Study on Access Selection Steering Mechanisms

Janne Tervonen (NSN)
Janne Marin (Nokia)

ICT SHOK Future Internet Programme
(ICT SHOK FI)

Phase 3: 1.4.2011 – 31.12.2012

Tivit, Yritysten tutkimus- ja kehittämisrahoitus, Päätös 516/09, 29.5.2009, Dnro 560/31/09

TKK, Tutkimusrahoituspäätös 40212/09, 29.5.2009, Dnro 925/31/09

www.futureinternet.fi

www.tivit.fi

This work was supported by TEKES as part of the Future Internet programme of TIVIT (Finnish Strategic Centre for Science, Technology and Innovation in the field of ICT).

Executive summary / Internal release

Title: Study on Access Selection Steering Mechanisms

Currently, there are several activities within different standardization bodies to define mechanisms for steering the terminal's network selection decisions. The purpose of this document is to present the available mechanisms from different standardization organizations, namely 3GPP and IETF. Mainly, the different mechanisms are considered from cellular network operator point of view. For the co-existence of the 3GPP and IETF–based mechanisms, two high-level options are defined to take most of the both mechanisms.

Content: Deliverable FI3-D1.2.1 for ICT SHOK Future Internet Phase 3.

Impact: The document describes how different, standardized mechanisms can be used effectively together. This work benefits at least both Nokia and NSN in their future WLAN offload solutions.

Contact info: Janne Tervonen, janne.tervonen@nsn.com

Link: http://www.futureinternet.fi/deliverables.htm

Table of Contents

Abbreviations and Terminology

3GPP	3rd Generation Partnership Project
ANDSF	Access Network Discovery and Selection Function
AP	Access Point
DHCP	Dynamic Host Configuration Protocol
DIDA	Data Identification for ANDSF
DNS	Domain Name Server
DSMIPv6	Dual-Stack Mobile IPv6
GGSN	Gateway GPRS Support Node
HESSID	Homogeneous Extended Service Set Identifier
IETF	Internet Engineering Task Force
IFOM	IP Flow Mobility
ISMP	Inter-System Mobility Policy
ISRP	Inter-System Routing Policy
LAN	Local Area Network
MAC	Medium Access Control
MIF	Multiple Interfaces IETF working group
OMA DM	Open Mobile Alliance Device Management
PBRM	Policy-Based Resource Management
PDN GW	Packet Data Network Gateway
RA	Router Advertisement
RFC	Request For Comments
SIM	Subscriber Identification Module
SSID	Service Set Identifier
URI	Uniform Resource Identifier
WFA	Wi-Fi Alliance
WLAN	Wireless LAN

1 Introduction

Currently, there are several activities within different standardization bodies to define mechanisms for steering the terminal's network selection decisions between the available different radio access networks. For example, 3GPP is working on a solution called Access Network Discovery and Selection Function (ANDSF). The main idea behind ANDSF is to provide operators some means to influence also non-3GPP network, i.e. in practice WLAN, usage. Also, Wi-Fi Alliance (WFA) is working on a similar solution: HotSpot 2.0 working group is trying to provide better mechanisms for WLAN roaming as well as WLAN – 3GPP interworking. The aim is to make WLAN roaming – i.e. moving between different WLAN networks – as seamless as it is currently in cellular networks. IETF, on the other hand, is not really working on radio interface, but above it: however, also IETF mechanisms can be used for guiding the terminal's network selections by affecting how the terminal should e.g. route packets belonging to certain application flow.

The purpose of this document is to present the available mechanisms from different standardization organizations. Also, the different mechanisms will be compared and studied to what kind of use scenarios they would fit. If possible, the best solution – or a combination of the best mechanisms – will be proposed.

The document is structured in the following way: first on chapter 2, the general issues related to access network selection between different radio access technologies is discussed. On chapter 3, the available different access selection mechanisms are briefly described. Chapter 4 discusses how the different mechanisms can co-exists, or if they can in the first place. Finally, chapter 5 concludes the findings of this study.

2 Access Selection

2.1 Service Provider Selection

In general, access selection in wireless network environment can be divided into two different procedures: radio access selection and service provider, i.e. core network, selection. Often, the two procedures are interrelated: when selecting an access network, it also automatically means selection of a certain service provider network. For example in case of 3GPP radio access, the selection of the radio access network and the service provider, i.e. the operator, is pretty much a single procedure. However in WLAN environment, the story is a bit different; a single WLAN access network may be used to access several service providers' services.

In practice, the selection of the service provider and its network is tied to the subscription agreement made between the user and an operator. Thus, there is normally not that much room for service provider selection: once the user has selected which operator services he wishes to use, the terminal always tries to connect to that service provider network. Of course, when the terminal is roaming, there may not be a direct access to the selected service provider network, and then the terminal (or the user) needs to make a selection which roaming partners' services the terminal will use while roaming. Also, it is possible that the user has subscribed to multiple operator services at the same time – e.g. with dual-SIM device in 3GPP environment, or there are separate subscriptions to different WLAN service providers –

and then either the terminal or the user is required to make the decisions what service providers' services are used. Since this selection will cause costs to the user, it is normally left for the user to manually select the service provider used in such a case. In practice, this is how the user is made responsible for any costs resulted from his reasoned service provider selection.

Mostly, the existing access steering mechanisms do not deal with the service provider selection, WFA HotSpot 2.0 being the only exception.

2.2 Radio Access Selection

Usually, for each separate wireless network technology, network discovery and selection procedures are well defined. However, that is only defined within that specific technology. For a heterogeneous network environment with multiple available radio accesses, it has not been possible to influence on the radio access selection of a different radio technology.

From network operator point of view, this is not an optimal solution: especially in the case the operator owns the different radio access networks – e.g. 3G and WLAN – the operator should also be allowed to affect how its networks are being used.

3GPP and WLAN radio access selection are different from each other. With WLAN, it is the terminal that makes all the decisions regarding network selection, i.e. to what WLAN AP to join and when. This is the opposite of the used mechanism in 3GPP networks: network is in charge of every network selection and mobility decision, excluding only idle mode operation (i.e. no active connection to the network).

So how to combine these two worlds? In practice, it is not possible to change either 3GPP or WLAN radio access selection core mechanisms; there are too many legacy devices out there. Also, the terminal vendors are not likely to give up their position in e.g. WLAN access selection: it is not probably in near future that there could for example be a common radio resource management entity within operator network to control both 3GPP and WLAN radio access selections, as it has from time to time been proposed especially within research community.

Currently, the most viable model to give the operators some degree of control also for WLAN radio access selections is to provide guidance for the terminals' network selection, but still keep the final decision in the terminal (or user, if the terminal vendor so wishes). This kind of an overlay model does not conflict with the existing WLAN radio access selection mechanisms. Of course, this "network selection guidance" mechanism requires support from both the network and terminals, and requires in practice some standardized mechanisms for a wider acceptance.

In this document, the available radio access selection steering mechanisms following the model above are described and discussed.

3 Different Access Selection Mechanisms

In this chapter, different access selection mechanism from 3GPP, WFA and IETF are considered. In 3GPP and WFA, there is in practice only one mechanism that is applicable for access steering. In IETF, on the other hand, there are several different standardized features that could potentially be used in access steering, although none of these features provide a complete solution.

3.1 ANDSF

3.1.1 Overview

Although ANDSF has been shortly introduced in previous PBRM deliverables completed during earlier Future Internet program phases – for example in [1] – the main concepts of ANDSF are presented here.

Currently, the cellular operators are actively seeking ways to increase their network capacity, and WLAN is seen very promising option for extending capacity. This so called WLAN offload could be applied to various types of WLAN deployments – including operator own networks, hotspots, home networks – but a tool to influence the terminal's network selection is needed: ANDSF can be used to deliver to the terminals instructions when and for what traffic to use WLAN instead of cellular networks.

In short, ANDSF is an operator tool to facilitate the subscribers' network selection and inter-system mobility between 3GPP and WLAN networks or within WLAN networks.

Within 3GPP Evolved Packet Core (EPC) architecture, ANDSF is an optional network element. ANDSF was introduced into 3GPP specifications in Rel-8. New functionality has been added in subsequent 3GPP releases. Figure 1 illustrates the general functionality of ANDSF.

The use scenario of ANDSF is such that first the operator defines some network selection policies into the ANDSF server, and then the terminal contacts the server and downloads the policies. After receiving these policies, the terminal follows the policies in subsequent network selection decisions, both in initial network selections as well as in handover decisions. In practice, the intention of ANDSF is to define the network selection policies to be pretty static, i.e. the terminal contacts the ANDSF server e.g. once per week or month. Thus, ANDSF information cannot be considered as dynamic.

As can be seen from the figure, both the network and the terminal need to have support for the ANDSF functionality.

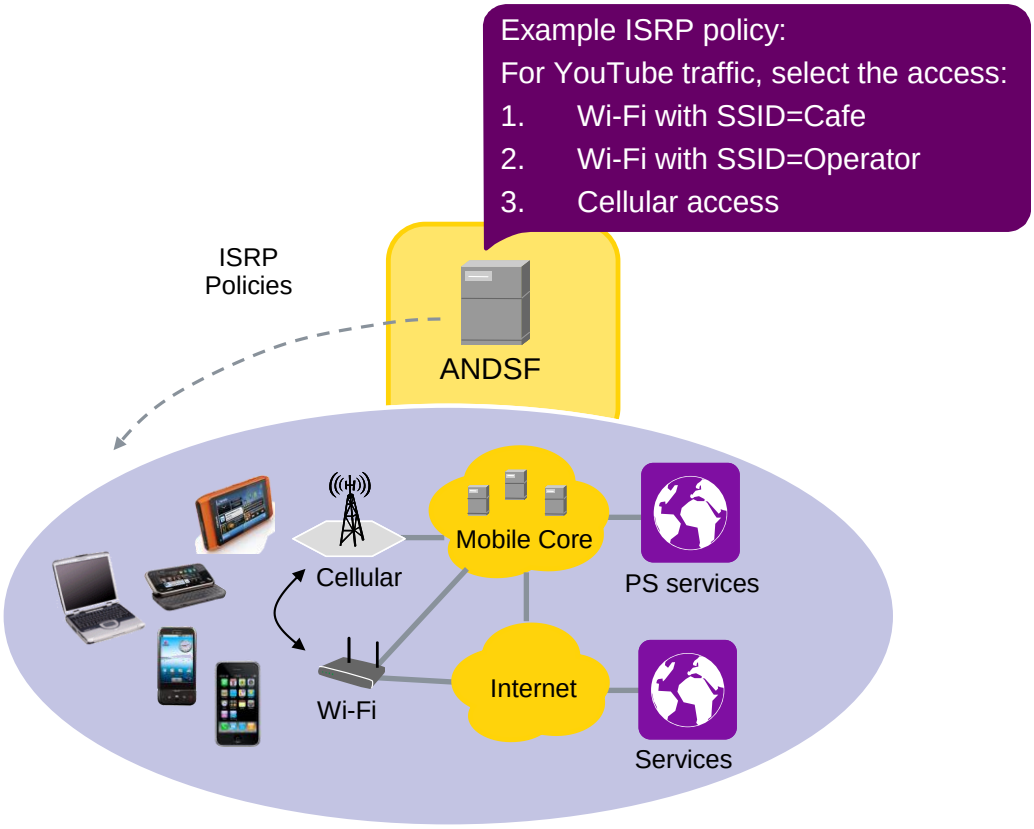

Figure 1. High-level functionality of ANDSF, showing an example policy delivered from the server to the terminals.

3.1.2 Standardization

ANDSF is being specified in 3GPP specifications 23.402 [2], 24.302 [3] and 24.312 [4]. 3GPP specifications are divided into so called stages: Stage1 defines high-level requirements, Stage2 finer-grained requirements and Stage3 finally specifies all the bits and details of each protocol or feature. 3GPP 23-series specifications contain Stage2 definitions, while 24-series is for Stage3 specifications.

ANDSF architecture is shown in Figure 2. The S14 interface between the terminal (UE in 3GPP terminology) and ANDSF server is defined to be based on Open Mobile Alliance (OMA) Device Management (DM) framework. OMA DM messages are transferred on top of IP, i.e. in order to contact ANDSF server, the terminal needs an active user data connection to the network. As illustrated in the figure, ANDSF supports both non-roaming and roaming scenarios, i.e. the ANDSF services are accessible also when a subscriber is roaming in a visited network. ANDSF supports both push and pull model.

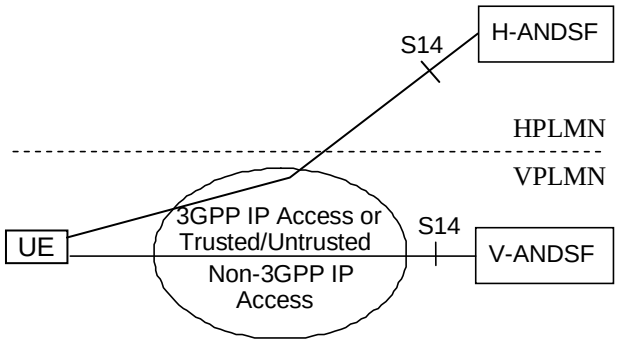

Figure 2. ANDSF architecture for roaming scenario [2].

3.1.3 ANDSF Information

Currently, the Release-10 ANDSF can provide three kinds of information:

1. Inter-System Mobility Policy (ISMP): this was the original network selection policy defined in Release-8. The idea is that the same network policy information is used for all the applications in the UE, i.e. there is no separate network selection policy per application. In practice, it is possible to prioritize different WLAN networks differentiated by SSID. For 3GPP radio access technologies, it is not possible to separate e.g. 3G radio access from LTE: ANDSF currently only identifies one umbrella 3GPP radio access technology that covers all the possible cellular radio accesses.

   An example ISMP policy:

   Priority 1: use WLAN with SSID==’Café’

   Priority 2: use WLAN with SSID==’Operator_A

   Priority 3: use 3GPP radio access

2. Access Network Discovery Information: the main usage of this is to facilitate terminals network discovery process to avoid unnecessary scanning. For example, it is possible to define an access network discovery information saying to the terminal that “scan for WLAN with SSID==’Café’ when you can hear 3G cell id==’1234’ “. For the terminal, the main benefit is battery saving: with the access network discovery information, the terminal can optimize e.g. WLAN scanning instead of using constant, periodic scans.

3. Inter-System Routing Policy (ISRP): ISRP policies were added into ANDSF in Release-10 that was just completed. The idea is that it is possible to identify different applications and define separate network policies for each application. ISRP policies can be applied for different 3GPP features: for example, for so called non-seamless WLAN offload ISRPs can be used to indicate what application traffic should be routed directly to the Internet.

In Figure 3, a part of ANDSF ISRP is shown. ISRP consists of three different parts, one is meant to be used 3GPP flow mobility solution (IFOM; based on DSMIPv6) and another one is for multi access PDN connectivity feature (MAPCON; the terminal can connect to the operator core via both 3GPP and WLAN access). The part of ISRP that is shown below on the figure is the third part: that is used to guide the terminal WLAN access per application. In 3GPP terminology, this is Non-Seamless WLAN Offload which in practice means a generic WLAN usage with the addition of having the possibility for the operator to instruct what traffic is routed via WLAN interface.

The two most important parts of the ISRP are marked as 1. and 2. in figure below. IPFlow – marked with 1. – defines what traffic this ISRP policy is applied for: in practice, the structure is a common IP 5-tuple that is widely used to identify packets e.g. in routing. RoutingRule – marked with 2. in the figure – defines what WLAN networks are preferred for the traffic identified with IPFlow IP 5-tuple: this is a preferred WLAN network list where the WLAN networks are identified with SSID. In short the logic is such that for traffic matching the IPFlow IP 5-tuple, the terminal should select the highest priority WLAN network available to route that specific traffic.

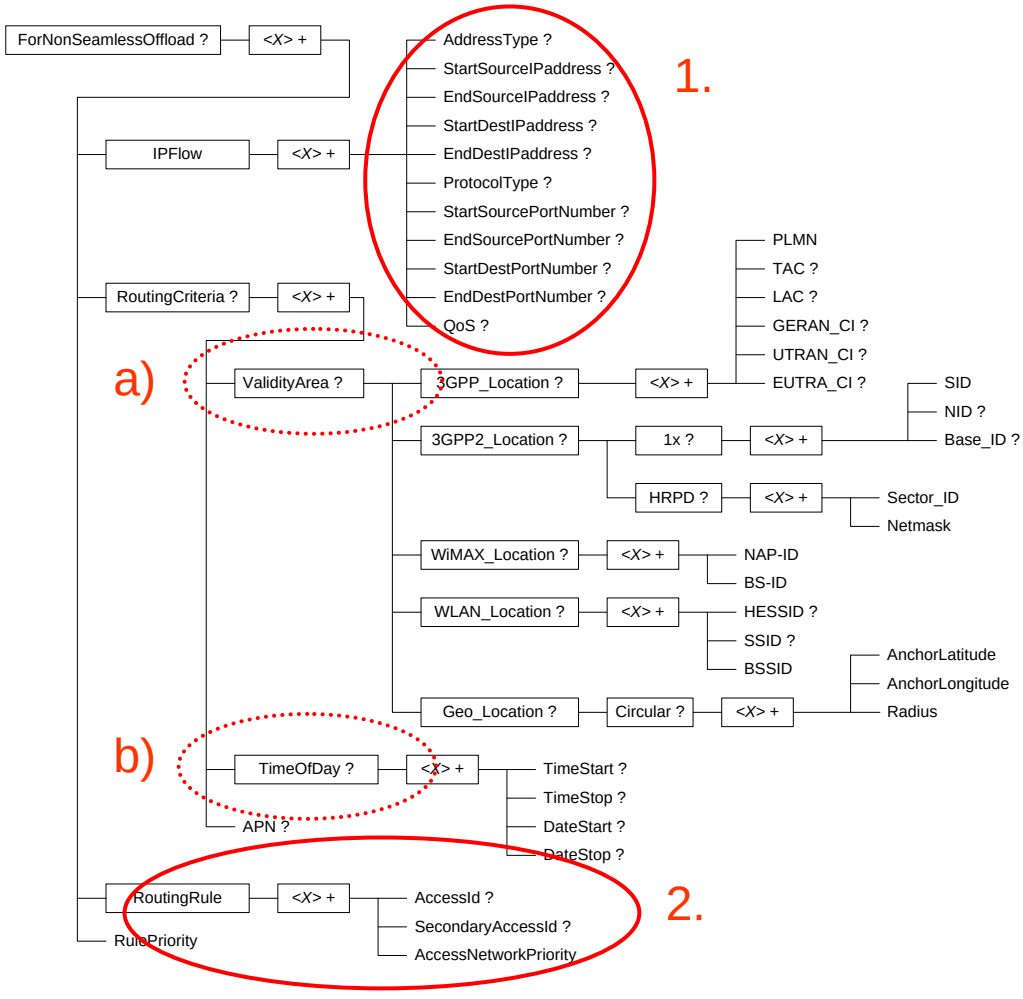

Figure 3. ANDSF ISRP policy for Non-Seamless WLAN Offload.

In addition to the above described features, ANDSF policies – i.e. ISMP and ISRP – both contain so called validity constraints, a) and b) in the figure above: with validity constraints, it is possible to define when an ISMP or ISRP is valid, i.e. when a certain policy can be applied. Validity can be defined in terms of location (geographical area, or based on e.g. cellular network identifiers, like tracking area or cell id, etc.) or time of day. With the validity constraints, the operator may define detailed policies that are applicable only where and when the operator wants to apply certain network selection criteria. The downside of this validity constraint definition possibility is that it potentially makes the policies complex to manage for the operator.

Currently, the work for Release-11 in 3GPP is already ongoing, although only in requirement definition phase. It seems the only work for ANDSF in Release-11 relates to how to better identify traffic than just with the traditional 5-tuple: the reasoning for that work is that nowadays it is common that the same IP address is used for a number of services, or the service is reachable from a number of IP addresses. Also, a lot of applications are for example using HTTP protocol and a single port to carry all the traffic. Thus, it may be difficult in real life to construct the IP 5-tuples in such a way that it matches the traffic the operator would like to offload, e.g. YouTube. The solution for this is worked on under Data Identification for ANDSF (DIDA) work item. Currently, the most promising solution for real life scenarios is to identify the application traffic simply with URI: for example, instead of 5-tuple (under IPFlow in Figure 3) the ANDSF server just identifies the traffic wanted to be offloaded with e.g. www.youtube.com. When the terminal receives such an ISRP policy with offloading information for www.youtube.com, the terminal is responsible to map this URI to IP 5-tuple or part of it (e.g. just a destination address) and form the local routing table entries for the YouTube traffic. In practice, terminal can find this information when performing the DNS query for the URI. This way, the management overhead for the operator to maintain the offload information in ANDSF server is minimized, and also the offload traffic identification is efficient in the terminal: there is no need to define all the possible destination addresses, for example, the terminal only maps the URI to really used destination address and forms its own routing rules based on that.

3.2 IETF Mechanisms

Unlike for example 3GPP, IETF as an organization does not specify systems, but components of a system. Further, IETF does not specify e.g. certain radio related functionality, instead the IETF mechanisms should be applicable on all different access technologies, whether it is 3GPP-based or WLAN.

For the access selection steering mechanisms, there are a number of different Internet drafts and few also RFCs available. Most of the related work in IETF is conducted within Multiple Interfaces (MIF) working group.

In this chapter, a short overview of the existing IETF mechanisms suitable for access steering is given. For the time being, both IPv4 and IPv6 based mechanisms will be needed. The transition to IPv6 networks has not really started commercially yet, but will happen in some future timeframe. Currently, IPv6 support on host side for PC/laptop form factor is pretty extensive on different operating systems, like Windows, Linux and MAC OS. However, the situation is a bit different on smart phone segment, where some platforms do have a good support (e.g. Symbian, Meego) while the others do not support IPv6 at all in practice (e.g. Windows Mobile 7, iOS 4).

3.2.1 General

What is common for the IETF access selection steering mechanisms is that they operate on packet routing level: regardless of the used mechanism, the network tells to the terminal to what first hop router / gateway the terminal should sent a specific traffic, or all traffic. Depending on the mechanism, this information is delivered with different protocols. In the following, mechanisms based on Router Advertisement of Neighbor Discovery Protocol and DHCP are considered.

3.2.2 IPv6: Router Advertisement

NOTE! The details of usage of Router Advertisement for WLAN offload is researched in another TEKES-funded project WiBrA (contact: Jouni Korhonen). Here, only the general functionality with available, public RFCs is described.

For IPv6, the Neighbor Discovery Protocol [5] is often used – among other things – for allocating IP addresses. When using IPv6 stateless address autoconfiguration [6], i.e. when address is not configured manually or with DHCP, the terminal relies on Neighbor Discovery Protocol: in general, the terminal sends a Router Solicitation message to a multicast address to request the receiving router to respond to it by sending its Router Advertisement message back to the terminal. Routers will also send Router Advertisement messages periodically, bit to speed up the address allocation, the terminal can send the Router Solicitation message. With IPv6 stateless address autoconfiguration, the Router Advertisement message contains prefix information option: the terminal forms its IPv6 address by combining the received prefix with a link-local address that is often generated from the interface's MAC address. Without describing all the details of the IPv6 stateless address autoconfiguration, this is how Router Advertisement is used in address allocation. It should also be noted that the way how the IPv6 addresses are allocated in practice depends on the deployment as well as the interface used: for example, 3GPP defines some tweaks of its own to the IPv6 address allocation process described above.

RFC 4191 [7] introduces new options for Router Advertisement message for communicating default router preferences and "more-specific routes" from routers to hosts. With default router preferences, it is possible to indicate also the preference for the terminal's "next-hop determination", as defined in RFC 4861 [5]. In practice, when a terminal is sending a packet to an off-link destination (i.e. through a router), the next-hop router to which the packet is forwarded is selected from the Default Router List. RFC 4191 brings the preference as additional selection criteria to this basic algorithm.

Additionally, the "more-specific routes" is introduced into Router Advertisement message. In practice, a new Router Advertisement option Route Information Option is added and its format is the following:

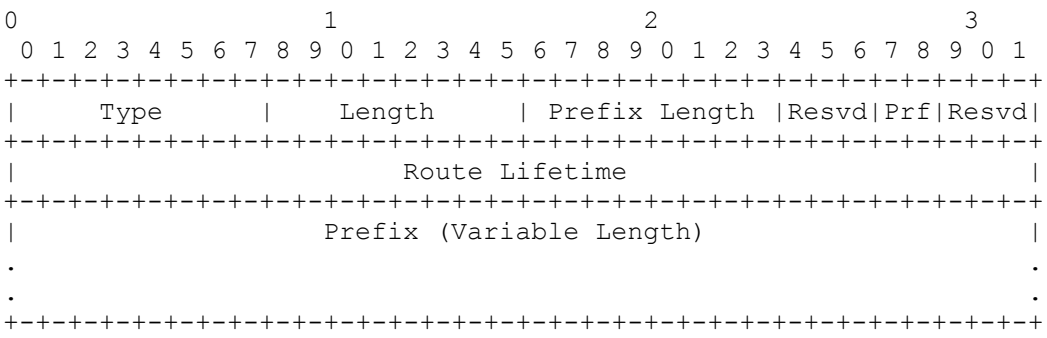

Figure 4. New Route Information Option to Router Advertisement message. [7]

The most significant fields are the Route Preference ("Prf") and Prefix fields. Route Preference can have three different values: high, medium (which is also default) and low. Prefix field contains an IP address or a prefix of an IP address. When a terminal receives a Router Advertisement message with information on Figure 4, the terminal will update its local routing table for each Route Information Option it received in the message.

When sending a packet, the terminal searches its local routing table to find the route with the longest prefix that matches the destination, using route preference values as tie-breaker if multiple matching routes have the same prefix length.

For example, assuming the terminal has received three Router Advertisement messages from the routers W, X and Y, and the terminal has corresponding three entries in its routing table:

Prefix: 2001::/16, Preference = High => router W
Prefix: 2001:db8::/32, Preference = Low => router X
Prefix: 2001:db8::/32, Preference = High => router Y

When the terminal is sending a packet destined to 2001:db8::1, the terminal first searches routing table entries with the longest prefix that matches with the destination address: for the router W, only 16 first bits with the prefix match, but for routers X and Y 32 bits matches. Thus, the terminal selects either the router X or Y as the next-hop router: now in this case, the preference value is used as tie-breaker for the router selection. Thus, the packet is sent to the router Y, the router with the longest prefix match and the highest preference.

So how can this be used in access selection steering? From the terminal point of view, behind each interface there can be one or more routers reachable. Basically, the terminal may receive Router Advertisement(s) from 3GPP and WLAN interfaces. This is potentially a source of conflict, if it is possible to receive Router Advertisements from two interfaces possibly identifying the same traffic (by prefixes). If the two networks, i.e. 3GPP and WLAN, are under the management of the same operator, it is possible to coordinate the Router Advertisement information delivered from both systems. However, more general setup would be achieved, if it is specified that in case the terminal has received Router Advertisements with "more-specific routes" information from 3GPP access, only those messages are treated as valid, i.e. the "more-specific routes" option(s) included in Router Advertisements from other interfaces are ignored.

The basic idea of applying Router Advertisements for access selection steering is that the router behind an interface informs the terminal explicitly about traffic the router wants the terminal to send to it.

Let's consider an example: the cellular operator wants the terminals to route important VoIP traffic via 3GPP interface to cellular core network, but all other traffic is treated bulk traffic that the operator wants to offload to WLAN, if available for a terminal. Further, in this example it is assumed WLAN network is not connected to EPC, i.e. the traffic sent over WLAN is routed directly to the Internet. Thus in practice, the two next-hop routers – the one behind 3GPP access, i.e. PDN GW, and the one behind WLAN radio access – can only be accessed through a single interface from the terminal point of view.

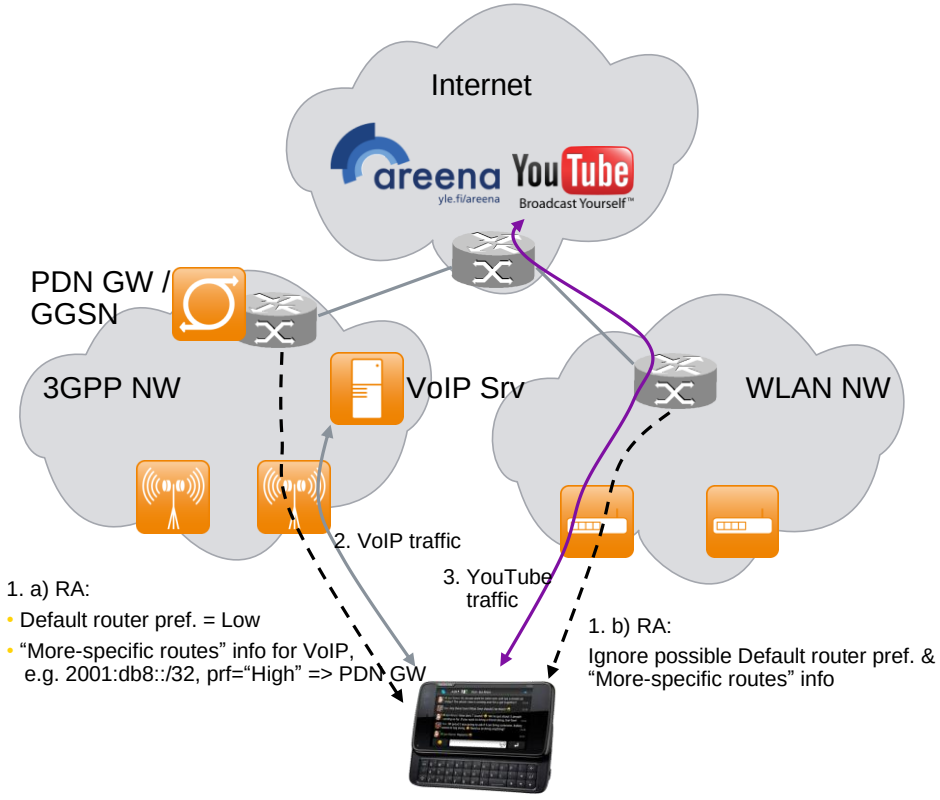

Figure 5. Offload with Router Advertisement.

Now in this example, PDN GW (or GGSN in case of 3G core network) sends a Router Advertisement specifying the value-added traffic – VoIP in this example – with "more-specific routes" option, indicating that the terminal should forward traffic matching the "more-specific routes" prefix(es) to PDN GW. Additionally, PDN GW may send a Router Advertisement message where Preference="Low" to indicate the terminal should treat PDN GW with low priority when selecting the default router for all other type of traffic. Thus, with this example, when there is VoIP traffic to send, the terminal selects the PDN GW as the next-hop router. This also automatically means that the VoIP traffic is sent over 3GPP radio access, since PDN GW is the next-hop router via 3GPP access from the terminal point of view. Further, for all

other type of traffic – i.e. traffic not matching VoIP "more-specific routes" prefixes – the terminal should treat the PDN GW as the least preferred router: in practice, the terminal should send all other traffic to some other next-hop router. Assuming the terminal is connected to WLAN, this other next-hop router is then the router behind WLAN air interface: in this scenario, all other traffic not matching the VoIP "more-specific routers" is then effectively offloaded to WLAN network. This scenario is illustrated in the Figure 5.

3.2.3 IPv6: DHCPv6

In addition to Router Advertisement -based solution described above, IETF is also working on a corresponding mechanism based on DHCPv6. This mechanism is defined in Interned draft draft-ietf-mif-dhcpv6-route-option-03 [8]. The basic idea is the same as with the Router Advertisement –based solution, but the information comes from DHCPv6 server, not a router: DHCPv6 server provides to the terminal information on next-hop address, i.e. a router, and a list of destination prefixes that represents the IPv6 destination prefixes reachable via the given next hop. Also –like the Preference field in Router Advertisement – there is a Metric field that indicates whether to prefer the next hop associated with this prefix over others, when multiple identical prefixes (for different next hops) have been received.

So, this is how the mechanism is used in high level: when a terminal – i.e. a DHCPv6 client – is interested in obtaining routing information from DHCPv6 server, it includes the new NEXT_HOP and RT_PREFIX options as part of its DHCPv6 Option Request Option (ORO) in messages directed to a server (i.e. DHCPv6 Solicit, Request, Renew, Rebind or Information Request messages). The server will provide the requested route information using one or more NEXT_HOP options in messages sent in response (i.e. DHCPv6 Advertise or Reply). The NEXT_HOP option specifies the IPv6 next hop addresses, i.e. the address of the intended next-hop router. Each NEXT_HOP option conveys in turn zero, one or more RT_PREFIX options that represents the IPv6 destination prefixes reachable via the given next hop, i.e. router. Each RT_PREFIX also contains the Metric field for that prefix and next hop address pair to prioritize the different received, identical prefixes (associated for different next hop address).

This DHCPv6-based access selection steering mechanism allows an operator an on demand and node specific means for configuring static routing information. Just like with Router Advertisement –based mechanism, it is possible to access DHCPv6 servers through different interfaces, i.e. through 3GPP access and WLAN. In order to avoid conflicts in cellular environment, it would be best to define that the terminal will follow the information received e.g. only from the DHCPv6 server accessible through 3GPP interface, and ignore NEXT_HOP and RT_PREFIX options received from any other DHCPv6 server, e.g. through WLAN.

In principle, the Router Advertisement –based and DHCPv6-based mechanisms offer the same functionality. However from WLAN offload point of view, the usage of DHCPv6 mechanism in 3GPP environment has challenges: DHCPv6 server is not a mandatory network element in an operator core where the IPv6 addresses are allocated without DHCPv6 server. Thus, the operator may not be too willing to install DHCPv6 server just for this functionality. On the other hand, different operators have different deployments, and it is perfectly possible to use DHCPv6 also in cellular environment.

Let's consider the WLAN offload example on Figure 5 in chapter 3.2.2: there, we want to route the operator's value-added VoIP service through 3GPP radio access to the operator core, but all other traffic is offloaded to WLAN and routed directly to the Internet (i.e. as described in chapter 3.2.2, 3GPP core network is not accessible through WLAN radio interface in the

example). The problem with the WLAN access with DHCPv6 mechanism is that in practice it is very difficult for the operator to know the next-hop router address behind the WLAN network the terminal happens to be connected (e.g. home WLAN, or whatever WLAN network). Basically, the only scenario, when the operator could know the next-hop address of the WLAN interface is when the WLAN is the operator's own network. So, with DHCPv6 it is safer just to specify the DHCPv6 options for the operators own next-hop router, i.e. PDN GW.

This is how the offload could work with DHCPv6: first, the terminal indicates it is interested in receiving the NEXT_HOP and RT_PREFIX options by sending an appropriate DHCPv6 request to the DHCPv6 server in 3GPP core network, as described above. As a response, DHCPv6 server provides the following information, the information only specifies options for the operator's own PDN GW in this example:

- NEXT_HOP option contains the next-hop address, i.e. the next-hop router address. In this case, it is the address of PDN GW (that is only accessible through 3GPP access in this example).

- RT_PREFIX option defines the prefix or prefixes (within multiple included RT_PREFIX options) that are reachable through the next-hop router defined in the NEXT_HOP option. RT_PREFIX field also contains the prefix length as well as the metric value for the prefix. The metric value means in practice a 'price' for the route, i.e. bigger the value, more expensive (= worse) the route is.

    - RT_PREFIX option 1 indicating prefix plus prefix length for VoIP (e.g. 2001:db8::/32). Metric set to a low value, e.g. to '1'.

    - RT_PREFIX option 2 indicating as short as possible prefix and prefix length for all other traffic (e.g. 2000::/3). Metric set to a high value, e.g. '250'. The idea is to make PDN GW (as indicated in the corresponding NEXT_HOP option field) to look really expensive route, and more importantly, to define the prefix so short that the standard IP routing algorithm trying to find the longest matching prefix very seldom hit the very short prefix of PDN GW: probably any other next-hop router, like the one behind WLAN access, will have longer prefix match, and thus that other router is selected as the next-hop router instead of PDN GW.

When the terminal receives the above information, it should modify its local routing table entries accordingly. When the terminal sends e.g. VoIP traffic (destination in the packets set to 2001:db8::1 in this example), the PDN GW indicated in the first RT_PREFIX gives the longest prefix match, and thus the packets are routed to PDN GW. Assuming the terminal is also attached to WLAN network, for all other traffic to be sent the longest prefix match is found (most probably, cannot guarantee) from another next-hop router than PDNG GW, in this example from WLAN next-hop router. Thus, all other than VoIP traffic is (most probably) offloaded to the WLAN.

3.2.4 IPv4: DHCPv4

RFC 3442 [9] defines the Classless Route Option for DHCPv4. In principle, the information delivered with that option is the same as above described for DHCPv6: with the Classless

Static Route Option, DHCP server can indicate to the terminal what router will be used when sending packets to specified destination(s).

For WLAN offload, DHCPv4 could be used just like DHCPv6 described in the previous chapter.

Currently, the DHCPv4 mechanism is the only IEFT mechanism available for access selection steering for IPv4-only systems.

3.2.5 IPv6 & IPv4 dual stacks

The Internet draft "Controlling Traffic Offloading Using Neighbor Discovery Protocol" [10] defines another mechanism for access selection steering specifically for the terminals having both IPv6 and IPv4 addresses allocated. The idea is that IPv6 Neighbor Discovery protocol message Router Advertisement is defined to carry a new option that can be used to manage also the usage of IPv4-only interfaces.

Currently, the terminals having both IPv6 and IPv4 addresses generally prefer IPv6 over IPv4 addresses when performing source and destination address selections. For example, a multi-interfaced terminals may have IPv6 enabled on a more 'expensive' (indicated with the Metric in the local routing table) interface and a 'cheaper' interface may have support only for IPv4. In such a scenario it might be desirable for the terminal to prefer IPv4 in communication instead of IPv6. [101010]

The above mentioned problem can occur, for example, when a terminal has simultaneously IPv6-enabled cellular connection and IPv4-only WLAN connectivity active. When connecting to dual-stack capable destinations it would oftentimes be generally more efficient to use WLAN network interface. Furthermore, a cellular network operator may want terminals to offload traffic away from cellular network whenever terminals have alternate network accesses available. [10]

In [10], a new option for Router Advertisement is defined: over IPv6 interface, Neighbor Discovery Offload Option can be used to indicate following:

- 'L' flag, i.e. Lower-than-IPv4 Preference flag: this flag indicates to the terminal that the router that sent this Router Advertisement message wants to be treated as lower preference than any possibly available IPv4 next-hop routers. With the 'L' bit set in the Neighbor Discovery Offload option indicates that the router should not be used for forwarding IPv6 traffic for destinations that are also reachable with IPv4 (via other interfaces) or for IPv6 destinations that are also reachable using other interfaces.

- 'D' flag, i.e. Default IPv4 Gateway Preference: this flag indicates the willingness of the Dual-Stack capable router (that originated the Router Advertisement) to serve as a default gateway for the IPv4 traffic. If 'D' flag is set (='1') then the router explicitly indicates it is not willing to serve as a default gateway for IPv4 traffic if there are other usable gateways present in the same or other available interfaces.

- Next-hop router IPv4 address: dual-stack capable router may indicate its IPv4 interface address with this parameter.

The described solution is intended to be used during transition towards IPv6, during which time multi-interfaced terminals are often likely to have network interfaces with IPv4-only capability.

A common scenario where coexistence of IPv4 and IPv6 network interfaces is expected to occur is when a smartphone has IPv6-enabled cellular connection and IPv4-only WLAN connection active at the same time. [10]

So how this mechanism can be used for access selection steering? First of all, as indicated above, this mechanism is only applicable for terminals having both IPv4 and IPv6 enabled interfaces at the same time. Just like with previous IETF mechanisms, it should be agreed that the terminals only follow the information received through 3GPP access, not from other accesses. The Internet Draft [10] defines few scenarios that illustrate how the mechanism can also be used for access selection steering. In the examples, it is assumed that WLAN interface does not provide Neighbor Discovery Offload Option (or, if it does, the information is ignored), even though WLAN interface would also be IPv6 capable.

Example 1: A terminal has obtained global IPv6 address, 2001:db8::2, on a cellular interface and with it has received Router Advertisement message including Neighbor Discovery option with 'lower-than-IPv4' preference. The terminal also has global IPv4 address, 192.0.2.2, on a WLAN interface.

When connecting to a dual-stack enabled destination, both 2001:db8::2 and 192.0.2.2 are considered as source addresses candidates. IPv4 address is selected, because 2001:db8::2 is considered deprecated, as indicated with the 'lower-than-IPv4' flag. Since the source address selection also defines what interface is used (the selected [source] address is allocated from that interface), the terminal uses WLAN for communication.

When connecting to IPv6-only destination, 2001:db8::2 is selected as the source address and cellular network used (2001:db8::2 allocated from cellular access), as there are no other IPv6 addresses available.

Example 2, dual-stack WLAN and cellular interfaces, cellular's IPv4 treated as not default route: A terminal has obtained IPv6 address, 2001:db8::2, and IPv4 address, 192.0.2.2, from cellular network. The cellular network has indicated 'lowert-han-IPv4' preference ('L' flag set to '1') for IPv6 and 'not your default router' ('D' flag set to '1') for IPv4. The terminal also has dual-stack WLAN access with 2001:db8:1::3 and 192.0.2.30 addresses allocated from WLAN network.

When connecting to IPv4-only destination, terminal selects 192.0.2.30 as the source address because default gateway on the interface of 192.0.2.2 address (i.e. cellular access) is 'not default gateway'. WLAN is used for communication.

When connecting to IPv6-only destination, terminal selects 2001:db8:1::3 from WLAN interface as the 2001:db8::2 is considered deprecated ('lowert-han-IPv4' preference received from cellular access, i.e. for 2001:db8::2 address, and 'not your default router' == true). WLAN is used for communication.

3.3 Wi-Fi Alliance HotSpot 2.0

In March 2011, Wi-Fi Alliance announced that it will start working on a new hotspot certification program [11]. This work is carried out in WFA HotSpot 2.0 working group. The new program will address authentication and provision of service for public Wi-Fi networks.

The aim of the WFA Hotspot 2.0 is to ensure that the end users can easily access hotspot networks from various providers. The vision is to provide an automated, cellular-like experience for Wi-Fi users around the world in security-protected service provider hotspots.

WFA draft specifications are only available for the members. Further, the draft specifications are confidential. At the time of writing of this report, WFA HotSpot 2.0 specification starts to get mature, but it is still in draft status. Thus, it is not possible to refer to WFA HotSpot 2.0 specification from this public document. Unfortunately, it means that WFA HotSpot 2.0 needs to be left out from this study for the time being.

If WFA can complete its work for HotSpot 2.0 within the lifetime of Future Internet program (before March 2012), it is possible that also this document is updated to cover the HotSpot 2.0 specification.

4 Co-existence of the Different Access Selection Mechanisms

Having the possibility to receive access selection steering information through multiple sources is a possible source of conflicts. For example, if ANDSF provides some network selection policy, but an IETF mechanism provides conflicting information, what should the terminal do? Here, it is assumed that there is a SIM card in the device, i.e. the user has made a subscription agreement with a cellular operator. This information can be exploited when deciding what information from what interface is followed.

For the SIM-less devices, the situation is trickier: if there is no SIM card in the device, it is not straightforward to define what interface or what mechanism should be followed with highest priority for access selection steering. Of course, if there is no SIM card in the device, it leaves out 3GPP-based mechanism, i.e. ANDSF, and then it is up to the different IETF mechanisms. However, most of the mechanisms described in the previous chapter are written from cellular operator point of view: thus, the co-existence of different IETF mechanisms for SIM-less devices is not considered further in this document.

4.1 IETF Mechanisms

As discussed in chapter 3.2, there are several possible IETF mechanisms that could be applied for access selection steering. DHCPv4 (chapter 3.2.4) is the only mechanism identified in this document for an IPv4-only terminal. However, a dual-stack terminal might receive access selection information with DHCPv4, dual-stack mechanism (chapter 3.2.5), DHCPv6 (chapter 3.2.3) and/or with Router Advertisement (chapter 3.2.2). And IPv6-only terminal could receive that information with DHCPv6 and/or Router Advertisement –based mechanisms. Since the information received from different IETF mechanisms is pretty much similar to each other, it is

very easy to receive conflicting information with different mechanisms, of course assuming all the different options are supported. Further, if considering only a single IETF mechanism, that single mechanism may also be applied on different interfaces – e.g from terminal point of view, on WLAN, 3GPP or wired accesses – possibly providing conflicting information from different interfaces.

Assuming there is the SIM card in the terminal, it is easy to define that the terminal will only interpret the access selection steering information (as described in chapter 3.2) received from 3GPP network.

It should be noted that the terminal may be connected to mobile core network via both 3GPP and WLAN radio accesses. In that case, the terminal could receive access selection steering information from both interfaces. However, the terminal knows when it is connected to the mobile core network, and for access selection steering information it does not really matter through which interface it was received: it is the responsibility of the operator to make sure that the access selection steering information is not conflicting, if it is possible to receive through both 3GPP and WLAN interfaces.

As was mentioned earlier in 3.2.3, DHCP server is not normally deployed in 3GPP mobile core network. Thus, the mechanisms relying on DHCP are less likely to be implemented in cellular environment.

However, just like in any other IP networks, also mobile core networks need to implement router functionality. For example, the PDN GW can be configured to send e.g. Router Advertisement messages to the terminals. Thus, from cellular operator point of view, the mechanisms relying on Neighbor Discovery protocol (and Router Advertisement) are the most promising ones. Especially for the mechanism described in 3.2.2, there are operating systems already supporting the required functionality (Linux, Windows, Mac OS, MeeGo). The downside is that it requires IPv6, and that is not currently well supported within the smartphones.

4.2 3GPP and IETF Mechanisms

For the access selection steering mechanisms, 3GPP has been working on ANDSF, as described in 3.1. In cellular environment, the mechanisms defined in 3GPP have traditionally had a strong position also in the eyes of the mobile operators. However, for the access selection steering it is not at all clear that cellular operator will prefer 3GPP-specified ANDSF functionality.

What is common to all IETF mechanisms described earlier is that they only can provide access selection steering information only **after** the terminal has made the selection to access e.g. certain WLAN network. Thus, with IETF mechanisms it is not possible to provide hints for access network selection before the selection decision, i.e. when the information actually would be needed. However, ANDSF can be used for that: either Rel-8 ISMP policies or Rel-10 ISRP policies can be used to prioritize available WLAN network prior the access network selection.

As was described in 3.1, the ISMP policy is "terminal-wide" network selection policy (list of prioritized networks), meaning that the same policy is applied regardless of the applications used. The ISRP policy adds to this basic functionality the possibility to define to what applications the network selection policy applies: for example, for VoIP traffic, select some defined WLANs in a prioritized order. From three different usages of ISRP, the most important

is the one that is used for so called Non-Seamless WLAN Offload (3GPP name for a feature, where the ANDSF policies can be used to guide what traffic is offloaded to different defined networks). This part of ISRP contains more or less the same information for access selection steering as the different IETF mechanisms. Thus, this ANDSF information can conflict with an IETF mechanism information used at the same time.

As mentioned in 3.1, ANDSF information is pretty static by nature. For example, if the static ANDSF policies should be modified dynamically, e.g. due to some event in the network, it will take quite some time before the new policies are updated to the terminals. However, IETF mechanisms can easily operate in a dynamic environment: whenever there is need to send a new access selection steering information, a router just broadcasts new Router Advertisement message, and it is immediately taken into use in all active terminals supporting the mechanism.

Thus, the best combination of access selection steering functionalities is to combine the ANDSF network selection policies together with the dynamic features of IETF mechanisms, and especially in cellular environment the mechanism(s) relying on Router Advertisement.

In practice, there are two options:

1. ANDSF ISMP network selection policy information is used for WLAN network selection. Router Advertisement –based mechanism is used to deliver information what application is to be offloaded.

2. ANDSF ISRP (from ForNonSeamlessOffload node, refer to figure Figure 3) is used for WLAN network selection and for providing information on what application traffic to offload. With Rel-11 functionality, it is possible to identify the application traffic by URIs, greatly reducing the management overhead of the operator (when compared to identifying all traffic by IP 5-tuples). Router Advertisement –based mechanism can also be used to deliver information what application is to be offloaded. In case there is conflict with ISRP and RA information, RA information takes precedence.

5 Conclusions

On this paper, different access selection steering mechanisms from 3GPP and IETF were considered. Mainly, the different mechanisms were considered from cellular network operator point of view. For cellular environment, the Router Advertisement –based mechanisms were identified more suitable than DHCP based mechanisms. For the co-existence of the ANDSF and Router Advertisement –based mechanisms, two options were defined to take most of the both systems.

6 References

[1] Realization of Policy-Based Resource Management Concept, version 1.0, 16th of February 2010, Janne Tevonen & Jari Mustajärvi.

[2] 3GPP TS 23.402, Architecture enhancements for non-3GPP accesses, Release 10, v10.4.0, June 2011.

[3] 3GPP TS 24.302, Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks, Release 10, v10.4.0, June 2011.

[4] 3GPP TS 24.312, Access Network Discovery and Selection Function (ANDSF) Management Object (MO), Release 10, v10.3.0, June 2011.

[5] Neighbor Discovery for IP version 6 (IPv6), IETF RFC 4861, T. Narten et al., September 2007.

[6] IPv6 Stateless Address Autoconfiguration, IETF RFC 4862, S. Thomson et al., September 2007.

[7] Default Router Preferences and More-Specific Routes, IETF RFC 4191, R. Draves et al., November 2005.

[8] DHCPv6 Route Options, Internet Draft, draft-ietf-mif-dhcpv6-route-option-03, W. Dec et al., September 10, 2011.

[9] The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4, IETF RFC 3442, T. Lemon et al., December 2002.

[10] Controlling Traffic Offloading Using Neighbor Discovery Protocol, Internet Draft, draft-korhonen-mif-ra-offload-02.txt, J. Korhonen et al., September 2011.

[11] Wi-Fi Alliance press release: "Wi-Fi CERTIFIED™ Hotspot Program to Ease Subscriber Connectivity in Service Provider Wi-Fi® Hotspots", March 22, 2011, http://www.wi-fi.org/news_articles.php?news_id=1048