ERICSSON

SmartEdge OS Release 11.1.2.4

NETWORK IMPACT REPORT

11/109 48-CRA 119 1170/1 Uen A

Contents

1 Introduction

The Network Impact Report (NIR) describes how the current release of the SmartEdge® OS, with new and changed features, differs from the previous release of the SmartEdge OS and how this affects the operator's overall network, including all affected products and functions.

1.1 Purpose

This document provides sufficient information at an early stage to Ericsson system operators to help them plan the introduction of new products and upgrades to their networks. This document is intended for personnel responsible for planning, implementation, and product handling of the SmartEdge router, the SmartEdge Border Gateway Function (BGF), and the SM router.

This is a living document and subject to change during the development of the new release.

This document applies to both the Ericsson SmartEdge® and SM family routers. However, the software that applies to the SM family of systems is a subset of the SmartEdge OS; some of the functionality described in this document may not apply to SM family routers.

For information specific to the SM family chassis, including line cards, refer to the SM family chassis documentation.

For specific information about the differences between the SmartEdge and SM family routers, refer to the Technical Product Description *SM Family of Systems* (part number 5/221 02-CRA 119 1170/1) in the **`Product Overview`** folder of this Customer Product Information library.

1.2 Related Information

Trademark information, typographic conventions, and definition and explanation of acronyms and terminology can be found in Reference [2] and Reference [3].

1.3 Revision Information

Other than editorial changes, this document has been revised as follows:

Table 1 Revision Information

Rev	Date	Description
A	March 07, 2012	First edition.

2 General Impact

This section describes the general impact due to the introduction of this release of the SmartEdge OS.

New hardware is required for several of the new features; see individual features for specific information.

2.1 Capacity and Performance

This section provides information about capacity and performance.

2.1.1 Subscriber Capacity

No changes to subscriber capacity occurred in this release.

2.1.2 Network Performance

No changes to network performance occurred in this release.

2.2 Hardware

There is no new or changed hardware in this release.

2.3 Implementation

This section describes the minimum software requirements for implementing a new revision of the SmartEdge OS and provides release-specific upgrade information.

For detailed software installation and upgrade instructions, see Reference [1].

2.3.1 Upgrade Paths

The system can up be upgraded to the SmartEdge OS Release 11.1.2.4 from Release 6.2, Release 6.4, Release 6.5, Release 11.1.1.1, Release 11.1.2.1, and Release 11.1.2.3.

However, keep the following in mind:

- Release 11.1 does not support PPA1-based line cards. PPA-1 based line cards can still be installed and detected in SmartEdge chassis, but the SmartEdge OS does not recognize and initialize them to a usable state.
- Release 11.1 does not support the XCRP3 Controller card.

If your system does not include this deprecated hardware, you can upgrade directly to this release. For systems running the deprecated hardware, upgrade to this release:

- If your current software release supports the newer PPA and XCRP cards, upgrade your hardware. Then, upgrade your software to Release 11.1.
- If your current software release does not support the newer PPA and XCRP cards, move to an intermediate release that does (for example, Release 6.2.1.7). Using that release, upgrade your hardware. Then, upgrade your software to Release 11.1.

2.3.2 Required System Components

The following system components are required in this release.

2.3.2.1 Required Boot ROM Versions

This release requires the boot ROM versions listed in the following table.

Table 2 Required Boot ROM Versions

Card Type	Version	Filename
XCRP4 SMRP2	2.0.2.66	OFW-XC4-2.0.2.66.fallback.md5
SmartEdge 100 Controller	2.0.1.4	OFW-se100-2.0.1.4.primary.bin
ASE	2.0.2.66	OFW-ASE-2.0.2.66.fallback.md5
ASE2	2.0.2.66	OFW-ASE-2.0.2.66.fallback.md5
SSE	2.0.2.65	OFW-FSSB-2.0.2.65.ofwbin.md5

2.3.2.2 Required Minikernel Versions

This release requires the minikernel versions listed in the following table.

Table 3 Required Minikernel Versions

Card Type	Version	Filename
XCRP4 SMRP2	11.7	MINIKERN_RBN64-xc4.p11.v7
SmartEdge 100 controller	2.7	se100-minikernel.p2.v7.bin
ASE	13.10	MINIKERN_ASE64-ase.p13.v10
ASE2	13.10	MINIKERN_ASE64-ase.p13.v10
SSE	N/A	N/A

2.3.2.3 Required FPGA Versions

This information is not available at this time. Please contact your technical support representative for this information.

2.3.3 Licenses

No new licenses are added in this release.

2.3.4 Upgrade Alerts

This section identifies situations that require additional steps or may affect your system before you upgrade to this release.

In addition, before you upgrade, check for any relevant security notifications on the Ericsson E-business portal at https://ebusiness.ericsson.net.

Stop!

The Advanced Services Engine (ASE) card and the SmartEdge OS must both be running the correct version of the boot ROM. To avoid a serious equipment outage in the field, if you are running SmartEdge OS Release 6.2.1.5 or later on either the ASE or the SmartEdge OS system, DO NOT DOWNGRADE to 6.2.1.4 or earlier. If you must downgrade, contact your support representative for an equipment-safe procedure. Downgrading from these releases can cause permanent damage to the ASE.

2.4 Interface

This section describes interface changes between the existing and new revisions of the SmartEdge OS that may require changes to the operators' systems, technical plans, training of network operator personnel, and so on.

2.4.1 Inter-Node Interface

No changes to inter-node interfaces occurred in this release.

2.4.2 Man-Machine Interface

No changes to man-machine interfaces occurred in this release.

2.5 Memory

In general, memory usage in the base system, increases slightly from release to release due to changes for new software and hardware features.

From image to image, higher memory usage may occur across applications such as BRAS, Layer 2 to Layer 3 operation, DPI, and IPsec. This is typically due to support for new features or infrastructural changes in the release. Memory increase may also vary based on configuration and which features are enabled.

2.6 Operation

This section describes major changes between the existing SmartEdge OS and new revisions that affect the daily operations of the network operator.

2.6.1 BRAS and Metro Ethernet Operation

This section describes impacts to the Broadband Remote Access Server (BRAS) Market Application on the SmartEdge router and Metro Ethernet features for the SM family of routers.

2.6.1.1 Support for Fragmentation in Carrier Grade NAT

This release provides support for IPv4 fragmented traffic within the Carrier Grade NAT feature. The system now supports processing fragmented traffic, including out-of-order fragments, for both NAT inbound and NAT outbound traffic. To protect the system against fragmentation-based DoS attacks and related malformed packet attacks, static limits have been placed on the amount of resources that are used to process fragmented traffic. In determining whether fragmented traffic is malicious, the system also tracks traffic patterns, including the number of sources from which fragmented traffic is arriving, and

the number of out-of-order fragments, and whether the fragment forms part of a tiny fragment attack. The supported fragmented packet length is a minimum of 220 bytes (including the header).

This feature is supported for UDP, TCP, and ICMP traffic, except ICMP error messages, where the headers of the original packets are repeated, and which generally are small enough that fragmentation is not required. For ICMP error messages, if the original outbound datagram was fragmented, reverse ID mapping is not performed.

This feature was designed for traffic containing 1% or fewer fragmented packets and is supported for the following carrier grade NAT configurations:

- Dynamic NAPT with all types of pools: paired, multibind, and logging
- Destination NAT
- Port limiting and Call Admission Control

This feature is also available over LAG and LNS.

First fragments of L4 fragments are dropped if they match an already-stored fragment.

Fragmentation processing for NAT is performed on the line card facing the access network. To be able to route inbound fragmented traffic from the trunk to the access card, the routes must not contain Layer 4 information. This means that port-based routing cannot be used together with this feature. Since port-based routes are created for external IP addresses defined in a NAT pool, if fragmentation support is enabled in a particular context, no port block ranges may be defined for NAT pools until fragmentation support is disabled.

To minimize the chance of a fragment ID collision (where two hosts behind the same NAT device use the same ID and their internal address gets mapped to the same external address), ID mapping is performed in the outbound direction.

Fragmentation support can be enabled and disabled at the context level, using the [**no**] **nat fragments** command in context configuration mode. Fragmentation can be enabled under the following conditions:

- There is no configured NAT pool with a port block range in the context.
- There is no bound NAT policy in the context.
- There is no bound NAT pool (that is, a NAT pool which is referenced by an already-bound NAT policy) in the context.

Fragmentation can be disabled under the following conditions:

- There is no bound NAT policy in the context.
- There is no bound NAT pool in the context.

2.6.1.2 More Efficient Memory Preallocation in Paired Carrier Grade NAT Mode

To improve performance, the system preallocates memory for NAT pools. In paired mode, which uses more pools, the system's method of preallocating memory did not work effectively for low oversubscription rates. Specifically, the low and high "watermarks" used by the system to control the amount of unused, but preallocated, memory sometimes caused the card to approach the number of supported translations and approach its memory limits. In this release, the system uses a more effective method of calculating the amount of memory to preallocate in paired mode, such that low oversubscription rates do not cause this problem. The system supports two million translations per line card (PPA2 and PPA3).

Note: Paired and non-paired configurations on the same line card is not recommended, as there are special cases where translation creation performance is negatively affected when paired and non-paired configurations are mixed.

2.6.1.3 PPA Feature Support

Note: For information about which traffic cards support each PPA version, see the device hardware guides.

Table 4 describes PPA support for features described in this section.

Table 4 PPA Feature Support

Feature	PPA2	PPA3	Notes
Carrier Grade NAT Fragmentation Support	Yes	Yes	Supported on PPA2 ATM and Ethernet line cards, and PPA3 Ethernet line cards.
More Efficient Memory Preallocation in Paired Carrier Grade NAT Mode	Yes	Yes	

2.6.2 Border Gateway Function Operation

There is no impact to the Border Gateway Function Operation in this release.

2.6.3 DPI Operation

There is no impact to the Deep Packet Inspection (DPI) Application in this release.

2.6.4 Platform Operation

This section describes impacts to Layer 2/Layer 3 and Infrastructure functionality.

2.6.4.1 Card Identifier Spoofing

To streamline operations in some deployments, this release provides a utility function that allows you to "spoof," or alias the identifier string of two Gigabit Ethernet DDR line cards with the identifier strings of two legacy FCRAM predecessor cards. When this option is configured, the **`show hardware`**, **`show chassis`**, and **`show card`** commands, as well as SNMP operations for the ENTITY MIB (such as SNMP GET, GETNEXT, and GETBULK) return the FCRAM card identifier strings instead of the DDR card identifier strings. All optional keywords for these commands also display the FCRAM identifier strings instead of the DDR card identifier strings.

DDR card identifier strings are spoofed only if a DDR card is present in the slot but an FCRAM card is configured.

This command is available for the SmartEdge router and SmartEdge BGF. It is not available for the SM router.

Table 5 shows the spoofed DDR cards and the corresponding FCRAM identifier strings returned or displayed by the system.

Table 5

Actual ("Spoofed") Identifier		Identifier Returned by the System	
`10ge-oc192-1-port`	10-port Gigabit Ethernet DDR	**`10ge-1-port`**	10-port Gigabit Ethernet 1020
`ge2-10-port`	1-port 10 Gigabit Ethernet/OC-192 c DDR	**`ge-10-port`**	1-port 10 Gigabit Ethernet

This feature is enabled during upgrade. To enable this feature, perform the following steps:

1 Insert the cards in the chassis.

2 Upgrade the system to this release.

3 Enable the card identifier spoofing feature, by issuing the following command in the local context in global configuration mode

```
[local]Ericsson(config)#ddr2fcram
```

4 Restart the SNMP process, using the **`process restart snmp`** command.

To disable this feature, issue the **`no ddr2fcram`** command in the local context in global configuration mode and then restart the SNMP process, using the **`process restart snmp`** command.

2.6.4.2 PPA Feature Support

Note: For information about which traffic cards support each PPA version, see the device hardware guides.

Table 6 describes PPA support for features described in this section.

Table 6 PPA Feature Support

Feature	PPA2	PPA3	Notes
Card Identifier Spoofing	Yes	No	Supported only for the 1-port 10 Gigabit Ethernet/OC-192c DDR and 10-port Gigabit Ethernet DDR line cards.

2.7 Obsolete Features

No features were removed, replaced by others, or renamed in this release.

2.8 Other Network Elements

No other network elements added to this release.

2.9 Other Impacts

There are no other impacts in this release.

3 Summary of Impacts Per Feature

This section summarizes the impact of each feature on the system. (For specific information about the impact of individual features, see the description of the feature in Section 2.6 on page 5.) It is organized by the Market Applications supported by the SEOS. The description of impacts is as follows:

- "Major Impact" means one or more of the following:
  - The feature includes an incompatible change, such that another node requires an update.
  - New hardware is required to use the feature.

- "Minor Impact" means that the feature includes changes that affect other nodes but with additional configuration, the previous behavior can be retained.
- "No Impact" means that the feature has no impact on the system.
- "Basic" means that the feature is enabled by default.
- "Optional" means that the feature requires an additional license or configuration.
- "New" means that the feature is new.
- "Enhanced" means that the feature is enhanced.

3.1 Broadband Remote Access Server and Metro Ethernet

Table 7 Summary of Impacts

Feature	**Impact**	**Basic or Optional** **New or Enhanced**	**Relation to Other Features or Nodes**
Carrier Grade NAT Fragmentation Support	No Impact	Optional Enhanced	Needs to be enabled by configuration.
More Efficient Memory Preallocation in Paired Carrier Grade NAT Mode	No Impact	Basic Enhanced	

3.2 Border Gateway Function

There is no impact to the Border Gateway Function Operation in this release.

3.3 Deep Packet Inspection

There is no impact to the Deep Packet Inspection (DPI) Application in this release.

3.4 Platform

Table 8 Summary of Impacts

Feature	Impact	Basic or Optional New or Enhanced	Relation to Other Features or Nodes
Card Identifier Spoofing	No Impact	Optional New	

4 Additional Information

This section describes additional information, including new or changed documentation.

4.1 New Documentation

With this release, no documents have been added to the SmartEdge router documentation library.

4.2 Obsolete Documentation

With this release, no documents have been removed from the SmartEdge router documentation library.

Glossary

ASE
Advanced Services Engine

ATM
Asynchronous Transfer Mode

BGF
Border Gateway Function

BRAS
Broadband Remote Access Server

CLI
command-line interface

DoS
Denial of Service

DPI
Deep Packet Inspection

FPGA
Field-Programmable Gate Array

ICMP
Internet Control Message Protocol

IP
Internet Protocol

iPPA
Processing ASIC

IPv4
Internet Protocol Version 4

IPv6
Internet Protocol Version 6

L2TP
Layer 2 Tunneling Protocol

LAG
link aggregation group

LNS
L2TP Network Server

MDU
memory data units

MIB
Management Information Base

NAPT
Network Address and Port Translation

NAT
Network Address Translation

PPA
Packet Processing ASIC

SGC
Session Gateway Controller

SNMP
Simple Network Management Protocol

TCP
Transmission Control Protocol

UDP
User Datagram Protocol

XCRP
Cross-Connect Route Processor

Reference List

SmartEdge OS Software (EN/LZN 783 0011/1)

[1] *Installing the SmartEdge OS*, 1/190 47-CRA 119 1170/1

Other CPI

[2] *SmartEdge Border Gateway Function Survey*, 155 13-CRA 119 1170/1

Standards and Recommendations

[3] *Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications, 3GPP TR 21.905*