ERICSSON

BGF Troubleshooting Guide

Border Gateway Function

FAULT TRACING DIRECT

16/154 51-CRA 119 1170/1 Uen B

Contents

1 Introduction

This document provides troubleshooting procedures and functions for Border Gateway Function (BGF) on the SmartEdge® router. For information about the role of contexts in troubleshooting and how to get help with a command, perform basic debugging tasks, use basic troubleshooting commands, access the SmartEdge router components, perform backups, collect troubleshooting data, and enable logging, refer to Basic Troubleshooting Techniques, Reference [3]. For information about troubleshooting general issues, including hardware, refer to General Troubleshooting Guide, Reference [2].

The scope of the document includes:

- Tools used for troubleshooting
- Troubleshooting functions
- The troubleshooting procedure
- The backup and recovery procedure

The following are not covered in this document:

- Installation and initial configuration instructions
- Periodic maintenance tasks
- Configuration parameters

This document is intended for personnel involved in troubleshooting BGF.

1.1 Prerequisites

It is assumed that the user of this document is familiar with H.248 messages, Ethereal, GDB, and the relevant RFCs.

It is also assumed that users of this document are familiar with performing operations in the area for operation and maintenance (O&M) in general.

1.1.1 Conditions

Certain troubleshooting activities can impact node performance. For example, trace or log activation can slow traffic and is not recommended without first consulting Ericsson.

2 Tools

This section describes the tools that you can use to troubleshoot BGF.

2.1 Wireshark/Ethereal

Use Wireshark or Ethereal to trace and retrieve traces of IP interface.

3 Troubleshooting Functions

This section describes the troubleshooting functions for BGF.

3.1 Show commands

This section lists the `show` commands commonly used for troubleshooting.

3.1.1 Calls and Contexts on SmartEdge OS

The following `show` commands are used to view the calls and contexts on SmartEdge OS:

- **show media-gateway [instance *instance-id*] statistics call**
- **show media-gateway [instance *instance-id*] statistics mgc-group *name* call**
- **show media-gateway [instance *instance-id*] statistics stream** displays IPv4 or IPv6 and SRTP E2E or E2AE streams.
- **show media-gateway [instance *instance-id*] mgc-group *name* context**
- **show media-gateway [instance *instance-id*] statistics media**
- **show media-gateway [instance *instance-id*] statistics realm *name***

3.1.2 PTEs on SmartEdge OS

The following `show` commands are used to view the path-terminating equipment (PTE) on SmartEdge OS:

- **show media-gateway [instance *instance-id*] media-flows**
- **show media-gateway [instance *instance-id*] media-flows detail full**

3.1.3 PTEs on ASP

The following `show` commands are used to view the PTEs on the Advanced Services Processor (ASP):

- **show media-gateway card *slot-number/asp-number* port detail**
- **show media-gateway card *slot-number/asp-number* port grid *grid_id***
- **show media-gateway card *slot-number/asp-number* port grid *grid_id* port *port_number***

3.1.4 MGMd

The following commands are used for Media Gateway Manager daemon (MGMd):

- **show media-gateway manager license**
- **show media-gateway manager mgc-group**
- **show media-gateway manager media-address-group**
- **show media-gateway manager realm**

3.1.5 MGd

The following commands are used for Media Gateway daemon (MGd):

- **show media-gateway [instance *instance-id*] media-address-group**
- **show media-gateway [instance *instance-id*] realm**

3.1.6 Alarm Statistics

The following command is used to view the alarm statistics:

show media-gateway statistics alarm

3.1.7 MGd Debug Statistics

The following command is used to view MGd debug statistics:

show media-gateway [instance *instance-id*] statistics debug

3.1.8 ASP Data-Path Statistics

The following command is used to view ASP data-path statistics:

show media-gateway card *slot-number/asp number* statistics data-path

3.1.9 MGd Interface Statistics

The following commands are used to view MGd interface statistics:

- **show media-gateway [instance *instance-id*] statistics interface gci**
- **show media-gateway [instance *instance-id*] statistics interface pmi**
- **show media-gateway [instance *instance-id*] statistics interface card *slot-number***
- **show media-gateway [instance *instance-id*] statistics interface asp *asp-number***

3.1.10 ASP Interface Statistics

The following command is used to view ASP interface statistics:

show media-gateway card *slot-number/asp-number* statistics ipc

3.2 Debug Logs

This section describes commonly used tracing and logging methods for debugging BGF issues.

3.2.1 IPC Logs

Use the following command for interprocess communication (IPC) between MGMd and Media Gateway Manager (MGM).

- **show media-gateway manager ipc**

Use the following command for media port IPC between MGMd or MGd and ASP:

- **show media-gateway card *slot-number/asp-number* log detail**

3.2.2 MGMd Debugging

Enable debugs by using the **debug media-gateway manager** command.

For more information about the MGMd debugging command, see Reference [5].

3.2.3 MGd Debugging

1. Enable debugs by using the **`debug media-gateway all`** command.

   For more information about the MGd debugging command, see Reference [5].

2. Enable PD or IPS logs:

   a In the file `/usr/siara/config/mgd.conf` on the active and the standby cards, remove the semicolon at the beginning of the following lines, if any, and update their values as shown here.

   ```
   ips_buf_size = 100000
   pd_buf_size = 100000
   ips_size = 100000
   pd_size = 100000
   ips_tracing = YES
   ```

   b Enable debug logs on the BGF using the following commands:

   – **`debug media-gateway call level buffer 1`**

   – **`debug media-gateway protocol level buffer 1`**

   c Restart the MGd processes for the above configuration to take effect.

3.2.4 MGDP Debugging

Use the following commands for Media Gateway Data Plane (MGDP) debugging:

- **`debug media-gateway card`** ***`ase-card-number/asp-number`***
- **`debug media-gateway card`** ***`ase-card-number/asp-number`*** **`dp`**
- **`debug media-gateway card`** ***`ase-card-number/asp-number`*** **`dp-proxy`**

For example,

```
[local]Redback#debug media-gateway card 4/1?
dp  Enable Media Gateway DP debugging
dp-proxy  Enable Media Gateway DP-Proxy (DPP) debugging

[local]Redback#debug media-gateway card 4/1 dp?
all  DP all debugging
config  DP Config debugging
general  DP General debugging
init  DP Init debugging

[local]Redback#debug media-gateway card 4/1 dp-proxy?
all  DPP all debugging
dp  DPP DP debugging
general  DPP General debugging
mgd  DPP MGD debugging
mgmd  DPP MGMD debugging
```

4 Troubleshooting Procedure

This section describes the troubleshooting procedures for BGF.

4.1 H.248 Link Failure

Perform the following checks when there is a H.248 link failure:

1. Check IP address connectivity between session gateway controller (SGC) and BGF using the `ping` command:
   - Log on to SGC and type `ping <ip_bgf>`.
   - Log on to BGF and type `ping <ip_sgc>`.
2. Check the H.248 link between SGC and BGF using the following `show` commands:
   - **show media-gateway [instance *instance-id*] statistics mgc-group *mgc-grp-name***
   - **show media-gateway [instance *instance-id*] mgc-group *mgc-grp-name***
3. Check Stream Control Transmission Protocol (SCTP) link using the following `show` commands:
   - **show sctp**
   - **show sctp statistics**
4. Check SCTP and H.248 message exchanges through Wireshark.

4.2 Call Setup Failures

Perform the following checks when there is a call setup failure:

1. Check the rejection code of H.248 messages through Wireshark.
2. Check whether BGF is overloaded and whether any time-out responses sent to SGC are pending, in any of the following ways:
   - Use the **show media-gateway [instance *instance-id*]** command.

     For example,

     ```
     [local]Redback#show media-gateway instance 1
     statistics call
     Current Calls:        20
     ```

```
Peak Calls:           20

Call Type             Current     Peak
=============================================
Normal Calls:        20          20
Emergency Calls:     0           0

Rejections Due To
==================
Emergency Threshold:     0
Licensing Limit:         0
Stream Limit:            0
Bandwidth Limit:         0
Insufficient Resources:  0
Routing Failures:        0
```

- Capture the H.248 messages on the Ethereal on SGC.

4.3 Mid-Call Failures

Perform the following checks when there is a mid-call failure:

1. Check whether subscriber circuits are down.
2. Check for media idle in any of the following ways:
   - Use the SmartEdge OS PTE `show` commands:
     - **show media-gateway [instance *instance-id*] media-flows**
     - **show media-gateway [instance *instance-id*] media-flows detail**

     Ensure that `Status` is `In`

4.4 Media Forwarding Failures

Perform the following checks when there is a media forwarding failure:

1. Use the **show media-gateway instance *instance-id* media-flows detail** command to verify whether the incoming packets are from addresses other than the latched address.

   In the packets sent to the latched address, ensure that Real-Time Transfer Protocol (RTP) and Real-Time Transfer Control Protocol (RTCP) traffic is latched independently.

2. Use the following command to ensure the default value of `stream mode` is equal to *`In`* for RTP packets and the default value of `rtcpMode properties` is equal to *`SendReceive`* for RTCP packets. Also, you can use this command to view the media flow state, type and status for RTP/SRTP, RTCP/SRTCP and MSRP streams, along with Configured Services, BW params and SRTP params information.

   For example,

```
[local]Redback#show media-gateway instance 1 media-flows detail

Context Id:     0x40080002
IpAddress:      10.10.11.1              Port:           35844
State:          Unbound                 Type:           SRTP E2AE
Circuit:        Unknown circuit
Remote User IP: 25.10.10.2              Port:           16000
 PPA Slots:   None
ASP id:             6
Configured Services:
        Send-Recv
        DSCP Remarking      : 0x1e
Inactivity Duration: 86400          Direction:      Both
Slot:               04              Status:
Media Stop Time: NULL
BW params
Realm Index:   0    IN:       247  OUT:      247
Policing:      Disabled  SDR:      0    MBS:      0
Route Lookup:  Prefix:       25.10.10.2/32   RIB Prefix length: 32
SRTP params
Session Flags:
        Unencrypted SRTP Session
Cipher Action: Decrypt                      SRTP Tag    : 1
Crypto Suite : AES-CM-128-HMAC-SHA1-32      Key Params : 1
Lifetime  [1]: 2^20
MKI       [1]: 1:4

------------------------------------------------------------------------
Context Id:     0x40080002
IpAddress:      10.10.11.1              Port:           35845
State:          Unbound                 Type:           SRTCP E2AE
Circuit:        Unknown circuit
Remote User IP: 25.10.10.2              Port:           16001
 PPA Slots:   None
ASP id:             6
Configured Services:
        Send-Recv
        DSCP Remarking      : 0x1e
Inactivity Duration: 86400          Direction:      Both
Slot:               04              Status:
Media Stop Time: NULL
BW params
Realm Index:   0    IN:       0    OUT:      0
Policing:      Disabled  SDR:      0    MBS:      0
Route Lookup:  Prefix:       25.10.10.2/32   RIB Prefix length: 32
Receiver Freq:  0                       Sender Freq:    0

------------------------------------------------------------------------
Context Id:     0x40080002
IpAddress:      10.10.11.1              Port:           35846
State:          Unbound                 Type:           RTP
Circuit:        Unknown circuit
Remote User IP: 55.10.10.2              Port:           15000
 PPA Slots:   None
ASP id:             0
Configured Services:
        Send-Recv
        DSCP Remarking      : 0x1e
Inactivity Duration: 86400          Direction:      Both
Slot:               04              Status:
Media Stop Time: NULL
BW params
Realm Index:   0    IN:       247  OUT:      247
Policing:      Disabled  SDR:      0    MBS:      0
```

```
Route Lookup:  Prefix:       55.10.10.2/32   RIB Prefix length: 32

------------------------------------------------------------------------
Context Id:     0x40080002
IpAddress:      10.10.11.1                Port:           35847
State:          Unbound                   Type:           RTCP
Circuit:        Unknown circuit
Remote User IP: 55.10.10.2                Port:           15001
 PPA Slots:   None
ASP id:             0
Configured Services:
        Send-Recv
        DSCP Remarking      : 0x1e
Inactivity Duration: 86400          Direction:      Both
Slot:               04              Status:
Media Stop Time: NULL
BW params
Realm Index:   0    IN:       0    OUT:      0
Policing:      Disabled  SDR:      0    MBS:      0
Route Lookup:  Prefix:       55.10.10.2/32   RIB Prefix length: 32
Receiver Freq:  0                         Sender Freq:    0

------------------------------------------------------------------------
Context Id:     0x40080002
IpAddress:      10.10.12.1                Port:           35844
State:          Unbound                   Type:           SRTP E2AE
Circuit:        Unknown circuit
Remote User IP: 10.10.12.1                Port:           35846
 PPA Slots:   None
ASP id:             6
Configured Services:
        Send-Recv
        DSCP Remarking      : 0x1e
Inactivity Duration: 86400          Direction:      Both
Slot:               04              Status:
Media Stop Time: NULL
BW params
Realm Index:   1    IN:       247  OUT:      247
Policing:      Disabled  SDR:      0    MBS:      0
Route Lookup:  Prefix:       10.10.12.1/32   RIB Prefix length: 32
SRTP params
Session Flags:
        Unencrypted SRTP Session
Cipher Action: Encrypt                    SRTP Tag    : 1
Crypto Suite : AES-CM-128-HMAC-SHA1-32    Key Params : 1
Lifetime  [1]: 2^20
MKI       [1]: 1:4

------------------------------------------------------------------------
Context Id:     0x40080002
IpAddress:      10.10.11.1                Port:           16398
State:          Non Flow Bound            Type:           MSRP
Circuit:        1/10
Remote User IP: 10.10.11.1                Port:           16400
 PPA Slots:   01
ASP id:             0
Configured Services:
        Send-Recv
Filter IP Address:  10.10.11.1      , Mask: 32
Filter Port No., MIN: 16400           , MAX: 16400
Inactivity Duration: 0              Direction:      None
Slot:               None            Status:
Media Stop Time: NULL
BW params
Realm Index:   0    IN:       309  OUT:      309
Policing:      Disabled  SDR:      0    MBS:      0
Route Lookup:  Prefix:       10.10.11.1/32   RIB Prefix length: 32
MSRP Params:
Local Conn Setup:   Passive   Remote Conn Setup:      Flags:    0x6
Local URI:  msrp://10.10.11.1:16398/core_session_orig;tcp
Remote URI: msrp://10.10.11.1:16400/core_session_term;tcp
```

3. Use the **show port counters detail** and **show circuit counters detail** commands to verify if the drops are due to rate-limiting or shaping and so on.

4.5 Media Gateway Reconfiguration Failure

After undoing the configuration of the media gateway at the global configuration level, we recommend that you reconfigure the media gateway only after the MGMd and MGd processes on both and standby XC cards change to demand state. Use the **show process mgmd** and **show process mgd** commands on the active and standby cards to check the state of the processes.

4.6 CLI or the Process Is in Hung State

Perform the following checks when CLI or the process is in hung state:

1. Use the **show process mgd instance** *instance-id* command to get the process-level statistics.

   The output displays the possible completions:

```
chunk-statistics          Display process chunk memory statistics
crash-info                Display process crash information
detail                    Display detail process information
dmalloc-statistics        Display process dmalloc statistics
ipc                       Display process IPC statistics
ipc-pack-statistics       Display process IPC pack statistics
shared-memory-statistics  Display process shared memory statistics
thread-history            Display thread history information of a process
thread-info               Display thread information of a process
thread-log                Display thread log information of a process
```

2. Use the **process coredump** *process-name* command to perform a core dump of MGMd and all 3 instances of MGd sequentially.

   Ensure the `/md directory` is cleaned up before performing the coredump.

Caution!

Ensure that you do not perform the core dump if the BGF is overloaded.

4.7 Recovery After Process Restart or Switchover

Perform the following checks to recover after process restart or switchover:

- Use the **show redundancy** command on the active card before and after switchover or process restart.

- Use the **show process mgd instance*instance-id* detail** command to verify whether both active and standby are in sync before and after switchover or process restart.
- Use the **show media-gateway statistics call** command to check the number of calls before and after switchover or process restart.

5 Backup and Recovery Procedure

Memory storage on the SmartEdge router is on two Compact Flash (CF) cards on the Cross-Connect Route Processor (XCRP) cards, in three partitions:

- `p01`
- `p02`
- `flash, with UNIX-based file systems.`

p01 and p02 store the OS image files; the partition stores the most recent image installed, and the standby partition stores the previous image. If they are installed, external CF cards provide mass storage capacity, in two partitions, an `/md` partition and another partition for crash files. If no external CF card is installed on an XCRP card, the `/md` directory is placed on the internal CF card.

We recommend that you back up the following regularly:

- Crash files to remote location (optionally per context) — with the `service upload-coredump ftp:url [context ctx-name]` command (in global configuration mode).
- Log files to a syslog server (per context) — with the `logging syslog ip-addr [facility sys-fac-name]` command (in context configuration mode).

Before upgrading the SmartEdge OS or performing an XCRP switchover, perform the following backups:

1. Save the configuration with one of the following methods:
   - Save the current configuration to or flash or to a remote location (by FTP or SCP) with the save configuration `/flash/filename` or `ftp://username@hostname/filename` commands.
   - Back up the configuration during an upgrade. When the system prompts you to save the current configuration, enter **`y`** and specify the location and filename. If you do not specify the location and filename, the SmartEdge OS saves the configuration to `/flash/redback.cfg`.
2. Back up the contents of the `/flash` and `/md` disk partitions by accessing the `NetBSD shell` and backing up `/flash` and `/md` with the FTP command. For example, to backup `/flash` to `isp:test@192.168.145.99`, use the following commands:

```
[local]Redback#start shell
#ftp 192.168.145.99
Connected to 192.168.145.99. 220 (vsFTPd 1.2.2)
Name (155.53.12.7:root): isp:test
```

```
331 Please specify the password.
Password:password
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bi
200 Switching to Binary mode.
ftp> ha
Hash mark printing on (1024 bytes/hash mark).
ftp> prompt
Inter mode off.
ftp> cd backup-directory
250 Directory successfully changed.
ftp> mput *.*
```

When the files are copied, you see a message such as `226 File receive OK. 1595 bytes sent in 00:00 (1.02 MB/s).`

To back up the data on the external CF card, enter the **`bye`** command to exit FTP, switch to the `/md` directory and repeat the process.

After the upgrade, restore the configuration from the location where you saved it with the `configure filename` or `configure ftp:url/filename` commands.

6 Trouble Reporting

Problems identified that cannot be solved by using this document must be reported to the next level of maintenance support.

This report may result in either a Trouble Report (TR) or a Customer Service Report. Instruction regarding these processes is out of scope for this document. For more information on data that must be collected and enclosed in a Customer Service Request (CSR), refer to Data Collection Guideline for the SmartEdge Router, Reference [4]

Glossary

ASE
Advanced Services Engine

ASP
Advanced Services Processor

BGF
Border Gateway Function

CBA
Consumer and Business Applications

CF
Compact Flash

CSR
Customer Service Request

MGd
Media Gateway daemon

MGDP
Media Gateway Data Plane

MGMd
Media-Gateway Manager daemon

MSRP
Message Session Relay Protocol

NAT
Network Address Translation

O&M
Operation and Maintenance

PD
Prefix Delegation

RTCP
Real-Time Transfer Control Protocol

RTP
Real-Time Transfer Protocol

SCTP
Stream Control Transmission Protocol

SGC
session gateway controller

SRTP
Secure Real-Time Transport Protocol

TR
Trouble Report

Reference List

Ericsson Documents

[1] *Typographic Conventions*
DESCRIPTION, 1/1551-FCK 101 05

[2] *General Troubleshooting Guide*
FAULT TRACING DIRECT., 2/154 51-CRA 119 1170/1

[3] *Basic Troubleshooting Techniques*
FAULT TRACING DIRECT. , 15/154 51-CRA 119 1170/1

[4] *Data Collection Guideline for the SmartEdge Router*
DESCRIPTION, 92/1543-CRA 119 1170/1

[5] *BGF Command Reference*
COMMAND DESCRIPTION , 27/190 82-CRA 119 1170/1