ERICSSON

Advanced Services Infrastructure Overview

TECHNICAL PRODUCT DESCRIPTION

1/221 02-CRA 119 1170/1-V1 Uen E

Contents

1 Introduction

This document describes the Advanced Services Engine (ASE) card and the software infrastructure that supports the applications that can be installed and run on these cards.

The 3GPP Long Term Evolution (LTE) project and the System Architecture Evolution (SAE) effort for the common IP based core network are addressing these needs through the 3GPP Release 8 standardization. This evolved architecture referred as Evolved Packet Systems (EPS) will be capable of providing data rates of 50/100 Mbps up-link/down-link service for users and supporting mobility across various access technologies.

1.1 Scope

Each ASE card contain two Advanced Service Processors (ASPs) that provide additional processing power on a SmartEdge® router. Each ASP can be configured to provide ASE-based services, support high availability, and support load balancing. This document describes ASE card functionality and placement in a SmartEdge router. In addition, it describes how to use ASP pools and ASP groups to distribute the processing capabilities of the ASPs, provide load balancing when multiple ASPs are installed, and support resiliency when excess ASPs are available.

1.2 Target Groups

This document is intended for network planners responsible for the design of advanced network services that use the SmartEdge router and for operators of the SmartEdge OS responsible for entering the configuration on individual SmartEdge routers.

2 ASE Card Description

The ASE card provides advanced services that are beyond the scope of the terminating and forwarding capabilities provided by line cards. ASE-based services available in this release include Security Service, which provides support for IP Security (IPSec) Virtual Private Network (VPN) and Application Traffic Management.

Unlike a line card, an ASE card does not have any input/output (I/O) interfaces that are used for traffic processing; it receives all traffic it processes through the backplane. The ASE card provides additional processing to specific flows after ingress processing is completed on an incoming line card but before the flows are forwarded to an outgoing line card for egress processing.

Security features on the ASE card protect the network at its edge, ensure minimal network disruption, and provide secure tunnels for end-user applications. Using Deep Packet Inspection (DPI), the ASE card can identify and process point-to-point (P2P) applications, and provide a more efficient and secured network operation. You perform IP Security (IPSec) configuration, management, and reporting with NetOp Element Manager System.

Several ASE cards can be deployed in a SmartEdge chassis, and one or more line cards can send traffic to them. Unlike a line card, which processes the traffic it receives, an ASP on an ASE card processes specific traffic flows forwarded to it, regardless of the line card that received the flow. You use ASP pools and ASP groups to specify the ASE-based service to be provided, balance the processing load, and provide high availability of services by the ASE card. ASP pools and ASP groups allow you to use more than one ASP on more than one ASE card to provide the same set of ASE-based services to specific traffic flows and to provide fail-over support. For more information, see Section 3 on page 5.

2.1 Supported Routers

The following SmartEdge routers support the ASE card.

- **SmartEdge 400 router**—The SmartEdge 400 router is a 6-slot node that manages packet traffic to provide customer access to the IP network and to aggregate traffic from other routers in the IP network.
- **SmartEdge 600 router**—The SmartEdge 600 router is a 8-slot node that manages packet traffic to provide customer access to the IP network and to aggregate traffic from other routers in the IP network.
- **SmartEdge 800 router**—The SmartEdge 800 router is a 14-slot node that manages packet traffic to provide customer access to the IP network and to aggregate traffic from other routers in the IP network.
- **SmartEdge 1200 router**—The SmartEdge 1200 router is a 14-slot node that manages packet traffic to provide customer access to the IP network and to aggregate traffic from other routers in the IP network.
- **SmartEdge 1200H router**—The SmartEdge 1200H router is a high-power variant of the SmartEdge 1200 router that supports a greater number of PPA3-based cards.

2.2 Card Placement

The ASE card can be installed in any slot other than the two slots reserved for Cross Connect Route Processor (XCRP4) Controller cards. The XCRP4 manages and monitors packet traffic, provides access to the Command-Line Interface (CLI), provides redundancy protection (one card is designated for this function), and manages general node operations.

The number of ASE cards that can be provisioned in a SmartEdge chassis is constrained by the power limitations of the chassis and the power consumption of the XCRP4 and line cards that are installed. The ASE card power consumption is rated at 175.20 watts.

For ASE card installation instructions, see Reference [1].

2.3 Service Selection

While the ASE card is designed to be a flexible high performance card that can be used to provide different types of ASE-based services, only one service can be provided on a given ASP at one time. During configuration, Security Service is set with a service type **`security`** .

Multiple security applications can map to the Security Service and may run concurrently on the same ASP. Currently, IPSec VPN and Application Traffic Management are the two applications supported by the Security Service.

3 ASP Pools, ASP Groups, and Service-Enabled Contexts

ASE-based services are provided at the Advanced Service Processors (ASP) level. To provide these services at the ASP level, you must define ASP pools. An ASP must be a member of an ASP pool to provide these services.

We use logical concepts for all installed ASPs to be configured to provide separate instances of ASE-based services.

- ASP pools

  An ASP pool is a set of ASPs on a SmartEdge router and identifies the service provided by those ASPs. One or more ASP pools can be configured for a given service. ASPs from the pool are dynamically allocated to the ASP groups associated with the pool. Excess ASPs in the pool act as backups to active ASPs to provide high availability for services.

  Note: The ASPs of the ASE card must be configured under an ASP pool before the processor can be brought up.

- ASP groups

  An ASP group specifies the number of ASPs required by the group and the ASP pool to use. The actual ASPs that will be used by an ASP group are dynamically allocated by the software. Load balancing is available when more than one ASP is allocated to a group.

- Service-enabled contexts

  A service-enabled context identifies the ASE-based service that is provided to the traffic carried on the context and specifies the ASP group that provides the service. You can configure more than one context with the same ASP group.

For more information, see Reference [2] or Reference [3].

Figure 1 shows the step-by-step sequence how an ASP is assigned to process the traffic on a service-based context.

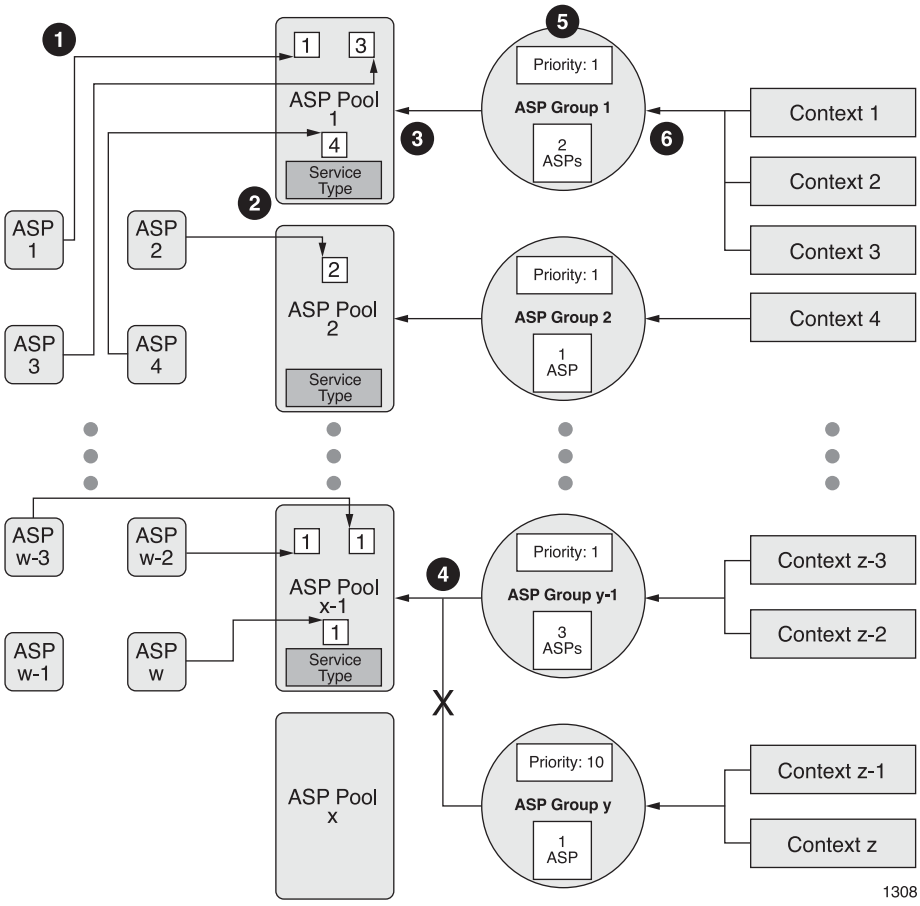

Figure 1 ASP Pools and Groups Mediate Between ASPs and Service-Enabled Contexts

1 An ASP on an ASE card configured on a SmartEdge router can be assigned to an ASP pool.

2 The ASP pool also specifies the ASE-based service that is provided by all the ASPs that are assigned to it.

3 An ASP group is associated with only one ASP pool.

4 More than one ASP group can be associated with the same ASP pool.

5 The ASP group also identifies the number of ASPs required to process traffic, and has a priority value that is used to determine ASP assignment when there are fewer ASPs than requested by all the groups in the pool.

6 A context is associated with one ASP group. Multiple contexts can be associated with the same ASP group.

Traffic for a given context is load balanced across the ASPs assigned to the ASP group with which the context is associated.

3.1 High Availability

High availability mechanisms enable the handling of runtime fault conditions by switching over to a backup ASP or by rebalancing the traffic load among existing active ASPs. When backup ASPs are available, existing services on an active ASP that fails are reestablished on one of the backup ASPs. Active and backup ASPs both contain the current configuration; however, IPSec tunnels will go down briefly and some traffic loss occurs during the switch from a failed active ASP to a backup ASP, which can take several seconds to complete.

For more information, see Reference [4].

3.2 Load Balancing

Load balancing defines how traffic is distributed across different ASPs in a chassis. Load balancing can be viewed at two levels: a high level that is defined through configuration and a low level that is controlled by the SmartEdge OS.

With the NetOp™ EMS client or the SmartEdge CLI, you create multiple ASP pools, allocate ASPs to the pools, and map the pools to specific services. You then create ASP groups, assign groups to each pool, and map contexts to ASP groups. After completing all of these tasks, contexts and associated services are mapped to a specific ASP group.

For a given context, IPSec tunnels and subscribers requiring application traffic management services, are load balanced across the available ASPs in the ASP group to which the context is bound.

3.3 Configurable Drop/Bypass Behavior

Drop/bypass configuration handles runtime fault conditions when there is no operational ASP to which to forward traffic requiring advanced services. Currently, the only application that supports configurable drop/bypass behavior is Application Traffic Management. For IPSec, if the tunnel is down due to lack of ASP resources, the traffic will be dropped (unless an alternate route is available).

For instance, if a SmartEdge chassis has only one ASE card and the ASE card is physically removed or develops a fault condition, then there will be no operational ASP to which traffic can be forwarded. Application Traffic Management provides two options.

- Drop
- Bypass the ASP (the default setting)

Drop/bypass behavior cannot be configured for policy configuration.

4 Guidelines for Defining ASP Pools and ASP Groups

You must define ASP pools and ASP groups to access ASE-based services provided by an ASE card. Together, an ASP pool and ASP group are used to identify the ASE-based service to provide, and, when multiple ASPs are employed, to support high availability and load balancing for all ASE cards. For an introduction to the concepts of ASP pools and ASP groups, see Section 3 on page 5.

You can configure multiple ASP pools on a SmartEdge router; however, the sum of all ASPs across all ASP pools for each type of SmartEdge router cannot exceed the total shown in the right-most column of Table 1.

Table 1 Maximum Number of ASPs by Type of SmartEdge Router

Chassis	Total Slots	Subtract Controller Cards	Subtract Minimum Number of Line Cards	Number of Available Slots	Multiply by Number of ASPs per ASE Card	Maximum Number of ASPs Possible
SmartEdge 400	6	2	1	3	2	6
SmartEdge 600	8	2	1	5	2	10
SmartEdge 800	14	2	1	11	2	22
SmartEdge 1200	14	2	1	11	2	22
SmartEdge 1200H	14	2	1	11	2	22

Note: The information in this table represents theoretical limits. To ensure proper operation of your system, always load your chassis to within the power and thermal (cooling) budget for that particular chassis.

General Guidelines

- An ASP can belong to only one ASP pool.
- ASPs assigned to an ASP pool must share the same system-level attributes, such as service type.
- An ASP pool defines the ASE-based service provided and lists the ASPs that are available to provide the service.
- Multiple pools may be configured for the same service.
- An ASP group identifies the pool and the number of ASPs from the pool that must be dynamically assigned to provide the service.
- The actual number of ASPs assigned to the group depends on the priority of the group relative to other groups in the same pool and the total number of available ASPs in the pool. Although configuration allows you to assign

fewer ASPs to a pool than is required by all of the groups referencing the pool, we strongly recommend that you allocate sufficient ASPs to a pool to meet the requirements of all groups referencing the ASP.

- Ensure that the sum of the ASPs specified in all of the groups referencing the same pool is less than the number of ASPs in the pool. This enables the excess ASPs to function as backup ASPs and provides for a fast switch over to the backup ASPs in the event of an ASP or ASE card failure.

- More than one ASP group can reference the same ASP pool.

With the ASP pool defining the service and the ASP group referencing the ASP pool and specifying the number of ASPs to provide service, the following functionality is enabled:

- High availability in case of operational failure

  When more than one ASP is associated with an ASP pool, excess ASPs (the number of ASPs in the ASP pool minus the total number of ASPs across all ASP groups referencing it) become backup ASPs. Backup ASPs are available to replace any active ASP in the ASP groups referencing the ASP pool in case of an ASP failure.

  When an ASP in an ASP group fails, the failed ASP is replaced by a backup ASP if one is available; the backup ASP takes over the role of the ASP that failed. When the original failed ASP recovers, it becomes a backup ASP.

- Load balancing

  When multiple active ASPs are processing traffic, the traffic belonging to multiple contexts and across all the ASPs in an ASP group is automatically balanced across the active ASPs belonging to that group.

You create an ASP pool to associate specific ASPs with a particular ASE-based service. Figure 2 shows the relationships between ASPs and ASP pools.

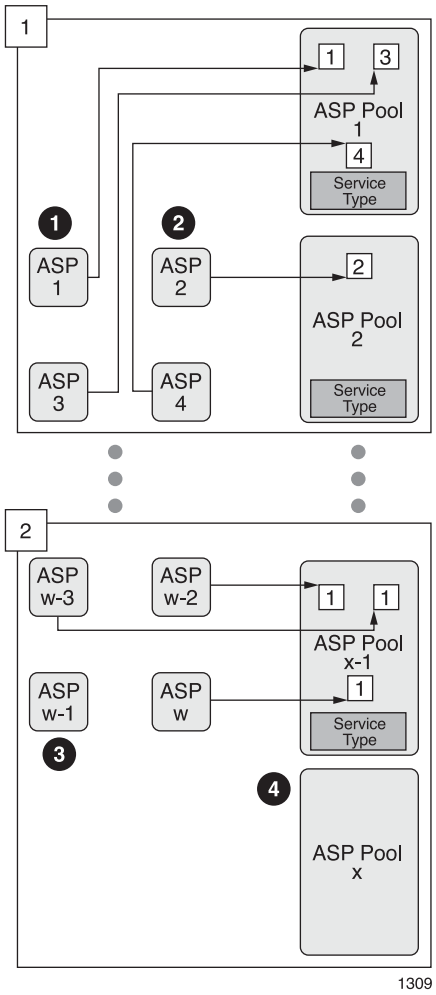

Figure 2 ASPs Are Assigned to ASP Pools

1 Several ASPs can be assigned to the same pool. An ASP pool assigned more than one ASP can support high availability and load balancing, depending on how many ASPs are allotted to ASP groups for traffic processing.

2 Although an ASP pool assigned only one ASP cannot provide high availability and load balancing, it can provide traffic processing for an ASP group responsible for several low-traffic contexts.

3 An ASP that is not assigned to an ASP pool cannot process traffic that needs Security services.

4 An ASP pool that is not assigned any ASPs cannot support the processing of traffic that needs Security services.

You create an ASP group to define the number of ASPs to allocate to an ASE-based service, specify the ASP pool that provides the ASPs and the advanced service, and a priority to use for ASP allocation. Figure 3 shows the relationships between ASP pools and ASP groups.

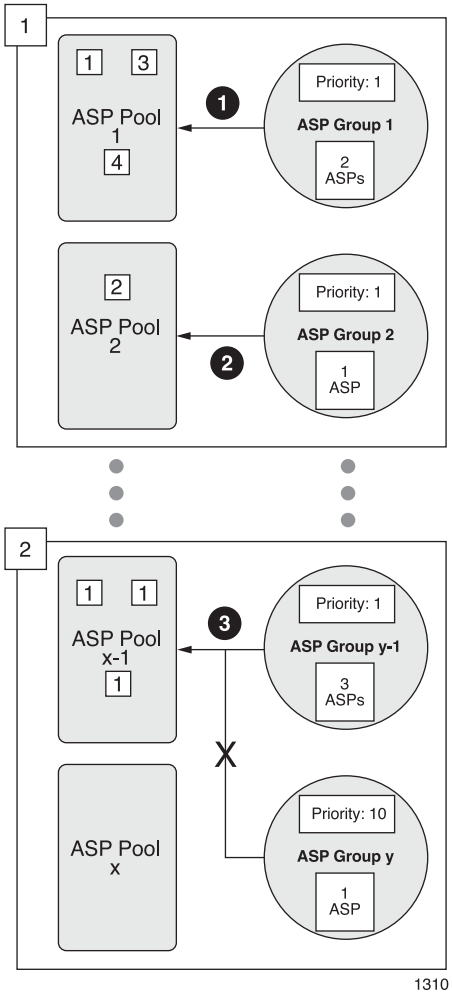

Figure 3 ASP Groups Request ASPs From ASP Pools

The number of active ASPs in an ASP pool is determined by the number of ASPs requested by all the ASP groups associated with the ASP pool. Figure 3 shows the following relationships:

1 When the number of ASPs requested by the ASP groups associated with the ASP pool is less than the number of ASPs in the pool, the excess ASPs function as backup ASPs for the pool. The traffic load is balanced across the active ASPs.

2 When the number of ASPs requested by the ASP groups is equal to the number of ASPs enrolled in the pool, the traffic load is balanced across the available ASPs, all the ASPs are active, and no backup ASP is available.

3 When a new ASP group is added to the ASP pool and all available ASPs are already active, no ASPs are assigned to the newly added group regardless of priority. There is no preemption of ASP resources once they have been allocated to an ASP group.

When a new ASP is added to the pool, it is assigned to the ASP group with the highest priority that still needs an active ASP.

Associating service-enabled contexts to ASP groups allows you to flexibly specify the number of active and backup ASPs available to process traffic that needs Security services. Figure 4 shows the relationships between ASP groups and contexts.

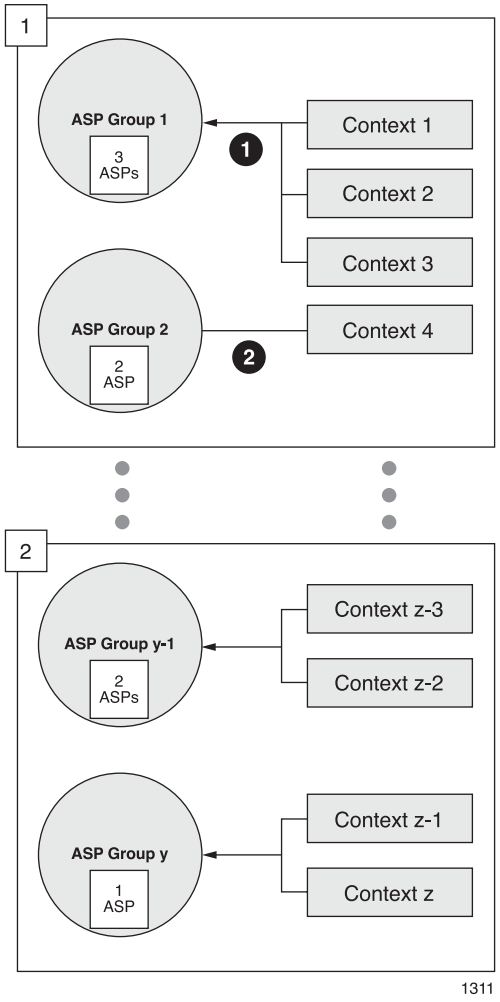

Figure 4 Service-Enabled Contexts Request ASPs From an ASP Group

Figure 4 shows the following relationships:

1 Traffic requiring Security services from multiple contexts can be directed for processing by the ASPs allocated to a single ASP group.

2 Traffic requiring Security services from a single context can be directed for processing by the ASPs allocated to a single ASP group.

Traffic requiring Security services from different contexts can be directed to different ASP groups.

For example, you can ensure sufficient processing power and high availability for traffic requiring Security services for a single context by associating that context to an ASP group that is the only member of an ASP pool with several ASPs. Allocate the required number of active ASPs from the ASP pool to the ASP group to provide the processing power while ensuring that there are additional ASPs available to function as backup; the unallocated ASPs provide the backup capability. Alternatively, you can provide basic processing support without any backup capability for several contexts by associating those contexts to one ASP group, which in turn can belong to an ASP pool with no backup ASPs.

5 High Availability and Load Balancing Deployment Scenarios

Support for high availability and load balancing is provided at the ASP level.

In the simplest case, you can create an ASP pool with one ASP and configure an ASP group that specifies a count of one ASP referencing that ASP pool and assign it to only one context, thereby dedicating the ASP to that context. Since no excess ASPs exist in the ASP pool, no backup ASPs are available to provide high availability. Also, because the ASP group specifies a count of one ASP, no load balancing is possible.

Alternatively, you can create an ASP group with multiple ASPs and associate multiple contexts to the ASP group; in this case, the software balances the traffic load belonging to the contexts and across the ASPs in the ASP group. Any excess ASPs in the ASP pool function as backup ASPs.

State synchronization between active and backup ASPs in any scenario is not supported in this release.

Glossary

ASE
Advanced Services Engine

ASP
Advanced Service Processor

CLI
Command-Line Interface

IPSec
IP Security

VPN
Virtual Private Network

Reference List

[1] *Quick Installation Guide for the SmartEdge Advanced Services Engine Card*, 9/153-30-CSA 119 1170/1

[2] *Advanced Services Configuration and Operation Using the NetOp EMS Software*, 1553-CRA 119 1170/1

[3] *Advanced Services Configuration and Operation Using the SmartEdge OS CLI*, 1/1543-CRA 119 1170/1-V1

[4] *Advanced Services Startup, Failure and Recovery*, 1/1553-CRA 119 1170/1-V1