# 3GPP TR 23.853 V1.0.0 (2012-11)

*Technical Report*

## 3rd Generation Partnership Project;
## Technical Specification Group Services and System Aspects;
## Operator Policies for IP Interface Selection (OPIIS);
## (Release 12)

Keywords

3GPP, Architecture, EPC, Interface, WLAN, ANDSF

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

# Contents

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# 1 Scope

This Technical Report describes solutions that define:

- operator policies for selecting an IP interface in the UE for routing of IP flows among a choice of available interfaces in both 3GPP and non-3GPP accesses;
- system architecture for distribution of these policies to the UE.

Editor's note: The working assumption is that the ANDSF architecture is used for distribution of the operator policies defined in this TR.

The solutions described in this TR shall clarify how the operator policies defined in this TR relate with the ANDSF policies.

The report is intended to document the analysis of the architectural aspects to achieve these objectives in order to select a solution and include it in the relevant technical specifications.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] IETF RFC 3442: "The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP)" version 4.

[3] IETF RFC 4191: "Default Router Preferences and More-Specific Routes".

[4] draft-ietf-mif-dhcpv6-route-option: "DHCPv6 Route Option".

[5] draft-ietf-mif-dns-server-selection: "Improved DNS Server Selection for Multi-Homed Nodes".

[6] draft-ietf-6man-addr-select-opt: "Distributing Address Selection Policy using DHCPv6".

[7] 3GPP TR 24.312: "Access Network Discovery and Selection Function (ANDSF) Management Object (MO)".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

# 4 Requirements

## 4.1 Scenarios

### 4.1.1 Scenario #1: Multiple PDN connections

In this scenario the user has two established PDN connections:

- connection PDN1 associated with APN1, used for access to the IMS core network;
- connection PDN2 associated with APN2, used for access to the Internet.

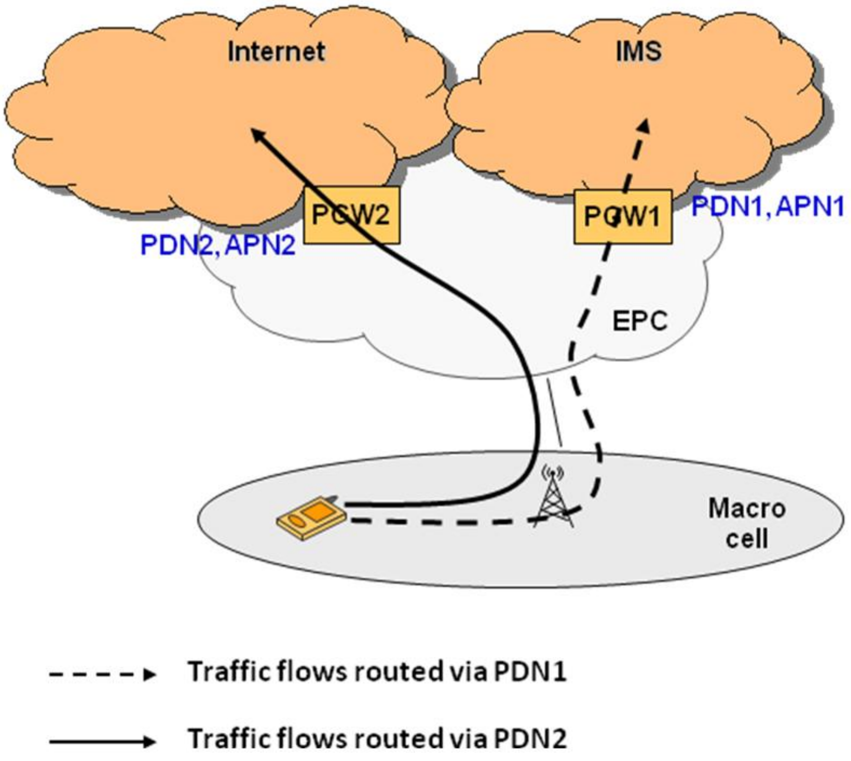

**Figure 4.1.1-1: Multiple PDN connections**

For traffic flows generated by applications that are not bound to an APN, the UE relies on operator policies defined in this TR to decide on which PDN connection to route the IP flows.

### 4.1.2 Scenario #2: Multiple PDN connections from a CSG cell

This scenario begins with the user outside of his home with an established PDN connection (PDN1) that is used for all traffic flows (e.g. IMS, Internet, etc). The PDN connection PDN1 is associated with APN1.

When the user returns home, a second PDN connection (PDN2) is established with a local gateway (LGW). The PDN connection PDN2 is associated with APN2.

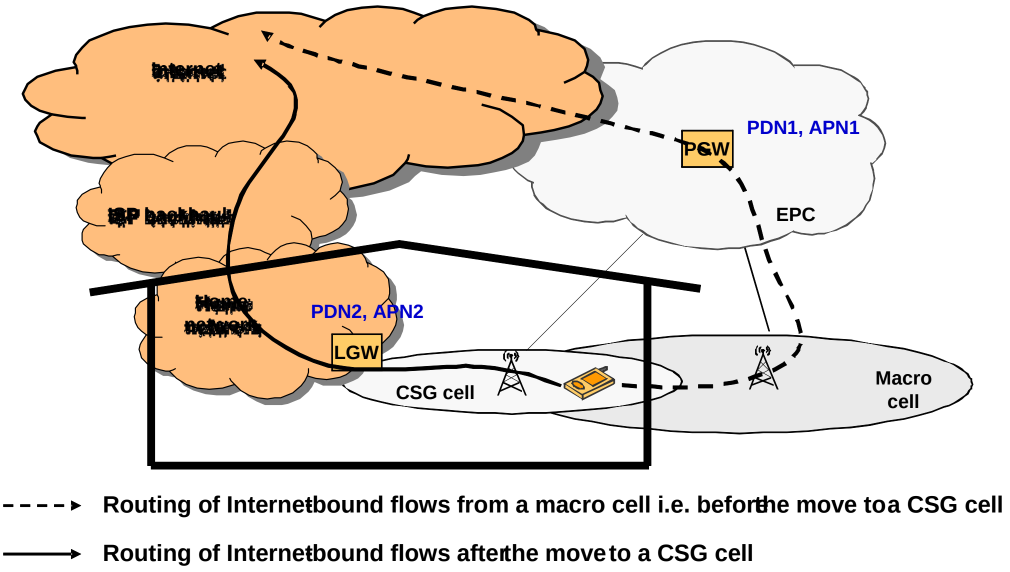
Internet
ISP backhaul
Home network
PDN2, APN2
LGW
CSG cell
PGW
PDN1, APN1
EPC
Macro cell
Routing of Internetbound flows from a macro cell i.e. beforthe move toa CSG cell
Routing of Internetbound flows afterthe moveto a CSG cell

**Figure 4.1.2-1: Multiple PDN connections from a CSG cell**

From this point on, some Internet-bound flows can be routed via PDN2, pending user's consent. The UE relies on operator policies defined in this TR for identifying the candidate Internet-bound flows that can be routed via PDN2.

NOTE: Based on UE implementation the UE may decide to re-route any *active* IP flows (i.e. flows that were established while the user was outside the home) via PDN2, in which case IP address preservation is not provided.

When the user leaves the home again, the PDN2 connection is released. The UE relies on operator policies defined in this TR for identifying the candidate Internet-bound flows that can be routed via PDN1 again.

## 4.1.3 Scenario #3: Multiple PDN connections and non-seamless WLAN offload

This scenario begins with the user outside of his home with an established PDN connection (PDN1) that is used for all traffic (e.g. IMS, Internet, etc). The PDN connection PDN1 is associated with APN1.

When the user returns home, a second PDN connection (PDN2) is established with a local gateway (LGW). The PDN connection PDN2 is associated with APN2. In addition, the UE's capability for non-seamless WLAN offload is enabled.

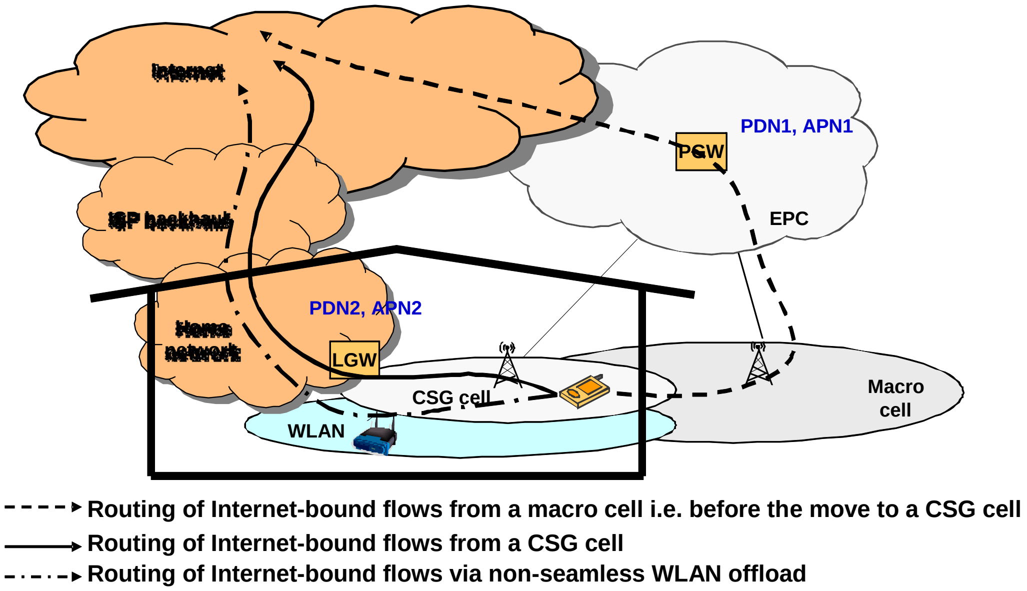
Internet
ISP backhaul
Home network
PDN2, APN2
LGW
CSG cell
WLAN
PGW
PDN1, APN1
EPC
Macro cell
Routing of Internet-bound flows from a macro cell i.e. before the move to a CSG cell
Routing of Internet-bound flows from a CSG cell
Routing of Internet-bound flows via non-seamless WLAN offload

**Figure 4.1.3-1: Multiple PDN connections and non-seamless WLAN offload**

From this point on, some Internet-bound flows can be routed either via PDN2 (pending user's consent) or via non-seamless WLAN offload. The UE relies on operator policies for identifying the candidate Internet-bound flows that can be routed via PDN2 or via non-seamless WLAN offload.

NOTE: Based on implementation the UE may decide to re-route any *active* IP flows (i.e. flows that were established while the user was outside the home) via PDN2 or via non-seamless WLAN offload, in which case IP address preservation is not provided.

When the user leaves the home again, the PDN2 connection is released and the WLAN coverage is not available. The UE relies on operator policies defined in this TR for identifying the candidate Internet-bound flows that can be routed via PDN1 again.

## 4.2 Architectural requirements

Based on the scenarios described in the previous clause, the following requirements are made:

- The solution for IP interface selection should minimize the conflict with the Inter-System Routing Policies (ISRPs).
- The solution shall allow the UE to override the rules for OPIIS for traffic that is explicitly bound to a local IP address of the UE and/or an APN, or due to user preferences.
- For UEs capable of operating multiple PDN connections simultaneously the EPS shall allow the operator to provide policies that assist the UE in selecting a specific APN for routing a specific IP flow. The operator policies may also indicate which APNs are restricted for a specific IP flow.
- For UEs capable of operating multiple PDN connections simultaneously and also capable of non-seamless WLAN offload, the EPS shall allow the operator to provide policies that assist the UE in deciding whether a specific IP flow should be routed on a specific APN. The operator policies may also indicate which APNs are restricted for a specific IP flow.

# 5 Solutions

## 5.1 Solution 1: Inter-APN Routing Policies

### 5.1.1 Description

To support policy-based IP interface selection based on the scenarios in section 4, a new set of routing policies is introduced called Inter-APN Routing Policies (IARP).

Figure 5.1.1-1 below shows the scope of IARP applicability and how IARP policies can be applied in conjunction with ISRP for NS-WLAN offload policies.

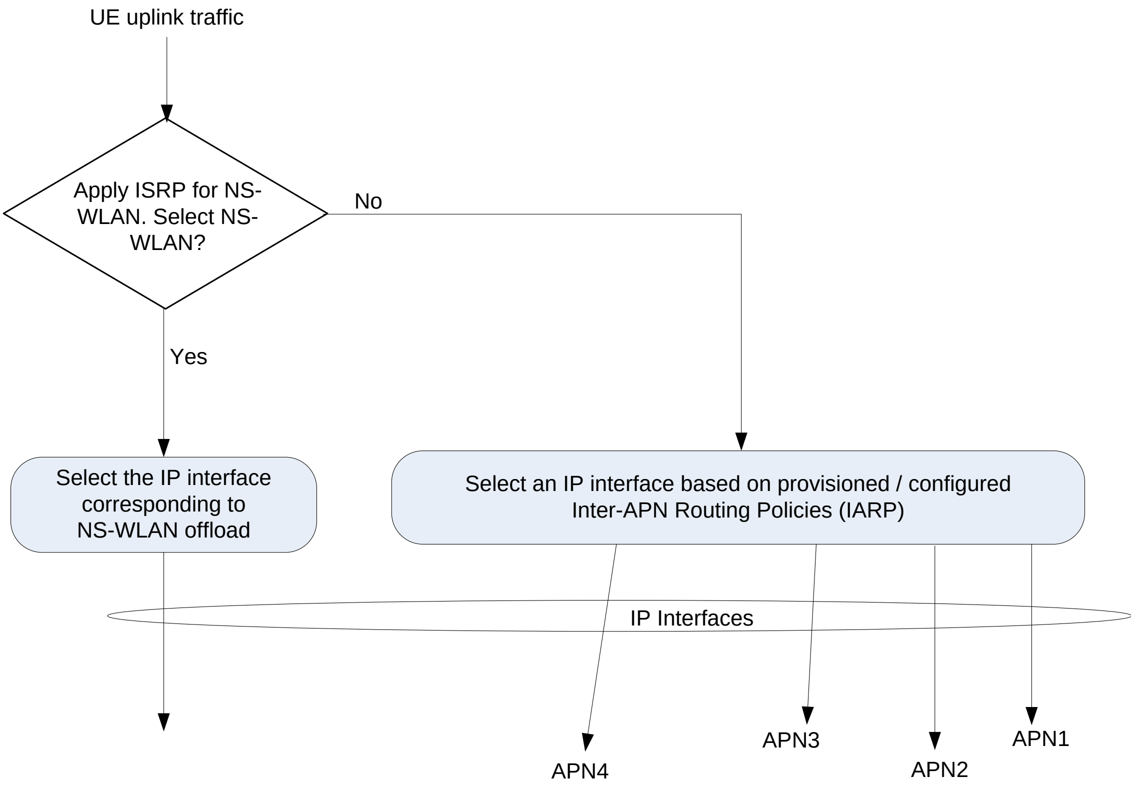
UE uplink traffic
Apply ISRP for NS-WLAN. Select NS-WLAN?
No
Yes
Select the IP interface corresponding to NS-WLAN offload
Select an IP interface based on provisioned / configured Inter-APN Routing Policies (IARP)
IP Interfaces
APN4
APN3
APN2
APN1

**Figure 5.1.1-1: Applicability of Inter-APN Routing Policies**

NOTE: The above figure aims at showing only the relationship between the ISRP for NSWLAN and the Inter-APN routing policies. For routing uplink traffic the UE may take into account other parameters (e.g. the local operating environment information) which are not shown in the figure for simplicity.

Editor's Note: Figure 5.1.1-1 assumes that the policies for non-seamless WLAN offload are evaluated by the UE before the evaluation of Inter-APN Routing Policies. It is FFS is this order of policy evaluation is necessary or if any possible order could be supported. It is FFS how this solution can enable scenarios where WLAN is not the default interface.

The Inter-APN Routing Policies (IARP) can be statically configured in the UE or they could be provisioned by the ANDSF. A UE that is inter-APN capable can use IARP to select an outgoing interface based on the preferred APN in IARP policies. A UE is defined to be inter-APN capable if it is capable of routing IP flows across multiple simultaneously active interfaces, each one associated with a different APN. These interfaces may be linked to different access networks or linked with the same access network.

The following assumptions and specifications apply:

- Every IP interface that can be selected with IARP is associated with a different APN:
  - IP interfaces not associated with an APN are considered outside the scope of IARP. Such interfaces could include e.g. an IP interface to a tethering device connected to UE over USB, or an IP interface corresponding to an enterprise VPN connection over WLAN, etc.
  - The scenario where multiple IP interfaces are associated with the same APN is also considered outside the scope of IARP.
- The ANDSF may provide a list of inter-APN Routing Policies to UE. A UE that is inter-APN routing capable uses these policies to select an existing IP interface to route IP flows that match specific criteria (e.g. all flows to a specific TCP port or to a specific destination address, etc).
- Each inter-APN routing policy includes the following information:
  - Validity conditions, i.e. conditions indicating when the provided policy is valid.

  - One or more Filter Rules, each one identifying a prioritised list of APNs which should be used by the UE to route IP flows that match specific IP filters. A filter rule also identifies which APNs are restricted for IP flows that match specific IP filters.

- An Inter-APN routing capable UE selects an existing IP interface, which is associated with a specific APN, to route IP flows based on the received / provisioned inter-APN routing policies and user preferences.

### 5.1.2 Impact on existing nodes or functionality

The relationship between IARP and ISRP policies (excluding MAPCON policies for simplicity) is schematically shown in Figure 5.1.1-1 above.

## 5.2 Solution 2: Extension of existing ISRPs with addition of Filter Rules for Inter-APN Routing

### 5.2.1 Description

This solution assumes that the Rel-11 ISRP rule is enhanced by defining new Filter Rules (a.k.a. *flow distribution rules* in Stage 3 terminology) for Inter-APN Routing. If the UE is capable of inter-APN routing, the UE shall be able to evaluate the ISRP rule even if it does not support non-3GPP WLAN access. Therefore the UE uses the ISRP when it can route IP traffic simultaneously over multiple radio access interfaces and/or over multiple APNs.

The Filter Rules for Inter-APN Routing are defined at the same hierarchical level as the existing Filter Rules for IFOM, MAPCON and Non-seamless WLAN offload, as illustrated in Figure 5.X.1-1. The rule evaluation is performed with the APNs which were established. The Filter Rules for IFOM, MAPCON, non-seamless WLAN offload and Inter-APN Routing are associated with a rule priority. If more than one valid Filter Rules match a specific IP traffic flow, the UE applies the Filter Rule with the highest rule priority.

Each inter-APN routing policy includes the following information:

- Validity conditions, i.e. conditions indicating when the provided policy is valid.

- One or more Filter Rules, each one identifying a prioritised list of APNs which shall be used by the UE when PDN connections to these APNs were established to route IP flows that match specific IP filters. This Filter Rule may also identify which APNs are restricted for IP flows that match specific IP filters.

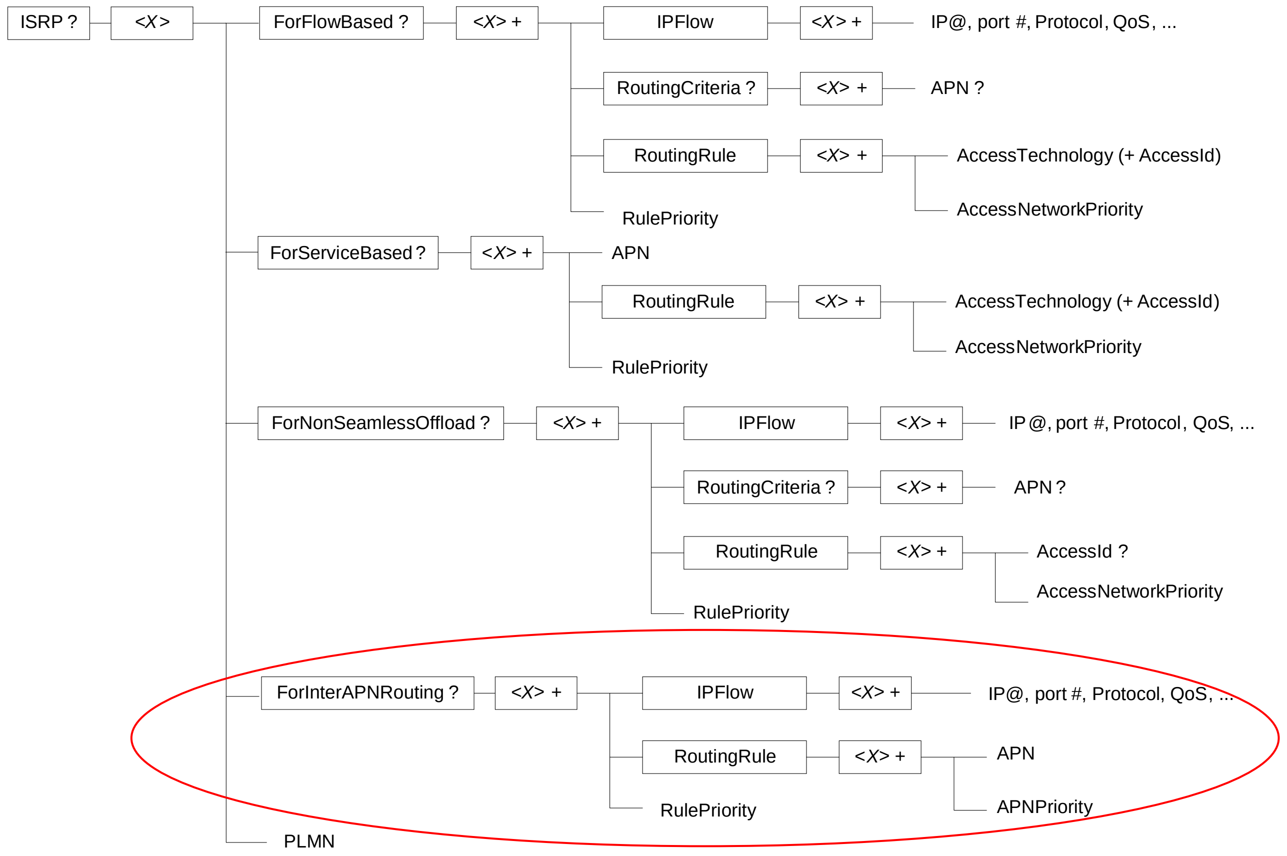

**Figure 5.2.1-1: Hierarchical location of Filter Rules for Inter-APN Routing (simplified and illustrative)**

NOTE: The figure above aims at showing the hierarchical location of Inter-APN Routing rules compared with the existing Filter Rules for IFOM, MAPCON and Non-seamless WLAN offload, and is purely illustrative. It is left to Stage 3 to define the exact realisation of the new Filter Rule in the OMA DM management object.

### 5.2.2 Impact on existing nodes or functionality

New Filter Rules for Inter-APN Routing are included in ISRPs. The introduction of new Filter Rules for Inter-APN Routing may require a two-round evaluation of ISRP rules in the terminal. Namely, if the UE selects a Filter Rule for Inter-APN Routing during the initial iteration and if the UE is IFOM- or MAPCON-capable, the UE needs to go through a second iteration of ISRP rule evaluation. During the second iteration the Filter Rules for Inter-APN Routing and for Non-seamless WLAN offload are not active.

If the UE is not capable of routing IP traffic simultaneously over 3GPP and WLAN access but the UE is capable of inter-APN routing, the UE still requires ISRP policies from the ANDSF.

## 5.3 Solution 3: Consolidation of Solution 1 and Solution 2

### 5.3.1 Description

To support policy-based IP interface selection based on the scenarios in section 4, a new set of routing policies is introduced called Inter-APN Routing Policies (IARP). The Inter-APN Routing Policies (IARP) can be statically configured in the UE or they could be provisioned by the ANDSF. A UE that is inter-APN capable can use IARP to select an outgoing interface based on the preferred APN in IARP policies. A UE is defined to be inter-APN capable if it is capable of routing IP flows across multiple simultaneously active interfaces, each one associated with a different APN. These interfaces may be linked to different access networks or linked with the same access network.

The following assumptions and specifications apply:

- Every IP interface that can be selected with IARP is associated with a different APN:
  - IP interfaces not associated with an APN are considered outside the scope of IARP. Such interfaces could include e.g. an IP interface to a tethering device connected to UE over USB, or an IP interface corresponding to an enterprise VPN connection over WLAN, etc.
  - The scenario where multiple IP interfaces are associated with the same APN is also considered outside the scope of IARP.
- The ANDSF may provide a list of inter-APN Routing Policies to UE. A UE that is inter-APN routing capable uses these policies to select an existing IP interface to route IP flows that match specific criteria (e.g. all flows to a specific TCP port or to a specific destination address, etc).
- Each inter-APN routing policy includes the following information:
  - Validity conditions, i.e. conditions indicating when the provided policy is valid.
  - One or more Filter Rules, each one identifying a prioritised list of APNs which shall be used by the UE when PDN connections to these APNs are established to route IP flows that match specific IP filters. This Filter Rule may also identify which APNs are restricted for IP flows that match specific IP filters.
- An Inter-APN routing capable UE selects an existing IP interface, which is associated with a specific APN, to route IP flows based on the received / provisioned inter-APN routing policies and user preferences.
- The priority values used for ISRP and IARP policies are chosen from a common range.
- A UE not capable of routing IP traffic simultaneously over multiple radio access interfaces uses the Inter-System Mobility Policies (ISMP) and uses also the Inter-APN Routing Policies (if any). The UE evaluates these policies in priority order and determines if any of them match an outgoing IP flow. The highest priority policy that matches an outgoing IP flow identifies the PDN connection (the one associated with the preferred APN in the policy) that should be used to route this IP flow.
- A UE capable of routing IP traffic simultaneously over multiple radio access interfaces uses the Inter-System Routing Policies (ISRP) and uses also the Inter-APN Routing Policies (if any). The UE evaluates the inter-system routing policies for IFOM, MAPCON and Non-seamless WLAN offload and also the inter-APN routing policies in priority order and determines if any of them match an outgoing IP flow. The highest priority policy that matches an outgoing IP flow indicates how this IP flow should be routed. If the highest priority policy that matches an outgoing IP flow is an inter-APN routing policy, then the UE routes this IP flow to the PDN connection associated with the preferred APN in this policy.
- The UE may be required to perform a two-round evaluation of ISRP and IARP policies. Namely, if the UE selects a filter rule for Inter-APN Routing during the initial iteration and if the UE is IFOM- or MAPCON-capable, the UE needs to go through a second iteration of ISRP rule evaluation. During the second iteration the Inter-APN Routing policies and the ISRP for Non-seamless WLAN offload policies are not evaluated.

NOTE: It is up to stage-3 to define how the Inter-APN Routing Policies are encoded in the ANDSF MO specified in TS 24.312 [7].

### 5.3.2 Impact on existing nodes or functionality

The ANDSF MO should be expanded to support inter-APN routing policies. The details should be handled by stage-3.

A UE capable of inter-APN routing but not capable of routing IP traffic simultaneously over multiple radio access interfaces should evaluate the inter-APN policies based on their priority order.

A UE capable of inter-APN routing and capable of routing IP traffic simultaneously over multiple radio access interfaces should evaluate the inter-APN policies together with the existing inter-system routing policies based on their priority order. In this case the UE may require a two-round evaluation of ISRP policies in the UE.

## 5.4 Solution 4: Select the IP interface based on the routing configuration

### 5.4.1 Description

Both DHCPv6 and RA can be used to deliver IPv6 the routing information to the UE. DHCPv6 is used for IPv6 parameter configuration and RA is used for SLAAC of handset.

- DHCPv6: The IPv6 parameter configuration via DHCPv6 is introduced from Release 8 in 3GPP. The DHCPv6 extension option can contains the routing information and respond to UE's DHCPv6 request. The policy (routing information) comes from the DHCPv6 server. The DHCPv6 server can be collocated with GGSN/PGW or be deployed in a central manner to which the GGSN/PGW relays the DHCPv6 message. In both cases the 3GPP PLMN operator where the PGW is located is responsible to configure the appropriate routing policies in the DHCPv6 server.

- RA: the RA can contain the routing information to UE (e.g., through RIO). The routing information is sent to UE periodically when the network updates the IPv6 prefix to UE in SLAAC. It is the 3GPP PLMN operator where the PGW is located responsibility to provide the routing policies, which advertised in the RA messages to the UE, to the PGW.

When UE obtains the routing information, the UE will select the proper source IP address according to the routing and the IP packets are routed accordingly to the corresponding IP interface.

The specific characters of using DHCPv6 or the RA are the following.

- Although it is an optional feature, the DHCPv6 is generally used for parameter configuration (e.g., prefix delegation, DNS or network server information of IMS configuration, etc.,). DHCPv6 is more management/operation friendly due to the central control mechanism when PGW/GGSN is used as DHCPv6 relay. It is easy to do per-user configuration.

- For RA approach, the RIO has been already specified in [RFC4191]. It if benefit on the "push mode" that can be distribute to the UE. It needs more work for the PMIP case. The point-to-point link is between UE and SGW (MAG). The prefix is obtained from PGW (LMA). The SGW needs to obtain the routing information from multiple PGWs and send the information to UE through RA. Such information shall be transferred from one SGW to another when SGW relocation happens due to the UE movement.

For IPv4, the routing information can be provided using the following options:

- **DHCPv4 + PCO**: The routing information is provided to the UE along with the IP address using DHCP (using RFC 3442). The preference (low, middle, high) of the default routing route is provided to the UE during setup of PDN connection using PCO.

- **PCO**: Both the routing information and the preference (low, middle, high) of the default routing route are provided to the UE during setup of PDN connection using PCO.

A UE supporting both ANDSF and solution 4 first runs the ANDSF policies and then apply the IP routing as follows:

- if the IP flow matches an ANDSF rule for NSWO, the UE routes the IP flow using only the IP routing rules received via NSWO;

- if the IP flow matches ANDSF rule for IFOM, the UE routes the IP flows via the access indicated by the ANDSF rule and using the IP routing rules of the PDN connection associated with the IP flow; and

- routes the IP flows for which no matching ANDSF rule exists using IP routing rules of the all IP interfaces.

NOTE: MAPCON policies are not IP flow dependent and thus not impacted.

When UE has multiple PDN connections and/or NSWO, the UE uses all routing rules provided by all PDN connections and NSWO. The UE selects the interface to send outgoing IP packets by searching UE routing table to find the route with the longest prefix that matches the destination address of the IP packet, using preference as a tie-breaker if multiple matching routes have the same prefix length.

In order to ensure deterministic routing to entities other than those providing PLMN services, the default routing rule provided in up to one PDN connection is marked with high preference (as in RFC 4191, section 2.1) and the default routing rule in other PDN connections are marked with the low p reference. Routing rules of NSWO is assumed to be marked with the medium preference.

When the UE has PDN connections with PGW in the VPLMN, the HPLMN needs to ensure in roaming agreement that the P-GW provides the correct preference of the default routing route.

### 5.4.2 Impact on existing nodes or functionality

For the DHCPv6 approach, the UE and PGW/GGSN support DHCPv6 route option. In this case the DHCPv6 server is configured with the routing policies to be delivered to the UE.

For the RA approach, the UE and PGW need to support the option used by RA for configuration. In this case the PGW is configured with the routing policies to be delivered to the UE.

For the **DHCPv4 + PCO** approach, the UE and the PGW (including L-GW)/GGSN support the DHCPv4 classless static route option to indicate the routing information and a PCO for indicating the preference of the default routing route. In this case the DHCP server is configured with the routing policies to be delivered to the UE and P-GW is configured with the preference of the default routing route.

For the **PCO** approach, the UE and PGW (including L-GW)/GGSN support a PCO for indicating both the routing information and the preference of the default routing route. P-GW is configured with the routing information and the preference of the default routing route.

The UE sets the routing preference to medium for NSWO and when the UE does not receive any preference for the route.

### 5.4.3 Evaluation

This solution enables IP interface selection using existing internet principles with the following characteristics:

- It supports IP interface selection for interfaces not associated with any APN;
- It supports multiple PDN connections using same APN; and

NOTE: Support for multiple PDN connections to same APN is not within scope of the WID.

- It works for UEs supporting ANDSF and for UEs not supporting ANDSF".

When the UE does not support ANDSF, the solution enables the UE to use existing IP routing table. If the UE uses ANDSF in combination with this solution, the UE needs, for an IP flow matching an ANDSF rule, to use a reduced IP routing table.

The limitations of this solution include the following:

- If user applies preferences, then they may differ from the preferences as part of the routing rules, in a similar manner as user preferences may override operator policies when applying ANDSF policies;
- It is only possible to have three preference levels which limit the possibility to provide different relative priority between multiple PDN connections that provides the same IP routing capabilities.
- It is limited to the cases when destination IP address can be used to identify services/applications which may not cover all cases addressed by the ANDSF policy with APN, Application ID and Domain Names;
- HPLMN needs to ensure in roaming agreement that the L-GW/P-GWs in VPLMN provides the correct preference of the default routing route.

Editor's Note: How the operator can control an L-GW is FFS.

# 6 Other considerations

Editor's note: This clause is a placeholder for any special considerations (e.g. scenarios where multiple PDN connections carry traffic with overlapping private IPv4 addresses, DIDA).

## 6.1 Potential Implications of Co-existence of OPIIS and IETF mechanisms

The purpose of this section is to provide examples of IETF mechanisms that may have to be considered for the co-existence with OPIIS.

Some of the IETF mechanisms considered are RFC3442 The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4 [2], RFC4191 Default Router Preferences and More-Specific Routes [3], draft-ietf-mif-dhcpv6-route-option, DHCPv6 Route Option [4], draft-ietf-mif-dns-server-selection, Improved DNS Server Selection for Multi-Homed Nodes [5], draft-ietf-6man-addr-select-opt, Distributing Address Selection Policy using DHCPv6 [6].

The following example of potential need for co-existence implications is based on IPv6 and on the split UE scenario, where the TE is represented by a laptop or any other off-the-shelf wireless device other than a 3GPP Mobile phone. In general the co-existence may be relevant not only to the split UE scenario but also to the scenario with a monolithic UE.

This example illustrates a case where a TE is connected to the Internet directly via local access, such as WLAN (i.e., non-seamless offloading), and via a cellular network as provided by a MT. In this scenario, ANDSF may be used to configure the MT, but not the TE. On the other hand, the PGW could utilize IETF mechanisms to "configure" TE's routing table to influence its routing decisions.

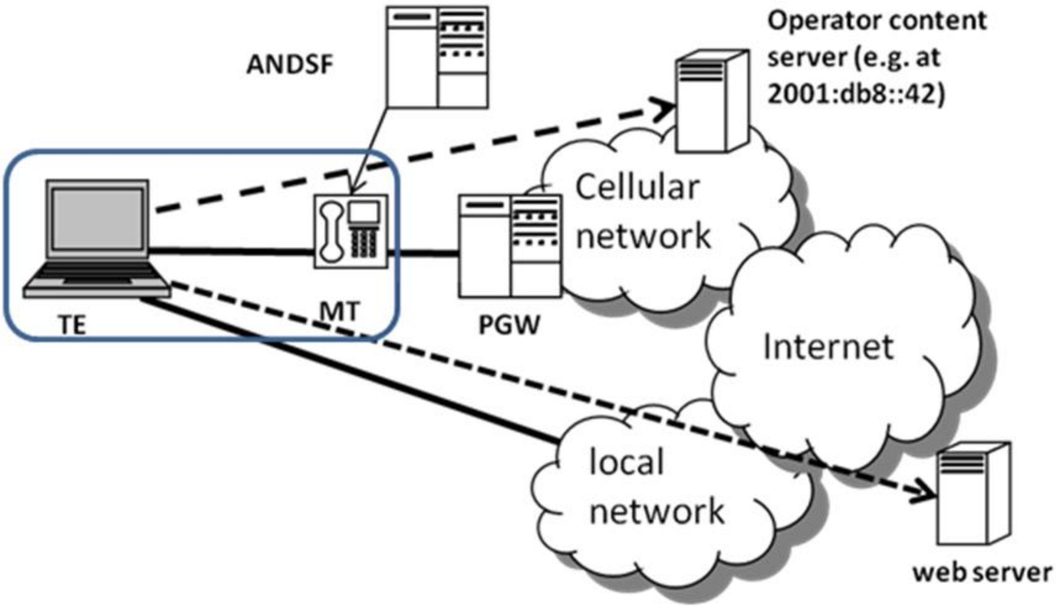

**Figure 6.1.-1: Split UE scenario using IETF mechanisms to configure the TE**

NOTE 1: The co-existence case with IETF mechanisms described above also applies to Rel-10 inter-system routing policies for non-seamless WLAN offload.

NOTE 2: The example considered above focuses mainly on IPv6 but similar considerations can be applicable to IPv4.

# 7 Conclusions

## 7.1 Analysis of solutions

Currently 4 solutions were agreed for OPIIS. The solution 1 and the solution 2 were consolidated to the solution 3 which was based on ANDSF policies. For the solution 4, the network may configure routing information in the UE through DHCPv6 or IPv6 Router Advertisement (RA). In the technical point of view, two different solutions (e.g. solution 3 and solution 4) can be compared to decide the normative work as follows:

**Solution 3: Consolidation of Solution 1 and Solution 2**

- This solution expanded the ANDSF MO to support inter-APN routing policies. A UE should evaluate the inter-APN routing policies based on their priority order. The evaluation based on the priority enables the UE to interact with existing ANDSF routing policies without conflict. This solution is also applicable to IPv4 and IPv6, and there is no limitation on use of Destination IP address, APN, Application ID and Domain Names to identify services/applications in the policies. On the priorities of routing policies provided by different PLMNs, the routing policies from VPLMN take precedence. So, no conflict between routing policies provided by different PLMNs is expected.

**Solution 4: Select the IP interface based on the routing configuration in IPv6**

- If user applies preferences, then they may differ from the preferences as part of the routing rules, in a similar manner as user preferences may override operator policies when applying ANDSF policies. It is only possible to have three preference levels which limit the possibility to provide different relative priority between multiple PDN connections that provides the same IP routing capabilities. It is limited to the cases when destination IP address can be used to identify services/applications which may not cover all cases addressed by the ANDSF policy with, Application ID and Domain Names. HPLMN needs to ensure in roaming agreement that the L-GW/P-GWs in VPLMN provides the correct preference of the default routing route.

## 7.2 Recommendation

This Technical Report has analyzed the 4 solutions for OPIIS. As a result of the analysis, it was agreed to define a policy for IP interface selection based on ANDSF according to the description of solution 3. Therefore, the solution 3 is recommended for normative specification.

During the specification phase, it should be reconsidered if the existing mechanism for conflict resolution between VPLMN and HPLMN policies should also apply to the new policies or if a new resolution mechanism is required.

The resolution of possible conflicts with IETF defined policies will be handled outside of OPIIS work, because any such conflicts may exist with IFOM and NSWO policies defined in Release-10.

# Annex A:<br>Change history

| Date | TSG # | TSG Doc. | CR | Rev | Subject/Comment | Old | New |
|---|---|---|---|---|---|---|---|
| 2011-04 | SA2#84 | | | | Version 0.0.0 Rapporteur's internal draft | | 0.0.0 |
| 2011-04 | SA2#84 | | | | Inclusion of P-CRs approved during SA2#84: S2-111935, S2-112186, S2-112187 | 0.0.0 | 0.1.0 |
| 2011-05 | SA2#85 | | | | Editorial (change of TR number) | 0.1.0 | 0.1.1 |
| 2011-05 | SA2#85 | | | | Inclusion of P-CRs approved during SA2#85: S2-112807, S2-112810, S2-112901, S2-112902 | 0.1.1 | 0.2.0 |
| 2011-07 | SA2#86 | | | | Inclusion of P-CRs approved during SA2#86: S2-113566, S2-113814, S2-113815 | 0.2.0 | 0.3.0 |
| 2011-08 | | | | | Editorial fixes in the figures | 0.3.0 | 0.3.1 |
| 2012-05 | SA2#91 | | | | Inclusion of P-CRs approved during SA2#91: S2-122609 | 0.3.1 | 0.4.0 |
| 2012-10 | SA2#93 | | | | Inclusion of P-CRs approved during SA2#93: S2-123694, S2-123948, S2-124111, S2-124188 | 0.4.0 | 0.5.0 |
| 2012-11 | SA2#94 | | | | Inclusion of P-CRs approved during SA2#94: S2-124340, S2-124640, S2-124641 | 0.5.0 | 0.6.0 |
| 2012-11 | SP-56 | SP-120730 | - | - | MCC editorial update to version 1.0.0 for presentation to TSG SA for Information | 0.6.0 | 1.0.0 |
| | | | | | | | |