuration failure examples that could result in this alarm include IPROUTE configuration failure. The FDN and additional alarm details contains the information for the object type (for example, VLAN, IP and IPROUTE) and the object identified (for example ID or the Name of the object) that failed to get configuration on the platform.	The operator provided a configuration of IP Address, IP Route etc. that was rejected by the underlying OS layer. This may happen when the given configuration is either not valid or already exists or conflicts with another configuration on the platform. The additional detail string in the alarm usually provides the error not received from the operating system which can be used to further debug the issues with the configuration data. The operator should check and correct/remove the invalid configuration data from the provisioning system and manually clear the alarm.
IPSec Policy Configuration Failed	Configuration	Major	Raised when the Policy Configuration fails to push the required data into the kernel through the Pluto daemon.	No corrective action is provided for the operator. If possible a "bnetipsec" service restart may resolve the issue if an alarm is raised for all policies in the system.
Licensed Transcoding Resources Usage above 90 percent	Overload	Major	This alarm is raised if the percentage of transcoding resources allocated is greater than 90%.	The alarm is cleared when the percentage falls below 85%.
Licensed Transcoding Resources Usage above 95 percent	Overload	Critical	This alarm is raised if the percentage of transcoding resources allocated is greater than 95%.	The alarm is cleared when the percentage falls below 90%.
License Expired	License	Critical	Indicates either that the trial/production license has expired.	Verify the License Contents on the Web GUI and purchase an updated new license.

Name	Category	Severity	Description	Corrective Actions
License Nearing Expiry	License	Critical	Indicates either that the trial/production expiry is nearing (15 days prior).	Verify the License Contents on the Web GUI and purchase an updated new license.
Maximum Active Sessions reached on Interface	QoS	Major	Calls were rejected at the Interface due to exceeding the configured Max Active Sessions at the Interface in the security profile.	Verify the Security Profile and Reports. Check the security profile.
Maximum Active Sessions reached on Peer	QoS	Major	Calls were rejected at the Peer due to exceeding the configured Max Active Sessions at the Peer in the security profile.	Verify the Security Profile and Reports. Check the security profile.
Maximum Incoming Sessions Rate Reached on Interface	QoS	Major	The rate of rejection for the incoming calls exceeded 10% of the maximum incoming rate at the Interface.	Verify the Security Profile and Reports. Check the security profile.
Maximum Incoming Sessions Rate Reached on Peer	QoS	Major	The rate of rejection for the incoming calls exceeded 10% of the maximum incoming rate at the peer.	Verify the Security Profile and Reports. Check the security profile.
Maximum Outgoing Session Rate reached on Interface	QoS	Major	The rate of rejection for the outgoing calls exceeds 10% of the maximum outgoing rate at the Interface.	Verify the Security Profile and Reports. Check the security profile.
Maximum Outgoing Session Rate Reached on Peer	QoS	Major	The rate of rejection for the outgoing calls exceeded 10% of the maximum outgoing rate at the peer.	Verify the Security Profile and Reports. Check the security profile.

Name	Category	Severity	Description	Corrective Actions
Media Inactivity Call disconnection	QoS	Minor	This alarm is raised when a call is disconnected due to media inactivity timer expiration.	The alarm is operator clearable only.
Memory Utilization crossed Critical Level	Overload	Major	The Memory usage crossed the following predefined thresholds: 75%-minor and 90%-major	
Packet Rate Limit Exceeded at Interface	QoS	Minor	Indicative alarm Peer received more than the configured packet rate.	No corrective action
Packet Rate Limit Exceeded at Peer	QoS	Minor	Indicative alarm. Peer received more than the configured packet rate.	No corrective action
Packet Rate Limit Reached at Interface	Overload	Critical		
Peer Blacklisted	Security	Major	The system received a high session rate - more than configured. The system received malformed SIP messages from a peer - more than allowed so it is blacklisted.	Verify with the Security Profile and Reports (peer-level statistics will be needed). First check if this is the desired behavior. If it is, then monitor to see if the peer is removed from the blacklist after the timeout, otherwise the dynamic blacklisting can be re-configured.
Peer Blacklisted Due to High Packet Rate	QoS	Minor	A particular peer gets more packets than configured and entered into the Blacklist.	Verify with Security Profile and Reports (peer-level statistics will be needed). First check if this is the desired behavior. If it is, then monitor to see if the peer is removed from blacklist after the timeout, otherwise the dynamic blacklisting can be re-configured.
Physical Ethernet Interface Failed	Network	Major	The system detects the physical interface failure.	Check the physical interfaces and ensure they are properly connected to the switch. If the problem persists check that the cables and the Ethernet link properties such as speed, duplex, auto negotiation are configured the same on both ends of the Ethernet link.

Name	Category	Severity	Description	Corrective Actions
Platform does not support IPSec	Hardware	Major	Raised when the BorderNet SBC platform does not have the hardware required to support the hardware acceleration provided by Cavium.	No corrective action is required. The alarm is cleared when the required hardware is installed.
Platform Failover	HA	Major	This alarm is informational to the operator when the platform failed over and the fault/failure or the operation that resulted in this failover action.	This alarm is informational to the operator to indicate platform failover and its reason.
Platform Memory Size not as Expected	Hardware	Major	The BorderNet SBC checks for the available physical memory on the platform during powerup checks. If memory is not as expected, the system raises this alarm.	Replace the bad memory card(s).
Power Supply Failed	Hardware		Indicates a power supply failure on the platform. The alarm detail identifies the power supply that is detected as failed and the cause of the failure. Is the power supply not present or not connected?	Check the power supply.
RAID Device Degraded	Hardware	Major	The system detected the RAID degraded possibly due to HDD failure. The alarm details indicate which of the two HDD failed.	Check hard disks on the platform that is showing RAID degraded.

Name	Category	Severity	Description	Corrective Actions
Registration with Gatekeeper failed	Configuration	Critical	The H.323 Interface failed to register with the Gatekeeper Peer.	Check the accuracy of the Gatekeeper information on the respective Peer. Check availability of the gatekeeper from the BorderNet SBC interface Turn Off and On the interface to reinitiate registration.
Root Extremely Low Disk	Overload	Major	This alarm is raised when <i>root</i> partition is 90% full.	
Extremely Low Disk for <fs name>	Overload	Minor	This alarm is raised when <i>root</i> partition is 80% full.	<fs name> values: ROOT. alarms for "/" CONFIG. alarms for "/config" ARCHIVE. alarms for "/archive" CORES. alarms for "/cores"
SCS Emergency Session Limit Reached	Overload	Critical	Emergency Limits exhausted beyond the license limit	Configure/Purchase higher License limits for call processing.
SCS Emergency Session Limit Reaching	Overload	Critical	Emergency Limits at 80% the license limit	Configure/Purchase higher License limits for call processing.
SCS Profile Emergency Session Limit Reached	Overload	Critical	Emergency Profile limit values reached	Increase the Profile limits for Emergency Calls
SCS Profile Emergency Session Limit Reaching	Overload	Critical	Emergency Profile at 80% of limit values reached	Increase the Profile limits for Emergency Calls
SCS Profile Max Session Limit Reached	Overload	Critical	Max Sessions Profile limit values reached	Increase the Profile limits for Max Sessions Calls
SCS Profile Max Session Limit Reaching	Overload	Critical	Max Sessions at 80% of limit values reached	Increase the Profile limits for Max Sessions Calls
SCS Resource Limit Reached	Overload	Critical	This alarm is raised when the threshold limit of 90% is reached on a resource used by the SCS. See the SCS Resources table for a list of the resources that are monitored by the SCS. System Resources exhausted.	This is raised as a warning by the system before it fails over. Reduce call load.

Name	Category	Severity	Description	Corrective Actions
SDR Extremely Low Disk	SDR	Critical	This alarm is raised when <i>/eventdata</i> partition is 90% full. At this point SDR stops recording the events.	
SDR Files are not Sent out Promptly	SDR	Critical	Unsent SDR files are accumulated.	Change the TCP parameters to increase the speed. Also, if SDR files are not compressed, you can change the setting to compress them.
SDR File Transport Failure	SDR	Critical	The SDR file transport to the billing server failed.	Ensure that the SDR destination IP Address and directory name are both correct. Make sure the network is working properly and the destination host has enough disk space.
SDR Low Disk	SDR	Major	This alarm is raised when <i>/eventdata</i> partition is 80% full.	
Session Data Record Disabled in Configuration	Configuration	Major	When the Session Detail Record (SDR) is disabled, no SDR records are generated while both signaling and media traffic are on-going.	To enable the Session Detail Record, select SDR Configuration from the System menu. Select Enable.
Session License Limit Reached	Overload	Critical	The number of concurrent sessions reached the licensed limit.	
SRTP Session License Limit Reached	Overload	Major	This alarm is raised if the percentage of the allocated SRTP sessions is greater than 95%.	The alarm is cleared when the percentage falls below 90%.
System Component Failed	HA	Major	The system detects the failure of some system components in the platform that affects the system functionality but does not result in failover.	The operator should review the available diagnostics to understand what component failed and the reason. If the issue persists the operator can contact Support for further troubleshooting.
System Session Limit Reached	Overload	Critical		

Name	Category	Severity	Description	Corrective Actions
System Session Rate Limit Reached	QoS	Major		
Temperature Sensor Reached Threshold (not relevant for virtualized BorderNet SBC)	Hardware	Major	The platform chassis inlet temperature is detected reaching above critical or non-recoverable thresholds.	Check the system hardware, fan and operating environment conditions and take adequate steps to provide proper system cooling.
TLS Connectivity to Configured Peer Failed	Security	Minor	TLS handshake with the remote configured peer fails.	Verify the certificates and cipher suites configured on the TLS profile for the interface used to connect to this peer.
TLS Connectivity to Un-Configured Peer Failed	Security	Minor	TLS handshake with the remote unconfigured peer failed.	Verify the certificates and cipher suites configured on the TLS profile for the interface used to connect to this peer.
Transcoding Interface Connection Failure (not relevant for virtualized BorderNet SBC)	Hardware	Critical	A transcoding card's interface has failed.	Check the transcoding card, and its interfaces' connectivity.
Transcoding Service Unavailable	Configuration	Critical		
VLAN Configuration Failure	Configuration	Critical	The received configuration fails to get configured and applied on the BorderNet SBC. VLAN addition/deletion is a configuration failure that could result in this alarm. The FDN and additional alarm details contain the information for the object type (e.g. VLAN, IP, IPRROUTE etc.) and the object identified (e.g. ID or the Name of the object) that failed to get configuration on the platform.	The operator provided a configuration of VLAN that was rejected by the underlying OS layer. This may happen when the given configuration is either not valid or already exists or conflicts with another configuration on the platform. The additional detail string in the alarm usually provides the error not received from the operating system which can be used to further debug the issues with the configuration data. The operator should check and correct/remove the invalid configuration data from the provisioning system and manually clear the alarm.

Table 5: Alarms Consequent Actions

11.2 SCS Resources

Resource	Description
Calls	The resource information of the call-leg objects.
Invite Lists	Every call-leg holds one list of "invite" objects to manage all its invite transactions. This is the resource information of all the allocated invite lists.
Invite Objects	The resource information of all the "invite" objects that are allocated by all call-legs.
Transaction Handles	The resource information of all the "transaction handle" objects that are allocated by all call-legs.
Transaction Lists	Every call-leg holds one list of "invite" objects to manage all its invite transactions. This is the resource information of all the allocated invite lists.
Header Pool	The pool of SIP headers for use during message processing.
Message Pool	The pool of SIP messages for use during message processing.
SDP Pool	The pool of SDP messages for use during message processing.

Table 6: SCS Resources