Data Collection Guideline for the SmartEdge Router

Submitting a Customer Service Request

DESCRIPTION

Copyright

Trademark List

Contents

1 Introduction 1

1.1 Scope 1

1.2 Target Groups 1

2 Workflow 1

3 Mandatory Data 2

3.1 Mandatory Logs and Data 4

3.2 Acceptable Compression Formats 6

4 Collecting Data Based on Problem Type 6

5 Severity Levels 8

5.1 Emergency 8

5.2 High 9

5.3 Medium 9

5.4 Low 9

1 Introduction

This document describes the troubleshooting data that must be collected and enclosed in a Customer Service Request (CSR) in case a problem is experienced with the SmartEdge® router. This guideline also describes the procedure for collecting the necessary information.

1.1 Scope

This document covers the following issues:

- Description of the mandatory data, which must be included in all CSRs.
- Description of the problem-specific data, which must be included in a CSR.
- Description of the severity levels for the CSR.

1.2 Target Groups

This document is intended for experienced operation and maintenance personnel troubleshooting the SmartEdge router.

2 Workflow

The workflow for collecting troubleshooting data for the CSR is as follows:

1. Collect the general mandatory data that is needed for any problem experienced. For more information, see Section 3 on page 1.
2. Collect specific data based on the problem type. For more information, see Section 4 on page 6.
3. State the severity level of the CSR (mandatory), see Section 5 on page 8.

3 Mandatory Data

The data described in this section is essential for any CSR, regardless of the problem type.

Use the following checklist when writing the CSR. A more detailed description of each line is presented after the checklist. Some parts are not applicable to certain types of requests, for example documentation faults or consultations, but all parts apply to software and hardware faults. Fill out as many as possible for each case.

Table 1 Checklist when Writing CSRs

```
SmartEdge release:
HW platform:

RECENT CHANGES
SW changes:
Configuration changes:
HW changes:
O&M procedures:
Environment:

CASE DESCRIPTION
Case description:
Date and time:
Problem frequency:
Problem reproducibility:
Problem effects:
Network diagram to illustrate the problem:

ATTACHMENTS
System logs:
Crashfiles:
Output of the show tech-support command:
Other attachments:

MEASURES
On-site or online support:
Work around:
```

FACTS

- Specify the release. For example, SmartEdge OS, Release 6.5.1.

- Specify the hardware platform on which the fault occurred. If known, specify on which device and on which card the fault was found, for example, the

Chassis `Serial No` from the output of the **`show chassis`** command or the ***`slot`*** for the card.

RECENT CHANGES

Specify if any of the following changes has been implemented or occurred recently:

- Software updates or upgrades.
- Board replacement or hardware upgrades.
- Changes in upgrade, update, or installation procedures.
- Changes in configuration.
- Changes in the network. For example, a cutover.
- Any other relevant changes.

CASE DESCRIPTION

Provide a clear description of the consultation or the problem, to make it easier for Ericsson to locate the problem in the log files:

- Describe the case by answering, for example, the following questions:
  - What is the end-subscriber impact of the problem?
  - What is the network impact of the problem?
  - What is the operational limitation of the problem?
- State the exact date and time when the fault occurred or when it was discovered.
- Specify the frequency of the problem.
  - A one-time or occasional fault

    State the exact date and time of the fault. This data helps in finding the needed log files.
  - A frequent fault

    Describe exactly how often the fault occurs.
- Specify the reproducibility of the problem.
  - A reproducible fault.

    Attach a step-by-step description of how to reproduce the fault, or under which circumstances the problem occurs.

  - A non-reproducible fault.

    Describe the circumstances before the fault occurred, and what happened after the fault took place. For example, XCRP Switchover, core dump generated, and so on.

- Describe the effects of the fault. For example, whether it affected traffic or O&M.

- If needed for the handling of the case, include a logical picture of the network diagram showing the direct environment of the affected node. For example, interfaces to which the node is directly connected.

ATTACHMENTS

Describe the file name and format of all attachments. Always include the mandatory files as described in Section 3.1 on page 4 and, when necessary, the data described in Section 4 on page 6.

MEASURES

- Describe if it was possible to stabilize the node by manual intervention, for example, with a reload.

- Provide a description of a possible work-around, including the commands used, if available.

3.1 Mandatory Logs and Data

The logs and data described in this section must always be included in the CSR.

System Log Files (/var/log/messages)

Collect system logs from both the active and standby XCRP cards to attach to your CSR. The files are named **`messages.`*`x`*`.gz`**.; they can be found in the **`/var/log`** directory through NetBSD shell mode.

The log file must include the time of the failure. Time stamps before and after the event occurred must also be included in the CSR. It is important to verify exactly in which file the actual failure is, since the `active message log` file is overwritten after a while. For example, the file can be in `/var/log/messages.2.gz` instead of `current message log`.

Verify the logging configuration on the router by collecting the output of the **`show configuration log`** command.

Crash Files From Both Active and Standby XCRP cards

Verify if related core dumps were generated at the time of the problem, by entering the following commands:

- **`show crashfiles`**
- **`show process crash-info`**

Transfer the files in binary mode from the router and include an md5 checksum of the original file.

Output of the show tech-support Command

The output of the **`show tech-support`** command must be included in the CSR.

Before troubleshooting or performing any recovery steps, run the **`show tech-support`** command (in exec mode) without any keywords on both the active and standby XCRP cards.

The basic command is a macro that runs **`show`** commands in the following areas:

- Startup and software revision
- System hardware
- Configuration
- Core system statistics
- Process and memory status and crashes
- Core system processes
- IP routes
- System logs
- Subscribers (basic)
- Shared memory routing
- DHCPv6

If you know that your problem is related to one of the following other SmartEdge hardware or processes, you can also collect the output of the command with an appropriate keyword; see Section 4 on page 6:

AAA

ASE

ATM

BFD

BGP

Database (RDB)

DHCP

DOT1Q

FLOWD

GRE

IGMP

IPV6

IS-IS

L2TP

LDP

Mobile-IP

OSPF

OSPF3

PIM

PPP

PPPoE

QoS

SNMP

3.2 Acceptable Compression Formats

Note: Ericsson only accepts the following compressing programs:

- Compressed tar (*.tar)
- gzip’d tar (*.tar.gz)
- win zip (*.zip)

4 Collecting Data Based on Problem Type

For more specific problems, collect the output of the following commands as needed to attach to the CSR, depending on the symptom of the fault.

The **`show tech-support`** command includes optional keywords to collect troubleshooting data about many SmartEdge OS modules or the ASE card. To collect data for specific problems, use the command (in exec mode) with an appropriate keyword that runs show commands for the module.

The command has the following syntax:

```
show tech-support [aaa | ase | atm | bfd | bgp | dhcp |
dot1q | flowd | gre | igmp | ipv6 | l2tp | ldp | mobile-ip
| ospf | ospf3 | pim | ppp | pppoe | qos | rdb | snmp]
```

For example, if you know your problem is related to PPP subscribers, enter the **`show tech-support ppp`** command.

Use the following commands to obtain additional information when a problem or outage occurs at the customer node. See the appropriate command reference guide for an explanation of the command syntax.

Note: Because the output of these commands is intended for use by the support engineers, the format might differ from typical **`show`** command output and might not be readable.

Warning!

Some **`show card`** commands might impact card performance.

- *show card*
- *show card acl log*
- *show card adjacency*
- *show card atm table*
- *show card circuit*
- *show card clips*
- *show card dot1q table*
- *show card fib*
- *show card ism*
- *show card link group*
- *show card mpls*
- *show card nat*
- *show card packet local statistics*
- *show card port*
- *show card ppp*
- *show card pppoe*

- *show card qos*
- *show card traffic*
- *show ism circuit*
- *show ism global*
- *show ism interface*
- *show ism linkgroups*
- *show log events*

5 Severity Levels

It is mandatory to state the severity of the CSR. The correct severity ensures that critical problems are fixed before less critical problems, therefore it is very important to apply the following guidelines.

If the priority is not clear to both the First Line Support (FLS) and the Second Line Support (SLS), they analyze it and decide on the severity. The FLS can increase priority due to commercial reasons at any time.

There are four types of severity, Emergency, High, Medium, and Low, described in the following subsections:

5.1 Emergency

Examples of emergencies are the following:

- Complete system failure – the system does not handle any traffic and a manual intervention is needed to restore the system.
- A major disturbance in the system's functionality – capacity is decreased by more than 30% of the core functionality of the system.
- Billing or charging function stops working or is seriously affected.
- Complete loss of I/O, provisioning, or communication for business critical systems.
- Critical functionality impacting customer business is not working.
- System startup or re-boot functionality fails.

The following problem types are not considered to be emergencies:

- Consultation requests.
- Configuration questions.
- Documentation problems.
- Change/improvement requests.

5.2 High

Examples of high severity problems are the following:

- Major fault or disturbance that affects a specific area of functionality, but not the whole system.
- A situation that is likely to result in an emergency.
- Major problems or disturbances that require immediate action, such as large restarts or a failure affecting billing.
- The failure affects connection with other operators.
- The system crashes or hangs.
- Critical functionality is not available.

5.3 Medium

Medium severity problems have minor customer impact.

Examples of medium severity faults are the following:

- Non-recurring small or large restarts where the system recovers automatically.
- Questions regarding operation and maintenance.
- Documentation errors that cause handling errors.

5.4 Low

Low severity CSRs must not be related to any fault in the end-customer's network or network elements.

See the SLS for general consultation.

Examples of low severity faults are the following:

- Questions about network expansion.
- Review of documents.
- Minor documentation errors.
- Configuration consultation.