ERICSSON

Aware Policy-Based Routing Configuration

OPERATION DIRECTIONS

68/1543-AXB 250 10/4-V3 Uen AT

Contents

1 Introduction

This document describes the configuration of the Aware Policy-Based Routing (APR) functionality in the Evolved Packet Gateway (EPG). APR can be used in both General Packet Radio Service (GPRS) and Evolved Packet System (EPS) networks and is supported for both GGSN and Packet Gateway (PGW) Access Point Names (APNs).

1.1 Scope

This document describes how to enable APR in the EPG, and how to configure APR related properties.

For an overview of APR, see *Aware Policy-Based Routing*.

1.2 Target Groups

This document is intended for personnel performing configuration of the EPG. The document is written with the assumption that the reader has basic knowledge of data communication and telecommunication.

2 Prerequisites

Before configuring the APR function, ensure the following prerequisites are met:

- License for the following features are required to enable APR:
  - Aware Policy-Based Routing
  - Packet Inspection and Service Classification (PISC)

  Optional licensed features in the EPG are turned off by default. In order to employ these features in the EPG, licenses must be purchased from Ericsson. For information on how to purchase licenses and enable licensed features, see *Software License Management* or contact the local Ericsson support.
- Both a base APN and a service APN must be configured. Refer to *APN Configuration* for more information.

- A routing instance must be configured for a service APN. Refer to *Routing* for more information.
- Service-Data-Flow IDs (SDF-IDs) must be configured. Refer to *PISC Configuration* and *SACC Configuration* for more information.
- Access Control Rules (ACRs) and Access Control Groups (ACGs) must be configured. Refer to *Gx+ Static Access Control Configuration* or *Gx+ Policy and Charging Control Configuration* for more information.
- The user category and the rule space must be configured. Refer to *SACC Configuration* for more information.

3 Enabling APR

The following actions must be taken to enable APR:

- Configuring service Access Point Names (APNs)
- Mapping a service APN to ACR in a rule space

3.1 Configuring Service APNs

This section describes the configuration of service APNs.

Note: The combination of routing instance and IP address range must be unique for each APN, that is for a base APN as well as a service APN. A service APN is associated with a unique routing instance.
NAT-enabled IPv4 only service APNs can be associated with the same routing instance, but it is not recommended. Using this configuration could cause an EPG exception when overlapped NAT IP addresses are allocated through RADIUS.
APR is not supported on an APN where L2TP or Routing behind MS is configured.

Configure a service APN and associate a routing instance with it by including the following statement:

```
(config) ManagedElement=1,Epg=1,Pgw=1,Apn=serviceApnName
   routingInstance=name
```

For information on configuring routing instances, see *Routing*.

3.2 Mapping a Service APN to ACR in a Rule Space

This section describes the mapping of service APNs with Access Control Rules (ACRs).

Note: An ACR can only be mapped to one service APN in a rule space.

Map a service APN to one or more ACRs in a rule space by including the following statement:

```
(config) ManagedElement=1,Epg=1,Pgw=1,RuleSpace=
name,AwarePolicyBasedRouting=1
   Map=serviceApnName
      accessControlRule=[accessControlRuleId|accessControlRuleIdRan
```

4 Blocking and Unblocking a Service APN

It is possible to block and unblock user session activation on a service APN.

4.1 Blocking a Service APN

Block user session activation on the service APN by including the following statement:

```
(config) ManagedElement=1,Epg=1,Pgw=1,Apn=serviceA
pnName,AwarePolicyBasedRouting=1
   creation=blocked
```

4.2 Unblocking a Service APN

Unblock user session activation by following the instructions below:

1. Unblock user session activation on the service APN by including the following statement:

   ```
   (config) ManagedElement=1,Epg=1,Pgw=1,Apn=servic
   eApnName,AwarePolicyBasedRouting=1
      creation=unblocked
   ```

2. Unblock user session activation on the base APNs as described in *Deleting and Modifying APNs*.

5 Configuring RADIUS Authentication for a Service APN

Configure Remote Authentication Dial-In User Service (RADIUS) authentication for a service APN by following the instructions below:

- Enable RADIUS authentication
- Enable IP Allocation through RADIUS (Optional)
- Configure a RADIUS server

The following sections describe how to perform these actions.

5.1 Enabling RADIUS Authentication

Enable RADIUS authentication by following the instructions below:

1 Block user session activation as described in Section 4.1 on page 3.

2 Enable RADIUS authentication by including the following statement:

```
(config) ManagedElement=1,Epg=1,Pgw=1,Apn=serviceApn
Name,AwarePolicyBasedRouting=1,Radius=1
   Authentication=1
```

5.2 Enabling IP Address Allocation through RADIUS

To enable IP address allocation through RADIUS for Network Address Translation (NAT), see Section 7 on page 8.

5.3 Configuring a RADIUS Server

APR supports inband RADIUS servers. Configure a RADIUS server for the service APN by following the same instructions as for a base APN, described in *RADIUS Configuration*.

Note: RADIUS Multicast is not supported for service APNs.

6 Configuring RADIUS Accounting for a Service APN

Configure RADIUS accounting for a service APN by following the instructions below:

- Enable RADIUS accounting
- Configure a RADIUS server
- Configure RADIUS accounting properties
- Configure accounting start on service access

The following sections describe these actions.

6.1 Enabling RADIUS Accounting

Enable RADIUS accounting by following the instructions below:

1. Block user session activation as described in Section 4.1 on page 3.
2. Enable RADIUS accounting by including the following statement:

```
(config) ManagedElement=1,Epg=1,Pgw=1,Apn=serviceApn
Name,AwarePolicyBasedRouting=1,Radius=1
   Accounting=1
```

6.2 Configuring a RADIUS Server

APR supports inband RADIUS servers. Configure a RADIUS server for the service APN by following the same instructions as for a base APN, described in *RADIUS Configuration*.

Note: RADIUS Multicast is not supported for service APNs.

6.3 Configuring RADIUS Accounting Properties

Configure RADIUS accounting properties for the service APN by following the same instructions as for a base APN, described in *RADIUS Configuration*.

Note: The following RADIUS properties and message attributes are not supported for service APNs:

- Interim update
- Acct-Input-Gigawords
- Acct-Input-Octets
- Acct-Input-Packets
- Acct-Output-Gigawords
- Acct-Output-Octets
- Acct-Output-Packets
- RADIUS-initiated user session termination

In addition, the `apnIdentifier` message attribute can be optionally configured for the service APN in acknowledge mode. For more information, see Section 6.3.1 on page 6.

6.3.1 Configuring the APN Identifier

The `apnIdentifier` is used to choose the value for the `Called-Station-Id` attribute in the accounting requests to the service APN.

To configure the APN identifier, include the following statement:

```
(config) ManagedElement=1,Epg=1,Pgw=1,Apn=servic
eApnName,AwarePolicyBasedRouting=1,Radius=1,Acco
unting=1,MessageAttributes=1
   apnIdentifier=(base-apn | service-apn)
```

- If the `apnIdentifier` is set to `service-apn`, the service APN name is used as the value of the `Called-Station-Id` attribute for `Accounting-Request (On)`, `Accounting-Request (Off)`, `Accounting-Request (Start)`, and `Accounting-Request (Stop)` messages. The default value for `apnIdentifier` is `service-apn`.
- If the `apnIdentifier` is set to `base-apn`, the base APN name is used as the value of the `Called-Station-Id` attribute for `Accounting-Request (Start)` and `Accounting-Request (Stop)` messages. In this case, the `Called-Station-Id` attribute is not included in `Accounting-Request (On)` and `Accounting-Request (Off)` messages.

6.4 Configuring Accounting Start on Service Access

The default behavior is to send the `Accounting-Request (Start)` message to the RADIUS accounting server configured for a service APN in

the selected rule space when the default bearer is created. In acknowledge mode, the GGSN or PGW can be optionally configured to send the `Accounting-Request (Start)` message to the RADIUS accounting server when a service access to the service APN is detected.

To enable accounting start on service access, include the following statement:

```
(config) ManagedElement=1,Epg=1,Pgw=1,Apn=servic
eApnName,AwarePolicyBasedRouting=1,Radius=1,Acc
ounting=1,StartRequest=1
   TransferOnService=1
```

Note: The configuration change is applied to the newly created PDP contexts or bearers, but not to already existing PDP contexts or bearers.

6.4.1 Configuring the Delay Timer

A delay timer is used to configure the time that the GGSN or PGW waits to forward the user packets to the service APN. The delay timer is started when the `Accounting-Request (Start)` message is sent to the RADIUS server. If the `Accounting-Response (Start)` message is received or the accounting response timeout is detected before the delay timer expires, the delay timer stops. Before the delay timer expires or stops, the GGSN or PGW can drop, buffer, or allow packets to pass depending on the packet handling configuration. See Section 6.4.2 on page 7 for information about the packet handling configuration.

The delay timer can be configured per service APN for RADIUS accounting in acknowledge mode. To configure the delay timer, include the following statement:

```
(config) ManagedElement=1,Epg=1,Pgw=1,Apn=serviceApnName
,AwarePolicyBasedRouting=1,Radius=1,Accounting=1,StartReq
uest=1,TransferOnService=1
   delayTimer=milliseconds
```

The configurable range of the delay timer is 0 to 3000 milliseconds with increments of 50 milliseconds. By default, the delay timer is not configured.

Note: The delay timer must be configured when the RADIUS accounting server does not support sending the `Accounting-Response (Start)` message to the GGSN or PGW.

Ericsson recommends to not configure the delay timer to exceed the total time allowed for RADIUS accounting start attempts, which is equal to (Time-out * Number of contact attempts). For more information about the total time allowed for RADIUS accounting start attempts, see *RADIUS Configuration*.

6.4.2 Configuring Packet Handling Pending Accounting

Before the accounting start response is received or the delay timer (if enabled) expires, the user packet to the service APN is handled according to the configured packet handling method for pending accounting. The default

behavior is to allow all packets to pass. The following three alternative methods are available:

- Buffer packets.
- Allow packets to pass.
- Drop all packets.

For detailed information about how to configure the GGSN or PGW to buffer, drop, or pass packets to a service APN, see *Credit Control Configuration*.

7 Configuring NAT for a Service APN

Configuring NAT for a service APN ensures that downlink packets belonging to a service APN are routed to that service APN.

Configure NAT by performing the following actions:

1 If configuring NAT for a service APN that is not previously configured for NAT, block user session activations as described in Section 4.1 on page 3.

2 Configure NAT address allocation for the service APN from a shared IP pool or through RADIUS.

For more information about routing packets to service APN, see *Aware Policy-Based Routing*.

Allocation from a shared IP pool

To configure allocation from a shared IP pool, include the following statements:

```
(config) ManagedElement=1,Epg=1,Pgw=1,Apn=servi
ceApnName,PdpContext=1
   addressAllocation=shared-ip-pool
   sharedIpPool=sharedPoolName
```

Allocation through RADIUS

To configure allocation through RADIUS, include the following statements:

```
(config) ManagedElement=1,Epg=1,Pgw=1,Apn=servi
ceApnName,PdpContext=1
   addressAllocation=radius
   Address=addressRange
```

Configuration of a Service APN without NAT

To configure a service APN without NAT, include the following statements:

```
(config) ManagedElement=1,Epg=1,Pgw=1,Apn=serviceApnName
   AwarePolicyBasedRouting=1
```

8 Configuring Destination Redirect for a Service APN

Configure destination redirect for a service APN by specifying a redirect set consisting of an original destination address and a redirection address. Specify the redirect set by including the following statement:

```
(config) ManagedElement=1,Epg=1,Pgw=1,Apn=serviceApn
Name,AwarePolicyBasedRouting=1,DestinationRedirect=1
,RedirectSet=originalDestinationAddress
   destinationAddress=redirectionDestinationAddress
```

Up to 100 redirect sets can be configured per service APN.

Multiple destination addresses (`originalDestinationAddress`) can be redirected to the same redirection destination address (`redirectionDestinationAddress`) within a service APN.