# Advanced Services Startup, Failure, and Recovery

USER GUIDE

## Copyright

## Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

## Trademark List

| | |
|---|---|
| **SmartEdge** | is a registered trademark of Telefonaktiebolaget LM Ericsson. |
| **NetOp** | is a trademark of Telefonaktiebolaget LM Ericsson. |

# Contents

# 1 Advanced Services Startup, Failure, and Recovery

This document describes the behavior of the Advanced Services Processor (ASP) during startup, failure, and recovery. The ASP is the device that provides services on the Advanced Services Engine (ASE) card. Every ASE card has two ASPs. For Security Service, each ASP can be configured to provide separate instances of the Security Service and support for high availability or load balancing.

For Distributed Control Plane (DCP), all ASPs are consumed by the DCP service-type.

**Caution!**

Risk of substantial delay when an ASE card is restarted. An ASE card can take several minutes to complete a shutdown and restart.

# 2 Verifying the Status of ASPs, ASP Pools, and ASP Groups

With the NetOp™ EMS software, use the card active view, ASP pool active view, and ASP group active view to verify the status of ASPs. These views provide a read-only display of the current status of the ASPs on a card, an individual ASP pool, or group; see Reference [1].

With the Command Line Interface (CLI) of the SmartEdge® OS, use the following commands:

- **`show asp detail`**—Lists details for each ASP on all ASE cards.

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

- **`show asp pool detail`**—Lists details for each ASP pool defined.
- **`show asp group detail`**—Lists details for each ASP group defined.

See Reference [2].

The card active view and the **`show asp detail`** command display the following information for each ASP on the card:

- The ASP ID (slot and ASP number)
- Operating state
- Active or backup state
- ASP pool assignment
- ASP group allocation
- Service provided

The ASP pool active view and the **`show asp pool detail`** command display the following information:

- The service assigned to the pool.
- Licensing information.
- ASP groups associated with the pool.
- Location and state of each ASP enrolled in the pool and assigned to ASP groups to provide the assigned service.

The ASP group active view and the `show asp group detail` command display the following information:

- The ASP pool the group is associated with.
- The number of ASPs allocated to the group.
- The location and state of each assigned ASP.

# 3 Managing ASP Failure and Recovery

This section describes how to manage ASP failure and understand the impact an ASP failure can have. It also provides information you can use to minimize that impact.

## 3.1 Handling ASP Failures

An operational ASP may become non-operational due to operator action, software faults, or hardware faults.

All events that render an ASP non-operational (shut down of the ASP, shut down of the ASE card, removal of the physical ASE card, deletion of an ASP configuration, deletion of an ASE card or ASP from the inventory, software faults, failure of the ASE card hardware, and so on) are mapped into either of the following states

- Transient failure: Most ASP failures result in the ASP being marked as being in a transient failure condition. A transient failure condition becomes a permanent failure if a factory-defined interval has elapsed and the ASP has not become operational yet.

- Permanent ASP failure: An ASP failing and not recovering within the factory defined interval. Note that certain failures, such as a card removal may be deemed to be permanent failures immediately without waiting for the factory-defined interval.

The fault handling differs depending on whether a backup ASP is available and whether the failure is transient or permanent:

- If a backup ASP is available, the backup ASP immediately becomes active and takes over the role of the failed ASP.

- If a backup ASP is not available and the failure is considered transient:

  - During the interval that an ASP is considered to be in transient failure condition, the traffic load served by the failed ASP is not rebalanced among other operational ASPs in the ASP group, if there are any. This is done to avoid rebalancing the traffic load at the time of ASP failure and again when the failed ASP recovers. The Internet Protocol Security (IPsec) tunnels remain down until the failed ASP recovers. If an alternate route is available, traffic is rerouted on the alternate route; otherwise IPsec VPN traffic is dropped, or subscriber traffic is subject to the configured drop/bypass behavior. The failed ASP is allowed to recover and:

    - If the failed ASP recovers within the factory-defined interval, the original traffic load is restored to the ASP, and the IPSec tunnels or subscriber sessions are reestablished on the recovered ASP.
    - If the failed ASP does not recover within the factory-defined interval, it is handled as described for permanent failure.

- If a backup ASP is not available and the failure is considered permanent:
  - If there are other ASPs in the ASP group, the traffic on the failed ASP is rebalanced among the remaining ASPs in the ASP group, subject to maximum capacity limits on each ASP. If the capacity limit of all remaining ASPs in the ASP group is reached, then any remaining IPsec tunnels are not brought up and stay down. Likewise, subscriber traffic will be subject to the configured drop/bypass behavior.
  - If there are no other ASPs in the ASP group, the IPSec tunnels remain down until the failed ASP recovers. If an alternate route is available, traffic is rerouted on the alternate route; otherwise IPsec VPN traffic is dropped, or subscriber traffic is subject to the configured drop/bypass behavior.

When an ASP recovers after it is deemed to have permanently failed, or when a new ASP is added to the ASP pool, the ASP is assigned as follows:

- All ASP groups referencing the ASP pool to which the ASP belongs are searched in order of priority to determine if any of the ASP groups have a permanently failed ASP. If yes, the newly operational ASP is made part of that ASP group and the ASP group is rebalanced to distribute the load across all operational ASPs of the ASP group.
- If not, then the newly operational ASP is marked as a backup ASP.

Rebalancing causes IPsec tunnels or subscriber sessions to go down before they are reestablished on the new ASP. In both cases, there is a potential for traffic loss for the affected tunnels or subscribers.

You can use the **`show asp`**, **`show asp group`**, and **`show asp pool`** commands to check the operational state of the ASP, see Section 2 on page 3.

## 3.2 Monitoring for ASP Down Alarms

A critical alarm in raised when an ASP on a configured ASE card goes down for any reason other than an explicit shutdown of the card by a user.

See Table 1 for details about each of the two possible alarms.

*Table 1 ASP Down Alarm Descriptions*

| Description | Severity | Probable Cause | Service Affecting |
|---|---|---|---|
| ASP 1 down | Critical | Processor Problem | Yes |
| ASP 2 down | Critical | Processor Problem | Yes |

ASP down alarms are raised for the slot of the SmartEdge router that contains the ASE card of the failed ASP.

Use the Fault view in the NetOp client to monitor alarms. You can filter this view to show only alarms, and sort the view by severity. The ASP down alarm will appear in the Fault view when Network, or the appropriate proxy or domain, is selected in the network navigator, as well as when the affected SmartEdge router or slot is selected in the object navigator. For more information, see the “Faults” chapter of Reference [3].

When an ASP alarm is raised, details are available to indicate the root-cause of the failure.

```
Source: Card
Severity: Major
Description: ASP 1 missing service association
Service Affecting: TRUE

Source: Card
Severity: Major
Description: ASP 2 missing service association
Service Affecting: TRUE
```

*Example 1 ASP Fault Isolation*

## 3.3 Understanding ASP Failover Behavior

The following examples illustrate many of the possible ASP failover behaviors:

- Example 1: Two ASPs in a pool with one backup ASP

  Configuration:

  - ASP pool: 2 ASPs
  - ASP group 1: ASP count = 1
  - Backup ASPs: 1 ASP

    One ASP is the backup since the pool has two ASPs and the sum of all ASPs from all groups is one; hence, the number of backup ASPs is 2-1=1.

Failure scenario:

The ASP failure occurs in the group:

- The failed ASP is immediately removed from the group.
- The backup ASP is added to the group and becomes active.
- Traffic switches to the newly active ASP.
- The failed ASP recovers and is made the backup ASP for the pool.

- Example 2: Multiple active ASPs with no backup ASPs

  Configuration:

  - ASP pool: 3 ASPs
  - ASP group 1: ASP count = 3
  - Backup ASPs: 0 ASPs

    All ASPs are active; hence, there are no backup ASPs available.

  Failure scenario: ASP failure in Group 1.

  Because no backup ASPs are available, no immediate failover occurs. The failed ASP is allowed to recover. All IPSec tunnels on the failed ASP are brought down. Two cases exist

  - Failed ASP recovers within the factory-defined interval: The failed ASP is made active and traffic again starts to flow to the recovered ASP. No rebalancing is required in this case.
  - Failed ASP does not recover within the factory-defined interval: The failed ASP is removed from the ASP group and is marked as having permanently failed. Traffic originally handled by three ASPs is now handled by the remaining two ASPs, subject to the maximum ASP capacity limits. If the failed ASP recovers subsequently, it is made active and the ASP group is again rebalanced to redistribute the load among three ASPs.

- Example 3: Multiple ASPs in two ASP groups with different priority values and one backup ASP

  Configuration:

  - ASP pool: 6 ASPs
  - ASP group 1: ASP count = 2, Priority = 100
  - ASP group 2: 3 ASPs, Priority = 200
  - Backup ASPs: 1 ASP

Failure scenario: Simultaneous failure of two ASPs, one from each ASP group (for instance, when an ASE card is removed)

Group 1:

- The failed ASP is immediately removed from Group 1.
- The backup ASP is added to Group 1 because Group 1 has higher priority compared with Group 2, and the ASP becomes active.
- Traffic switches to the newly active ASP.

Group 2:

- The failed ASP is immediately removed from Group 2 because an ASP that is physically removed is deemed to have permanently failed.
- Group 2 is rebalanced to distribute the traffic among the remaining two ASPs.

## 3.4 Automatic Software Reset of ASPs

An automatic software reset of an ASP occurs when a critical application or one of the data plane cores fails.

An automatic software reset is triggered when:

- Any data plane core fails.
- Any netbsd application process fails.
- An ASP device is removed from an ASP pool or ASP group.

## 3.5 ASP Shutdown and Reload

You can use the following commands available from the SmartEdge OS to shut down the ASE card or its ASPs and restart the card:

- When deprovisioning an ASE card using **no card** [ ***card_type slot***], you may see the following warning.

```
[local]Redback(config)#no card ase 4

Note: if ASP shutdown is not complete,
de-provisioning of card ase
commit to continue; abort to exit without change

[local]Redback(config)#
```

- **shutdown** [**asp** ***aspNum***]—Issued in config mode at the card level. Shuts down all ASP devices, or the specified ASP device on an ASE card.

  For example, to shut down the ASPs on the ASE card in slot 11, run the following commands:

  ```
  [local]Redback#config
  Enter configuration commands, one per line,
  'end' to exit
  [local]Redback(config)#card ase 11
  [local]Redback(config-card)#shutdown
  [local]Redback(config-card)#end
  ```

  To shut down ASP 1 on the ASE card in slot 11, run the following commands:

  ```
  [local]Redback#config
  Enter configuration commands, one per line,
  'end' to exit
  [local]Redback(config)#card ase 11
  [local]Redback(config-card)#shutdown asp 1
  [local]Redback(config-card)#end
  ```

- **reload card** ***slot***—Issued in exec mode. If the ASP devices are not already shut down, this command shuts down both ASP devices on an ASE card, downloads the software binaries, and then restarts the ASP devices. Otherwise, this command downloads the software binaries and restarts the ASP devices. This command can also be used to recover from certain situations when an ASE card fails to boot and the ASP devices are in an unknown state.

  For example, to restart (or shut down and restart) the ASPs on an ASE card in slot 11, run the following commands:

  ```
  [local]Redback#reload card 11
  The "reload" command will restart the
  card in slot 11
  Do you really want to reload? (y/n) y
  Slot 11: card reloaded successfully
  ```

The shutdown process for all of these commands takes 2 minutes to complete. When you issue a **shutdown** command, a message appears informing you not to physically remove the ASE card from the SmartEdge chassis for at least two minutes. This allows the ASP configurations to be backed up to the flash memory on the ASE card. When reloading an ASE card, ensure that traffic processing is not impacted while the card is out of service.

# Glossary

**ASE**
Advanced Services Engine

**ASP**
Advanced Services Processor

**CLI**
Command Line Interface

**IPsec**
Internet Protocol Security

# Reference List

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

[2] *Security Service Command Reference*, 1/190 80-CRA 119 1170/1-V1

[3] *Fault Management*, 6/1543-CRA 119 1171/1