Service Based Access Selection with PBRM

Future Internet Program of TIVIT,

Activity 2.4 Deliverable DA2.2.21

Contributors:

Pasi Seittenranta, NSN
Janne Tervonen, NSN

Abbreviations and Terminology

3GPP	3rd Generation Partnership Project
AMBR	Aggregated Maximum Bit Rate
ANDSF	Access network discovery and selection function
APN	Access Point Name
API	Application Programming Interface
ARP	Allocation and Retention Priority
BBERF	Bearer binding event reporting function
DL	Downlink
DM	Device Management
DSMIPv6	Dual Stack Mobile IPv6
EDGE	Enhanced Data rates for GSM Evolution
EPC	Evolved packet core
EPS	Evolved packet system
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network (4G)
GBR	Guaranteed Bit Rate
GERAN	GSM EDGE Radio Access Network, 2G
IAP	Internet Access Point
IANA	Internet Assigned Numbers Authority
IMS	IP Multimedia Subsystem
IP-CAN	IP connectivity access network
LTE	Long Term Evolution
MAPIM	Multi Access PDN Connectivity and IP Flow Mobility
MBR	Maximum Bit Rate
Monami6	Mobile nodes and multiple interfaces in IPv6
NWDS	Network discovery and selection
OMA	Open Mobile Alliance
PBRM	Policy Based Resource Management
PCC	Policy and charging control
PCEF	Policy and charging enforcement function
PCRF	Policy control and charging rules function
PDN	Packet Data Network
QCI	QoS class identifier
QoS	Quality of Service
RTP	Real-time Transmission Protocol
SAE	System Architecture Evolution
SIP	Session Initiation Protocol
SPR	Subscription profile repository
SSID	Service Set Identifier
TFT	Traffic flow template
UL	Uplink
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Access Network (3G)
VPN	Virtual Private Network
WiMAX	Worldwide Interoperability for Microwave Access

1. Introduction

This document is deliverable DA2.2.21 for the Future Internet program of TIVIT. During the first program year, Policy-Based Resource Management (PBRM) work was conducted in its own activity 2.4 under work package 2. For the second program year, PBRM will be merged into activity 2.2. The PBRM concept itself is defined in earlier FI deliverable [1].

User equipments that are capable to use several access networks, e.g. 3GPP GERAN/UTRAN/E-UTRAN, WLAN and WiMAX, are becoming common. However it is typically possible to use only one access network at a time and the mechanisms to choose appropriate network are not satisfactory. Selecting access for each traffic flow of an UE individually might give the following benefits:

- Service QoS requirements are fulfilled better. E.g. voice connection could use 3GPP network while FTP file download is using WLAN.
- There is a business opportunity in charging premium rates for prioritized treatment of high value traffic.
- Low priority traffic can be blocked in case of network overload or due to UE capacity limitations. E.g. users may generate excessive amount of peer-to-peer traffic for file sharing if flat fees are used, and operator needs to limit it to prevent network overload.

This document describes how service based access network selection could be implemented to systems with both 3GPP and non-3GPP access networks. Also, the possible role of PBRM in service based access network selection is discussed. The system for service based access network selection should fulfill the following requirements:

- UE (laptop or handheld) should be able to use more than one access concurrently.
- Access for each traffic flow can be selected individually (or blocked) taking into account characteristics of the flow, operator’s policies and user’s preferences.
- Mobility of traffic flows between accesses can be done using similar criteria as in initial network selection.

The latest finalized 3GPP release (Release 8) defines a new Evolved Packet System (EPS). EPS supports also connecting non-3GPP radio accesses to the same core network as 3GPP radio accesses. In practice, this means that WLAN and WiMAX radio accesses can utilize the same core network services as 3GPP radio accesses. In this document, it is assumed that 3GPP-defined EPS core network is used: radio accesses maybe based 3GPP or non-3GPP technologies. EPS architecture and the functionality of different network elements are not thoroughly explained in this paper: it is assumed the reader already has some knowledge on EPS as well as related IETF technologies.

2. Service based access selection overview

2.1 Filtering

Downlink traffic flows should be filtered, i.e. routed to selected access network or possibly dropped, in operator’s network (in PDN gateway; edge router between operator cellular core network and external packet networks). This is called forward filtering. Uplink traffic flows should be filtered in UE, and it is called reverse filtering.

UL and DL traffic flows may have different QoS requirements and also the access links may be asymmetric. Therefore in optimal solution, UL and DL direction traffic flows can be filtered independently. In practice, this separation of directions may be impossible and both directions must be routed through the same access network.

In filtering, IP packets of a flow can be identified by source/destination IP addresses, port numbers and transport protocol type. Filtering decision is based on operator’s policies, user’s preferences, QoS requirements etc. For this, the traffic flow should be identified somehow. This subject is discussed in section 5.

Next section describes what deployment alternatives we have in filtering.

2.2 Functional split between UE and network

Service based access selection decisions can be done either in UE or in operator’s network. Limited functionality may be possible without assistance from the other side, but to allow full featured access selection, both sides must contribute.

In UE based solution without support from operator’s network, operator’s access selection policies must be preconfigured to UE and can not be changed easily. Service based forward filtering could be possible using Mobile IP extensions described in section 4. In network assisted alternative network can send new service based access selection policies to UE. This can be done by e.g. extending PBRM functionality.

Network controlled solution without UE support does not seem to be feasible, as the network can not force UE to use selected non-3GPP access currently. However, network could decide the access e.g. based on selected QoS characteristics provided that UE has already attached to a non-3GPP network.

Section 7 describes EPS based solutions.

2.3 Enhancements to UE and network

If applications of a UE need to have simultaneous active connections to more than one access network, several enhancements need to be done in both the UE and network side. In this document, it is assumed that one 3GPP network and one non-3GPP network can be used simultaneously.

First, the UE must support dual-radio operation. A feasible combination is GERAN/UTRAN/E-UTRAN and WLAN. E.g. radio interference and energy consumption may restrict the possibilities to use other combinations.

Mobile IP (DSMIPv6) usage in UE and operator’s network needs to be enhanced so that one UE can have multiple care-of addresses. Current status in IETF standardization is described in section 4.

UE should be able to attach to two networks so that the traffic can be routed through both accesses. E.g. Release 8 EPS is not able to do this. Also handovers within and between 3GPP and non-3GPP connections should be done per PDN connection, and not per UE as is traditionally done.

3. Current Practices for Multiple Interface Hosts

This section is from [2]. Subsections 3.1 and 3.2 describe current access selection mechanisms in two common operating systems. Subsection 3.3 discusses the subject in more general level.

3.1 Nokia S60 3rd Edition, Feature Pack 2

S60 uses the concept of an Internet Access Point (IAP) that contains all information required for opening a network connection using a specific access technology. A device may have several IAPs configured for different network technologies and settings (multiple WLAN SSIDs, GPRS APNs, dial-up numbers, and so forth). There may also be 'virtual' IAPs that define parameters needed for tunnel establishment (e.g. for VPN).

For each application, a correct IAP needs to be selected at the point when the application requires network connectivity. If multiple applications utilize the same IAP, the underlying network connection can typically be shared.

The IAP for an application can be selected in multiple ways:

- Statically: e.g. from a configuration interface, via client provisioning/device management system, or at build-time.
- Manually by the user: e.g. each time an application starts the user may be asked to select the IAP to use. This may be needed, for example, if a user sometimes wishes to access his corporate intranet and other times would prefer to access the Internet directly.
- Automatically by the system: after the destination network has been selected statically or dynamically.

S60 3rd Edition, Feature Pack 2, introduces a concept of Service Network Access Points (SNAPs) that group together IAPs that lead to the same destination. This enables automatic or manual selection of the destination network for an application and leaves the problem of selecting the best of the available IAPs within a SNAP to the operating system. IAPs in the

SNAP list are prioritized, and the operating system should first consider the highest priority IAP, i.e. access, when selecting a new access network for an application.

When SNAPs are used, it is possible for the operating system to notify applications when a preferred IAP, leading to the same destination, becomes available (for example, when a user comes within range of his home WLAN access point), or when the currently used IAP is no longer available and applications have to reconnect via another IAP (for example, when a user goes out of range of his home WLAN and must move to the cellular network).

It is possible to configure SNAP lists on the UE remotely from an operator server that supports OMA DM based device configuration framework. Typically, this kind of feature is implemented in device management solutions provided by major network equipment manufacturers, like NSN.

3.2 Microsoft Windows

It is possible, although not often desirable, to configure default routers on more than one Windows interface. In this configuration, Windows will use the default route on the interface with the lowest routing metric (i.e. the fastest interface). If multiple interfaces share the same metric, the behavior will differ based on the version of Windows in use. Prior to Windows Vista, the packet would be routed out of the first interface that was bound to the TCP/IP stack, the preferred interface. In Windows vista, host-to-router load sharing [RFC4311] is used for both IPv4 and IPv6.

3.3 Common solutions

Essentially all operating systems use the same types of information to make decisions about multiple-interface operation: user input, operator/administrator provided information, and what has been statically configured or hard-coded. It is possible to design clever ways for tackling the problems related to multi-homing from the set of dynamically available information, vendor specific policies and design decisions.

It seems to be common practice to have a centralized connection manager entity, which does the network interface selection based on application input. The information used by the connection manager may be programmed into an application, learned from the users, or provisioned.

Routing tables are not typically used for network interface selection, as the criteria for network selection is not strictly IP-based but is also dependent on other properties of the interface (cost, type, etc.). Furthermore, multiple overlapping private IPv4 address spaces are often exposed to a multiple-interface host, making it difficult to make interface selection decisions based on prefix matching.

4. Mobile IP extensions

Dual Stack Mobile IPv6 (DSMIPv6) is used to handle mobility of UE in logical S2c interface between UE and PDN gateway in 3GPP EPS architecture (see Figure 2 in chapter 7 for an overview of EPS architecture). DSMIPv6 extends Mobile IPv6 to register an IPv4 care-of address instead of the IPv6 care-of address when the mobile node is attached to an IPv4-only access network. It also allows the mobile node to acquire an IPv4 home address in addition to an IPv6 home address for use with IPv4-only correspondent nodes. In order to route multiple IP flows to different accesses, extensions are needed. Sections 4.1 and 4.2 introduce ongoing IETF standardization work.

4.1 Multiple Care-of Addresses Registration

According to the current Mobile IPv6 specification, a mobile node may have several care-of addresses, but only one, called the primary care-of address, that can be registered with its home agent and the correspondent nodes. To get Internet access through multiple accesses simultaneously, UE needs to be configured with multiple active IPv6 care-of addresses. IETF draft [5] proposes extensions to the Mobile IPv6 protocol to register and use multiple care-of addresses.

4.2 Flow Bindings in Mobile IPv6

In [5] Mobile IPv6 is extended to allow the binding of more than one care-of address to a home address. IETF draft [6] further extends Mobile IPv6 and DSMIPv6 to allow it to specify policies associated with each binding. A policy can contain a request for a special treatment of a particular IPv4 or IPv6 flow, which is viewed as a group of packets matching a flow descriptor. Hence, [6] allows a mobile node to bind a particular flow to a care-of address without affecting other flows using the same home address. In addition, it allows binding a particular flow to a particular care-of address directly with correspondent node and mobility anchor point.

In [6], a flow is defined as a set of IP packets matching a flow descriptor. A flow descriptor can identify the source and destination IP addresses, transport protocol number, the source and destination port numbers and other fields in IP and higher layer headers. Specification [6], however, does not define flow descriptors and it is assumed that one or more ways of defining flow descriptors are going to be defined in other specifications.

Using the flow identifier option introduced in [6] a mobile node can bind one or more flows to a care-of address while maintaining the reception of other flows on another care-of address. Requesting the flow binding can be decided based on local policies within the mobile node and based on the link characteristics and the types of applications running at the time. Such policies are outside the scope of this document.

5. Identification of traffic flows

Table 1 and Figure 1 predicts what kind of devices (laptop vs. handheld) and applications will be used in mobile networks in the future.

Global monthly traffic	2007	2015		
		low	average	high
Wireless voice (PB)	90	159	159	159
Laptop (PB)	6	100	1000	7000
Handheld (PB)	0.5	50	900	2900
Per data sub (MB)	90	250	760	2700

Table 1: Traffic growth in mobile networks[1]

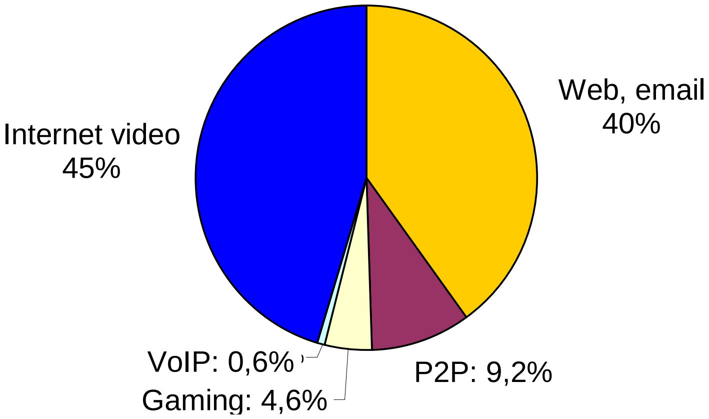

Figure 1: Applications in 2015 (average)[1]

In order to select suitable access for an application, its QoS requirements should be known. There are following possibilities to identify traffic flows:

1. User manually enters the required information to a software component in UE.
2. Application informs operating system when it starts a new flow. Current mobile devices use this method. Also IMS could inform the flow type in session establishment.
3. A software component in UE detects starts and ends of traffic flows and identifies them using techniques described below. No user intervention or application customization is needed, but traffic monitoring may consume limited UE resources.
4. Network can monitor the traffic instead of UE e.g. in PDN gateway.

[1] Source: Nokia-Siemens Networks, spring 2008

There are several methods that can be used to identify monitored traffic. The methods below are used in Nokia-Siemens Networks Flexi-ISN product (see [4]). In order to build an efficient implementation for traffic flow identification, all of the below described methods should be applied.

5.1 TCP/UDP port numbers

TCP/UDP port numbers range from 0 to 65535 and are divided to three categories.

- Well known ports have been assigned by IANA and range from 0 to 1023. Many common applications like e-mail, WWW, FTP use these ports when communicating with corresponding servers.
- IANA registered ports range from 1024–49151. Companies can register these ports for certain purposes.
- Dynamic/private ports range from 49152-65535. They are not permanently assigned to any publicly defined application and therefore can be used for any communication over TCP/UDP.

IANA registered ports can then be used to identify traffic flows. This method is efficient from a performance point of view and it works also when encryption is used. However IANA port assignments are only recommendations. Therefore sometimes ports are used for different applications or protocols than assigned by IANA. E.g. almost all P2P protocols use variable or well-known non-P2P protocol port numbers (HTTP, FTP, etc.) to avoid port-based identification and to enable firewall traversal. Also this method cannot automatically adapt to protocol changes or the introduction of new protocols.

5.2 Signature detection

Usually protocols have distinct fingerprints that can be used to identify a traffic flow belonging to a particular application. These fingerprints may include port numbers, bit string, ASCII characters etc. These fingerprints are collected in first stage from RFCs, public documents or by reverse engineering and empirically deriving a set of distinct bit strings by monitoring protocols. Once a database of fingerprints is built up then signature matching is performed by inspecting packet contents and/or header.

In some services, control flows are separated from service flows and therefore such service flows have no characteristic based on which they can be identified. In this case control flow is identified and a specific application layer gateway is selected to resolve corresponding service flows based on control flow protocol information.

For example SIP and H.323 protocol communications can be identified using this technique. Both of these protocols exchange signaling before acquiring data channels and data channels are always voice flows encapsulated in RTP format. However, only inspecting RTP flow cannot give any information about protocol used to setup the flow. Therefore complete analysis requires inspection of SIP and H.323 protocol signaling.

Signature matching based identification is accurate method. Disadvantages are that these methods cannot automatically adapt to protocol changes or the introduction of new protocols, analysis may generate significant processing load and encryption may prevent using these methods.

5.3 Network/transport layer heuristics

Behavior patterns can be identified from the monitored traffic based on prior study of application or protocol behavior. E.g. source and destination addresses of traffic flows can be analyzed and statistical information, such as packet size distribution and inter-arrival time, can be measured.

This kind of approach can be used to identify e.g. QoS requirements of flows or detect P2P traffic. It can be applied also to unknown protocols and encrypted traffic.

6. Release 8 EPS packet filtering

Release 8 is the latest 3GPP set of specifications that define Evolved Packet System (EPS). EPS consists of different radio accesses – like Long-Term Evolution (LTE) – connected to a new core network, called System Architecture Evolution (SAE). In practice, EPS is the 3GPP solution for 4G systems. The general EPS architecture is briefly described in chapter 7, and Figure 2 represents EPS architecture in high level. Due to new system architecture, also the bearer (i.e. connection) concept was revised.

In Release 8, EPS packets can not be filtered to different access networks (i.e. it is possible to use only one access network at a time), but there is filtering mechanism to differentiate service types with different QoS. This text is mainly from [7].

To fulfill end-to-end QoS guarantee for IP Multimedia System (IMS) services, 3GPP proposed an IP-connection based Policy Decision Function (PDF) in 3GPP Release 6. In the subsequent Release 7, the PDF and Flow Based Charging (FBC) specified in Release 6 were then combined, and the Policy and Charging Control (PCC) [10] subsystem was added between the service control layer and the access/bearer layer to implement resource admission control function. In practice, PCC is implemented in Policy Control and Charging Rules Function (PCRF) network element (refer to Figure 2).

A bearer is the basic level of QoS control granularity in Release 8 EPS, that is, all data traffic on the same bearer are granted identical QoS guarantee and various types of QoS guarantees can be provided for different bearers. An EPS bearer can be deemed as a logical circuit between UE and Packet Data Network Gateway (PDN-GW) (refer to Figure 2). EPS QoS mechanism is implemented based on the QoS Class Identifier (QCI) parameter, which can be used to supersede over a dozen of parameters in UMTS, that is, the evolved NodeB (eNodeB, the base station in LTE radio access system) can deduce all parameter features from QCI.

In EPS, the bearer level QoS parameters include QoS Class Identifier (QCI), Allocation and Retention Priority (ARP), Guaranteed Bit Rate (GBR), Maximum Bit Rate (MBR) and Aggregated Maximum Bite Rate (AMBR). QCI and AMBR are newly added into EPS, while other parameters are inherited from UMTS.

Both GBR and non-GBR bearers have values for QCI and ARP. As an order of magnitude, QCI refers to access point parameters used to control bearer level packet transfer, e.g. scheduling weights, admission thresholds, queue management thresholds, and link layer protocol configuration. ARP is used to determine whether to accept or reject the requests of establishing or modifying bearers in case of limited resources, and which bearer needs to be discarded in case of special resource limit (e.g., at handover). After a bearer is successfully established, ARP shall not have any impact on the bearer level packet transfer and processing.

Besides QCI and APR, every GBR bearer is also associated with GBR and MBR values. GBR bearers are mainly used to carry voice, video and real-time gaming services through dedicated bearers or static scheduling. The GBR represents the bit rate that can be expected to be provided by a GBR bearer, while the MBR indicates the upper limit for transferred bit rate of GBR bearer. On the following table, the different fixed QCI classes are shown. Additionally, an operator may define its own sets of parameters for new QCI classes, if e.g. there is need for a new class after introduction of some new, fancy application.

QCI	*Resource type*	*Priority*	*Packet delay budget (ms)*	*Packet loss rate*	*Example services*
1	GBR	2	100	1e-2	Conversational voice
2	GBR	4	150	1e-3	Conversational video
3	GBR	5	300	1e-6	Non-conversational video
4	GBR	3	50	1e-3	Real time gaming
5	Non-GBR	1	100	1e-6	IMS signaling
6	Non-GBR	7	100	1e-3	Interactive gaming
7	Non-GBR	6	300	1e-6	TCP-based:
8		8			WWW, e-mail, FTP,
9		9			p2p file sharing,…

Table 2: QCI characteristics

Packet filtering into different bearers is based on Traffic Flow Templates (TFTs). The TFTs use IP header information such as source and destination IP addresses and TCP port numbers to filter packets such as VoIP from web browsing traffic so that each can be sent down the respective bearers with appropriate QoS. UL TFT associated with each bearer in the UE filters IP packets to EPS bearers in the uplink direction. DL TFT in the PDN GW is a similar set of DL packet filters.

To set up a new traffic flow, UE signals to the operator’s application server to set up the end-to-end service. This is done on the application layer using the always-on default bearer. The signaling may indicate known service or include QoS parameters. The application server shall then request the set-up of the corresponding EPS bearer through the PCC infrastructure.

The usage of TFT filters with service based access selection is further described in the following chapter.

7. Service based access selection based on Release 8 EPS

Release 8 EPS introduced a multi access 3GPP system where different heterogeneous access systems are connected to a common core network (see Figure 2). However, in Release 8 EPS, the subscriber cannot communicate using multiple simultaneous accesses. The subscriber can establish one or more simultaneous PDN connections in Release 8 EPS, but all the traffic of a UE is routed through the same access system.

In Release 8 the PDN connection level operations are generally initiated by the UE. Without major architecture changes these UE initiated procedures can be extended to support multiple simultaneous PDN accesses. In the following, two options for realizing service based access selection in EPS system are discussed briefly.

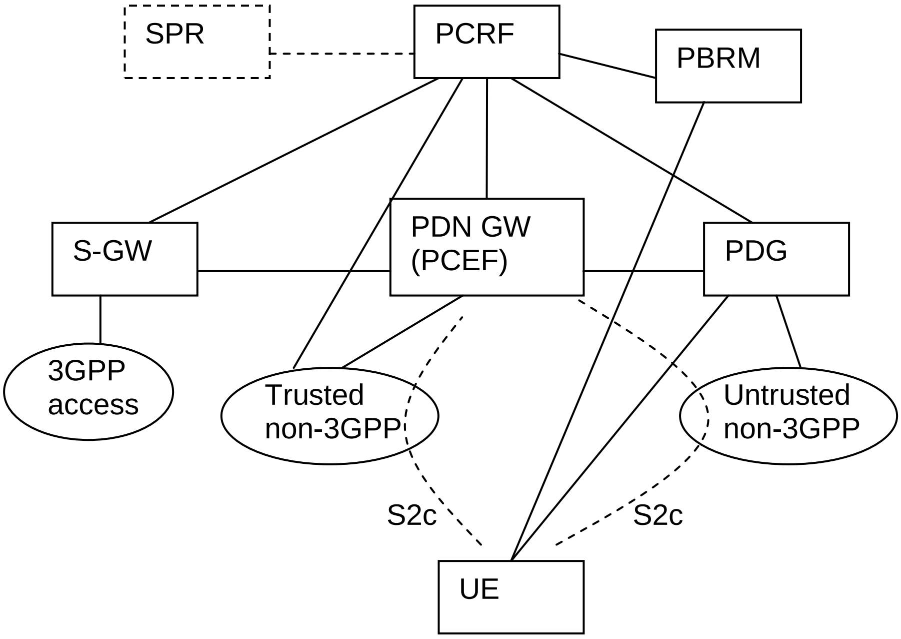

Figure 2: EPS architecture in high level (PBRM not part of the 3GPP architecture). [8]

7.1 Architecture alternatives

Two architecture alternatives are given below. In the former, UE decides the access network, but operator can restrict the access to certain networks. In the latter, operator has more control in the access selection, but the UE can still decide whether it attaches to a certain non-3GPP network or not.

1. User manually or UE automatically decides which access networks it attaches to, e.g. based on information provided by PBRM server. Operator can restrict service usage in certain access networks depending on user's subscription. UE decides what access it uses for a service taking into account network selection information and operator's policies provided by PBRM server. Then UE binds the flow to an access by sending an IP flow description and access network identifier to PCRF. The description is then associated to corresponding care-of address in home agent (see Table 3). Home agent does forward filtering to selected access first and then TFTs are used to filter the flow to an EPS bearer using that access based on QoS requirements. Similar kind of solution is described in a 3GPP technical report [9].

Home Address	Routeing Address	Binding ID	Flow ID	Routeing Filter
HoA1	CoA1	BID1	FID1	Description of IP flows…
			FID2	Description of IP flows…
HoA1	CoA2	BID2	FID3	…

Table 3: IP flow binding in home agent.

2. User/UE decides which access networks it attaches to. After that, network can select between the available accesses when establishing a new EPS bearer. In practice, this means that new connections (or EPS bearers) can only be established via the radio access networks UE has decided to enable beforehand. TFTs set by extended PCRF are used to filter flows to bearers using any access. Operator can restrict service usage in certain access networks depending on user's subscription. UE may receive this information from PBRM server to avoid useless attachments.

7.2 Extensions to network elements

In order to realize one of the above options for service based access selection, some modifications for EPS core network elements are required. These are shortly summarized on the following sub-chapters.

7.2.1 PCC extensions

Policy and Charging Control (PCC) architecture is defined in [10]. PCC architecture contains several network elements: in Figure 2, PCRF, SPR and PCEF are part of PCC. Although it has a fancy name, PCC main responsibility is to ensure the bearer (i.e. connection) establishments get their QoS requirements fulfilled. In that, PCRF is the central network element.

7.2.1.1 Policy Control and Charging Rules Function (PCRF) and Policy and Charging Enforcement Function (PCEF) extensions

PCRF and PCEF needs to be extended so that simultaneous active 3GPP and non-3GPP access is possible. DSMIPv6 should be extended to support multiple care-of addresses and IP flow routing as described in section 4. Access and QoS selection rules need to be enhanced so that traffic flows can be categorized using service type or QoS parameters.

Extended PCEF should provide information about available access systems to PCRF. Filtering rules must be updated when new access network for the UE becomes available or a connection to an access network is lost. If UE does not provide serviced type information, PCEF may need to detect the service type using the methods described in section 5.

7.2.1.2 Subscription Profile Repository (SPR) extensions

SPR should be enhanced to indicate to extended PCRF what services can be transferred using each access network. Users can be divided into different classes based on their subscription. In practice, SPR will be implemented as part of other subscriber management entities in operator networks.

7.2.2 PBRM in service based access selection

PBRM can be used to deliver network selection information from the network to the UEs. UE contacts PBRM server using IP connection, so it is not possible to get PBRM information before any connection to network is made. This means in practice that UE cannot contact PBRM server before every network selection event separately: the PBRM server should provide information that UE can use in all (or most) future network selections.

Since by nature service based access selection requires using of several radio accesses simultaneously, the information PBRM provides cannot be tied to a single radio access technology. Further, it is not practical to define PBRM information for each application separately: when a new application was introduced, it would require modifications to PBRM data base. This means that the best option would be to classify applications with some method, and then base PBRM information to these application classes.

One option to classify the applications is to use EPS QoS parameters (e.g. QCI and/or bitrate) for known service types. E.g. conversational voice and video (QCI 1-2) need access that has low delay. Depending on the operator network setup, PBRM information could indicate the usage of different radio access technologies or networks for different QCI values. In addition, operators may want to direct traffic flows with high bandwidth requirements to certain accesses and restrict peer-to-peer traffic in certain access in their policies. As an example, possible PBRM information based on QCI classification for different applications is shown on the following figure.

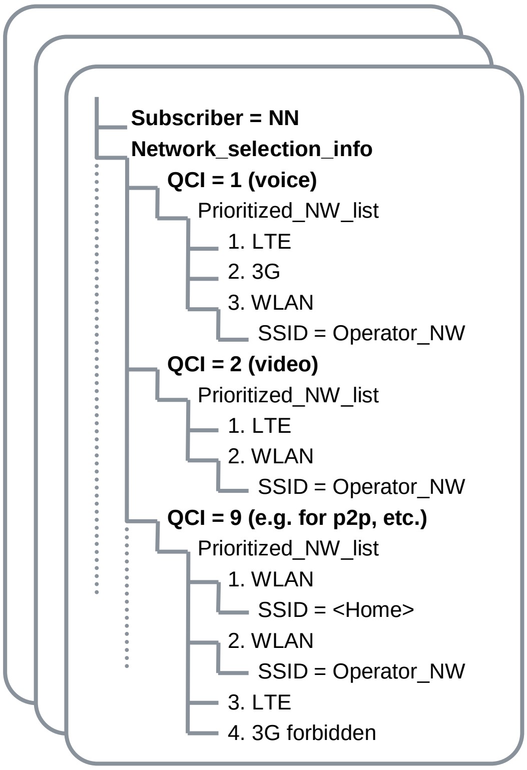

Figure 3. An example of PBRM server information for service based access selection.

UEs supporting LTE/E-UTRAN and/or SAE/EPC over non-3GPP radio accesses are required to have support for QCI classification for application connection setup. Thus, UEs employing QCI mechanisms for LTE could also use it for other non-3GPP radio accesses when communicating with EPC. Some other application classification mechanism, e.g. based on DiffServ, would be needed if no LTE/SAE is supported in the UE.

PBRM server can provide information for both network discovery and network selection, as defined in [1]. The PBRM network selection information can be used for the initial network selection as well as for handovers. For service based access selection, there should be no special cases where the same network selection information could not be used for both initial network selection and handovers.

8. Conclusions

Service based access selection is fairly complex feature that requires modifications to various specifications both in IETF and 3GPP. In 3GPP, there already has been a study item for similar kind of mechanism as described in this document. The work for the study item still continues, the current status can be found from [9]. However, currently it is unclear if service based access selection will ever be turned from study item to standardization work in 3GPP. Corresponding work on IETF will proceed irrespective of the 3GPP progress.

By nature, service based access selection requires that the UE is able to use more than one radio access technology at a time. It seems now that LTE/E-UTRAN (and SAE/EPC) will be the dominant 4G technology in future. Thus, if service based access selection is standardized some day, the solution will most probably involve EPS in a form or another.

It seems PBRM could have a role in service based access selection. PBRM could be used to inform UEs about the operator policies for network selection for different application classes. This is valuable information for an UE: by delivering this information via PBRM, there is no need for access network selection negotiation between UE and the network for every single connection and handover separately. This can make the implementation of service based access selection less complex both in the UE and network.

9. References

[1] Policy-Based Resource Management, Future Internet Program, Activity 2.4 Deliverable DA2.4.1, 2H2008

[2] IETF Internet-Draft, Current Practices for Multiple Interface Hosts, draft-mrw-mif-current-practices-02.txt (March 25, 2009)

[3] LTE, The UMTS Long Term Evolution, Stefania Sesia, Matthew Baker, Issam Toufik, Wiley & Sons, 2009

[4] Nokia Siemens Networks Flexi Intelligent Service Node, http://www.nokiasiemensnetworks.com/NR/rdonlyres/6C95AE1D-B085-4E0F-BA9F-5945FA55AE86/0/Flexi_ISN_Brochure.pdf

[5] IETF Internet-Draft, draft-ietf-monami6-multiplecoa-13.txt, "Multiple Care-of Addresses Registration", work in progress. (April 20, 2009)

[6] IETF Internet-Draft, draft-ietf-mext-flow-binding-01.txt, "Flow Bindings in Mobile IPv6 and Nemo Basic Support", work in progress. (April 28, 2009)

[7] QoS Mechanism in EPS, ZTE Corporation, Huang Tao, Zhang Zhijiang, Liu Yunjie, http://www.zte.com.cn/pub/endata/magazine/ztecommunications/2009year/no1/articles/200903/t20090319_170889.html

[8] 3GPP TS 23.402 Architecture enhancements for non-3GPP accesses (Release 8), version 8.4.1, January 2009.

[9] 3GPP TR 23.861 Multi access PDN connectivity and IP flow mobility (Release 9), version 1.1.1, April 2009.

[10] 3GPP TS 23.203 Policy and charging control architecture (Release 8), version 8.5.0, March 2009.

10. Acknowledgements

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